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 III

COMPTES RENDUS DES AUDITIONS
(du 11 mars au 9 juin 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

Audition, ouverte à la presse, de Mme Naomi Peres, secrétaire générale adjointe du secrétariat général pour l'investissement (SGPI), et de M. Clément Jakymiw, directeur adjoint du programme industries et services du secrétariat général pour l'investissement
(11 mars 2021)

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. Nous recevons Mme Naomi Peres, secrétaire générale adjointe, et M. Clément Jakymiw, directeur adjoint du programme industries et services, du secrétariat général pour l'investissement (SGPI).

Le secrétariat général pour l'investissement est chargé, sous l'autorité du Premier ministre, de mettre en œuvre le programme d'investissements d'avenir (PIA). Ce programme soutient les projets d'excellence dans les filières structurantes pour la France et fait l'objet d'un suivi attentif par le Parlement. Trois programmes d'investissements d'avenir ont été initiés depuis 2010. Un quatrième PIA, d'un montant total de 20 milliards d'euros sur cinq ans, a été créé par la loi de finances pour 2021.

Nous partageons, Mme la secrétaire générale adjointe et M. le directeur adjoint, bon nombre de problématiques : le soutien aux projets technologiques critiques est en effet nécessaire pour construire une forme de souveraineté numérique nationale et européenne – c'est l'objet du plan de relance et du PIA 4 dont votre service est chargé. Nous souhaitons donc vous interroger sur votre vision dans ce domaine et sur la façon dont vos activités s'articulent avec celles du Haut-commissaire au Plan.

M. Philippe Latombe, rapporteur. Je souhaite vous interroger sur trois points en particulier.

Nous aimerions d'abord vous entendre sur ce que la souveraineté numérique recouvre, selon vous. Ce sujet 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 vous appréhendez cette notion et de quelle façon les investissements d'avenir contribuent à promouvoir une forme de souveraineté numérique nationale ou européenne.

Je souhaiterais ensuite vous interroger sur les forces et faiblesses françaises dans les technologies stratégiques pour notre avenir, puisque vous disposez d'une vision très large de ces enjeux. Diverses initiatives ont d'ores et déjà été mises en œuvre au niveau européen, comme le plan intelligence artificielle présenté en 2018, le plan quantique annoncé plus récemment ainsi que le plan nano 2022. Nous souhaiterions connaître l'état des lieux des initiatives suivies par le SGPI et prendre connaissance des segments dans lesquels il nous faudrait, selon vous, renforcer notre action.

Enfin, j'aimerais que nous échangions sur le financement de l'innovation en France et sur la question des brevets. Nous avons auditionné France Brevets, structure créée en 2011 dans le cadre du PIA 1. Ses représentants nous ont indiqué que les entreprises françaises ont intérêt à se protéger des stratégies d'agression en achetant un certain nombre de brevets impactant leurs concurrents. La protection de nos pépites et les opportunités d'acquisitions d'acteurs clés semblent être un enjeu économique important. Je souhaiterais recueillir votre avis sur ce sujet, qui renvoie à une approche assez offensive de la souveraineté numérique.

Mme Naomi Peres, secrétaire générale adjointe du secrétariat général pour l'investissement (SGPI). Nous nous sommes intéressés à la notion de souveraineté avant la crise, lorsque nous avons commencé à préparer le quatrième PIA, en 2019. Nous avions alors convenu que la doctrine ou le principe d'investissement du PIA ne pouvait plus être la seule croissance – évidemment, le PIA vise à investir pour l'avenir, à créer des emplois et à développer la croissance, mais plus seulement. Nous avons donc réfléchi à compléter les principes d'investissement du PIA avec, d'une part, la transition écologique et, d'autre part, un concept rassemblant les aspects de résilience, de souveraineté et d'autonomie. Je vous rejoins sur le fait que la définition de la souveraineté n'est pas si simple. Nous retenons la définition suivante : la capacité d'apprécier une situation et de décider et d'agir sans contrainte et sans influence extérieure. Cette définition s'applique à l'État souverain. Nous lui avons préféré, dans le PIA 4, la notion de résilience, qui est à nos yeux plus large et emporte aussi une notion de souveraineté et d'autonomie. La résilience est la capacité d'un pays ou d'une organisation à résister aux conséquences d'une crise ou d'une agression et à retrouver le plus rapidement possible un fonctionnement normal, même si celui-ci est différent du fonctionnement précédent. La notion de résilience emporte donc mécaniquement la notion de souveraineté, en particulier en matière numérique. Les principes d'investissements du PIA sont donc constitués des trois concepts suivants : croissance potentielle, transition écologique et résilience des organisations socio-économiques au sens large.

En souhaitant appliquer cette notion à la matière numérique, nous avons réfléchi à trois grands aspects : le matériel, le logiciel et les usages. Ces trois éléments sont assez liés. Nous nous sommes posés la question suivante : dans quoi serait-il légitime d'investir, pas seulement dans une logique de retour sur investissement purement financier, mais extra-financier, c'est-à-dire dans une logique permettant d'augmenter notre autonomie, notre capacité à décider, notre capacité à rester maîtres de nos données, de nos logiciels et de nos matériels ?

Nous souhaitons appliquer cette notion à tous les domaines à chaque fois que nous bâtissons une stratégie, et pas seulement au numérique : la nouvelle logique du PIA 4 est construite autour de grandes stratégies d'investissement. Pour le PIA 4, nous avons souhaité prendre le temps de réunir l'ensemble des ministères compétents et de consulter assez largement, avant de lancer des appels à projets. Ainsi, nous associons largement les chercheurs, les parties prenantes, les collectivités territoriales, les entreprises. Avant de lancer un programme de recherche ou un programme d'investissement industriel, nous nous interrogeons de la manière suivante : dans ce domaine, quels sont les forces et faiblesses du pays, où se situent les besoins et un programme comme le PIA peut-il intervenir intelligemment ? Pour cela, nous essayons également d'articuler les outils normatifs, fiscaux et réglementaires, car nous avons plus de chances de réussir une transformation si nous nous sommes mis d'accord ensemble, auparavant, sur la feuille de route pour y arriver.

Nous avons travaillé de cette manière dans le secteur numérique. Les premières stratégies présentées par le Président de la République sont la stratégie quantique et la stratégie cyber. Plusieurs autres stratégies sont actuellement en cours d'élaboration, avec des consultations en ligne et des appels à manifestations d'intérêt. Nous tâchons d'appliquer cette notion de résilience et de souveraineté à tous les domaines. Nous l'avons, par exemple, appliquée à la stratégie hydrogène. Nous nous sommes interrogés de la manière suivante : quelle est la capacité de production d'hydrogène en France et à quel moment devons-nous déclencher le mécanisme d'aide à l'achat ? Il s'agit de trouver l'équilibre entre la volonté de développer rapidement l'hydrogène vert et bleu et le souci d'éviter d'acheter des catalyseurs chinois. Il y a donc un équilibre à trouver entre la volonté d'atteindre rapidement des objectifs et la volonté de garantir, grâce à ces investissements, notre autonomie et notre souveraineté.

En matière de numérique, cette logique est à l'œuvre dans les investissements conduits en faveur des matériels pour la 5G ou la 6G : nous veillons à ne pas être trop dépendants de matériels ou de composants dont nous ne maîtrisons pas la chaîne de production. Il en va de même pour le logiciel. Nous avons largement investi dans l'intelligence artificielle de confiance, avec le souci suivant : comment certifier les logiciels d'intelligence artificielle qui prendront peut-être, demain, une place prépondérante dans nos vies ?

Nous travaillons depuis trois ans à réaligner les investissements du PIA avec les activités de chaque ministère. Nous sommes un service du Premier ministre, afin de faire travailler ensemble toutes les parties prenantes avant de débloquer les fonds. Nous évitons d'adopter des prises de position et des points de vue qui ne seraient pas construits et partagés en interministériel. Le rôle du SGPI est très structurant dans le travail gouvernemental : il consiste à réunir tous les acteurs et à ouvrir la discussion avec des experts externes. Nous forgeons notre avis et nos convictions sur la base des avis d'experts, qu'ils soient issus des ministères, du Parlement ou de l'Organisation de coopération et de développement économiques (OCDE). Le SGPI ne regroupe que trente personnes, nous avons donc besoin de recourir à des sources d'expertise extérieures. Ce que je vous livre est donc le fruit d'une réflexion collégiale et ouverte au-delà du seul SGPI.

Nous avons travaillé sur la notion de souveraineté avec le Secrétariat général de la défense et de la sécurité nationale (SGDSN) et le Service de l'information stratégique et de la sécurité économiques (Sisse). Lors de la préparation du PIA 4, nous avons abouti à la conclusion suivante : la croissance économique est très bien caractérisée ; la transition écologique commence à l'être également, en particulier quant aux sujets de décarbonation et de référentiels d'appréciation de la biodiversité ; en revanche, il existe moins de littérature sur la résilience et sur la souveraineté. Nous avons donc collaboré avec les services qui travaillent de longue date sur ces sujets, pour savoir comment transposer une logique de souveraineté ou d'autonomie à d'autres champs, par exemple à l'éducation ou à la vieillesse. La notion d'autonomie et de résilience peut exister dans de nombreux autres domaines et nous devons réfléchir à la façon de la caractériser.

Nous nous efforçons d'apprécier les forces et faiblesses des différents secteurs en matière de souveraineté numérique. Nous considérons, par exemple, que la France dispose de toutes les compétences de haut niveau en matière quantique. Nous disposons de chercheurs compétents et nous réussissons à créer de formidables start-up dans ce domaine ; mais souvent, au moment où elles se mettent à grossir et qu'elles sont en capacité de conquérir des marchés, elles se heurtent à la fragmentation des marchés européens. Je pense que nous avons dépassé le sujet du financement en matière numérique : nous arrivons, à l'échelle européenne, à mobiliser les financements nécessaires pour permettre à ces entreprises de croître. Il se pose, en revanche, un sujet d'accès au marché en Europe. Il est plus facile, pour les entreprises, d'aller conquérir le marché américain que de s'adapter aux différents marchés européens. Nous essayons de mener ce diagnostic de forces et faiblesses, de manière très précise, pour chacune de nos stratégies. Les forces et faiblesses sont assez variables en fonction des secteurs considérés : en matière de cybersécurité, l'enjeu est de ne pas perdre l'avance gagnée ; en matière quantique, l'enjeu est d'abord d'investir dans l'amont, c'est-à-dire dans la recherche et le transfert technologique.

M. Clément Jakymiw, directeur adjoint du programme industries et services du secrétariat général pour l'investissement (SGPI). J'ajouterai un complément à propos du lien entre la notion de souveraineté et celles d'autonomie et de résilience. Ces notions sont différentes. On peut être souverain, sans nécessairement faire preuve d'autonomie ou d'une très forte résilience. Les enseignements de la crise sont extrêmement intéressants à cet égard :

ils ont montré que les notions d'autonomie et de résilience sont bien plus prégnantes que l'on pouvait l'imaginer auparavant. Cela est particulièrement visible dans le domaine de la santé, en raison des débats soulevés à propos des masques, des respirateurs ou des vaccins. Il faut bien entendu généraliser cette réflexion au secteur du numérique. Cette notion de souveraineté, avec un double prisme d'autonomie et de résilience, est au cœur des attentions médiatiques et des industriels.

M. Philippe Latombe, rapporteur. Petite équipe d'une trentaine de personnes, placée sous l'autorité du Premier ministre, ce format vous apporte-t-il de l'agilité, et cette agilité est-elle une force dans l'exercice de votre mission ? Le fait d'être placé sous l'autorité directe du Premier ministre vous donne-t-il une capacité à mobiliser, beaucoup plus importante ?

D'autre part, ne nous manque-t-il pas aujourd'hui une administration spécialisée dans l'innovation et le numérique ? Le secrétaire d'État au numérique est à Bercy ; la ministre déléguée à l'innovation l'est également. Les activités ne devraient-elle pas être plus transversales ?

Mme Naomi Peres. Il n'est pas facile de trouver le juste milieu entre une « agencisation » sur le format de l'Agence d'innovation de défense (AID) et notre format actuel. L' « agencisation » aurait beaucoup d'avantages, car les moyens de mise en œuvre des crédits seraient concentrés. Cela nous rendrait également plus visibles. Notre service est peu connu des bénéficiaires finaux. Nos grands opérateurs sont Bpifrance, la Caisse des dépôts et consignations, l'Agence de l'environnement et de la maîtrise de l'énergie (ADEME) et l'Agence nationale de la recherche (ANR) – nos bénéficiaires les connaissent beaucoup mieux que nous. Ce modèle a été décidé il y a dix ans : il explique que ce sont souvent ces grands opérateurs qui sont identifiés comme les acteurs de l'innovation dans leur domaine. Nous avons capitalisé sur l'image et sur la force de ces grands opérateurs.

Le fait d'être placés à Matignon nous offre effectivement une grande agilité. Ce rattachement est, à mes yeux, extrêmement important. Nous sommes un petit service, rassemblant des directeurs « métiers », experts dans leurs domaines et fonctionnant quasiment sous la forme d'un cabinet. Nous bénéficions d'une grande liberté d'accès aux administrations et aux ministères. En ce qui concerne la construction des stratégies et des politiques d'innovation, notre force est de pouvoir réunir des acteurs multiples pour les faire travailler ensemble à la construction d'un projet commun. Il est parfois difficile de garantir l'équilibre des arbitrages. Notre responsabilité est de proposer au Premier ministre des arbitrages et des décisions de financement. Il n'y a pas de lieu plus neutre que Matignon pour faire valoir les différents points de vue. *In fine*, Matignon arbitre et c'est son rôle. Le rattachement au Premier ministre est, à mes yeux, fondamental.

Ce sujet est un petit peu différent de la forme. L'équilibre du modèle entre, d'une part, « l'agencisation », sur le modèle de l'agence de l'innovation, et, d'autre part, un petit secrétariat, sur le format du secrétariat général à l'investissement qui s'appuie sur les opérateurs, pose une vraie question. Les deux options ont leurs avantages et leurs inconvénients. Cette question a été en partie développée dans le rapport de notre comité de surveillance. Le rapport a développé les différents modèles d'organisation possibles. Chacun des modèles suppose des moyens différents en administration centrale. Chaque modèle a également des impacts en matière d'appropriation des stratégies d'investissement par les ministres. Cela n'aurait pas beaucoup de sens de financer une stratégie *cloud* qui ne serait pas articulée avec ce qui est en train d'être négocié, par le secrétariat d'État au numérique, au niveau européen, sur la sécurisation du *cloud*, ou avec la stratégie de l'État en matière de *cloud*. Aujourd'hui, notre service est discret et ne concurrence pas les ministres, en termes de visibilité et de portage.

Cela est important, si l'on réfléchit au fait que ces actions doivent essaimer dans le temps. Le PIA est un programme d'innovation qui intervient dans beaucoup de secteurs et dont le rôle est de faire la preuve de concept. Ce programme ne sera jamais capable de gérer un déploiement. Si l'on centralise trop et que les ministères ne s'approprient pas le travail sur l'innovation, on risque alors, quand l'innovation aura fait ses preuves, que les ministères ne s'en emparent pas et ne lèvent pas les derniers verrous réglementaires à son déploiement. Il n'est pas si simple de trouver le bon modèle en matière d'innovation.

S'agissant du rattachement du secrétariat d'État au numérique à Matignon ou à Bercy, nous travaillons avec tous les ministres et les secrétaires d'État, quel que soit leur rattachement. Si le positionnement à Matignon aide dans la discussion interministérielle, en revanche, les moyens d'administration sont à Bercy. Il n'y a donc pas de réponse évidente, s'agissant du positionnement du secrétariat d'État au numérique. Nous nous attachons à faire vivre cette notion d'innovation en interministériel : un seul comité interministériel suit l'ensemble des stratégies d'investissements. Il est important de garder une dynamique collective : tous les ministères sont présents autour de la table, même quand nous discutons de sujets pointus, comme la 5G ou le *cloud*. Petit à petit, la transversalité se construit. Depuis dix ans, le PIA a toujours été capable de travailler en interministériel.

Le PIA 1 a financé France Brevets, dont le modèle économique et le format sont actuellement en cours d'examen. Le gouvernement ne s'est pas encore prononcé à ce sujet. Nous avons veillé à traiter du mieux possible la composante propriété intellectuelle au sein de chacune de ces stratégies d'accélération. Tout un chapitre lui est consacré dans les stratégies cyber et quantique. Nous nous demandons comment mobiliser les bonnes expertises. L'achat de brevets, qui est une stratégie agressive, n'est pas la seule solution. Nous réfléchissons également à accompagner nos start-up pour les amener à protéger leurs technologies, au bon moment, avant d'en acheter d'autres. Un défaut d'accompagnement persiste aujourd'hui à ce sujet et nous travaillons avec Bpifrance pour construire cette offre de services. Ce sujet est identifié, à la fois sur la base du retour d'expérience et des expertises de France Brevets, et du rôle d'accompagnement de Bpifrance auprès des start-up. Nous essayons de construire une offre de services, dont une partie sera quasiment assurée par du service public, et une autre partie recouvrira l'activité concurrentielle de France Brevets. L'intervention de l'État ne peut donc pas être la même dans les deux cas. Le PIA 4 accordera les moyens nécessaires afin que la protection de la propriété intellectuelle, et éventuellement, par la suite, les stratégies d'acquisition, puissent être mises en œuvre, si elles sont pertinentes dans le domaine considéré.

M. Philippe Latombe, rapporteur. Vous avez exprimé, dans votre propos liminaire, l'idée selon laquelle il est nécessaire d'arbitrer entre la volonté de développer rapidement la filière de l'hydrogène et la volonté de ne pas acheter des catalyseurs chinois : il faut donc trouver un moyen de promouvoir la filière en achetant des produits français ou européens. Dans le numérique, les entreprises françaises font part de leurs difficultés à accéder aux marchés publics. Dans le même temps, les acteurs publics mettent en avant la simplicité du recours à des solutions intégrées américaines, qui fournissent des prestations de *cloud* et les outils logiciels les accompagnant. Cela traduit une sorte de dissonance cognitive : d'un côté, les pouvoirs publics veulent promouvoir les solutions françaises et européennes et y investissent beaucoup d'argent ; de l'autre, les marchés publics sont construits de telle façon que seuls les grands acteurs peuvent y répondre. Comment voyez-vous les choses ?

Mme Naomi Peres. Il faut distinguer les sujets sur lesquels l'offre est déjà présente (ce qui n'est pas le champ d'intervention du PIA) et les sujets sur lesquels elle ne l'est pas. L'offre des géants du Web – Google, Apple, Facebook, Amazon et Microsoft (GAFAM) – ne recouvre pas le champ d'intervention du PIA. Le PIA s'intéresse à des solutions futures. En

matière de cyber, par exemple, la bataille n'est pas perdue : il est encore temps de construire une offre française, qui constituerait une troisième ou quatrième voie. Nos services publics, demain, pourraient recourir à des solutions de cybersécurité issues d'une offre industrielle française. Cette offre n'existe pas encore. Les entreprises reconnaissent que le marché constitué par les collectivités territoriales, les hôpitaux, les ports, les gares est considérable, mais il n'est pas du tout organisé pour leur parler.

Le PIA 4 va permettre de mettre en place des démonstrateurs territoriaux. Nous avons voulu contrecarrer la critique récurrente adressée au PIA, selon laquelle le programme produit de l'innovation sur étagère, sans aller au bout de la preuve de concept et sans tester cette innovation dans des conditions réelles. Nous avons donc créé un nouvel instrument, intitulé « soutien au déploiement », qui a vocation à financer des formations et à tester, dans des conditions réelles, les technologies en pré-déploiement.

En ce qui concerne la cybersécurité, les démonstrateurs territoriaux vont identifier des territoires pilotes, en avance sur le sujet, qui vont nous aider à qualifier l'offre industrielle française. Ensuite, nous financerons le surcoût de développement ou d'adaptation de cette offre pour qu'elle puisse se retrouver sur le marché. L'enjeu est de créer des solutions industrielles correspondant aux besoins des acteurs publics, collectivités locales, hôpitaux ou ports. Si nous ne faisons pas, aujourd'hui, les efforts nécessaires pour faire dialoguer les parties prenantes sur le sujet, un acteur extérieur viendra, demain, développer cette offre. Il serait très frustrant que cette offre ne soit pas française, car nous avons tout ce qu'il faut pour la développer.

La question s'est également posée, de manière très concrète, en matière éducative. En préfiguration de la stratégie sur l'éducation et le numérique qui sera annoncée par le Premier ministre à la fin du mois de mars, nous avons développé un certain nombre d'actions en 2020, pour un budget total de 300 millions d'euros de PIA. Nous optons pour une approche intégrée par territoire, et non plus par grand plan. Nous avons identifié quelques territoires pilotes et nous y avons investi dans la formation des professeurs et des parents ainsi que dans les équipements. Les start-up et les entreprises des technologies de l'éducation (*EdTech*) ne veulent plus de financements, elles veulent que nous les aidions à faire sauter le verrou d'accès au marché de l'Éducation nationale. Sur ces démonstrateurs financés par le PIA, nous avons pu faire « sauter les verrous ». Avec les vingt démonstrateurs territoriaux du PIA 4, nous espérons montrer que donner aux acteurs de terrain la liberté de choisir eux-mêmes des solutions – dont on sait, grâce à l'ANSSI, qu'elles sont solides – fonctionne. Nous souhaitons casser la logique de passer par d'énormes marchés publics qui ne peuvent être obtenus que par d'énormes entreprises, alors que de petits marchés peuvent être satisfaits par de petites entreprises.

Dans le PIA 4, nous avons souhaité que les procédures compétitives et ouvertes puissent prendre d'autres formes, y compris celle des partenariats d'innovation. Les marchés publics permettent beaucoup de choses. Nous sommes frileux à l'idée d'utiliser les outils à disposition : les partenariats d'innovation sont un outil formidable, qui est très peu mis en œuvre. Il est toujours plus facile et moins risqué de mettre en œuvre des marchés publics classiques. Les partenariats d'innovation permettent de travailler avec de plus petits partenaires sous la forme du dialogue compétitif. Ils permettent également de travailler en direct, en faisant appel à plusieurs entreprises pour des sommes inférieures à 40 000 euros. Nous y avons régulièrement recours pour les besoins très spécifiques du SGPI. Il est facile de blâmer les marchés publics : le droit des marchés publics autorise beaucoup d'outils, que nous n'utilisons pas encore assez.

M. Philippe Latombe, rapporteur. En matière éducative, vous vous êtes rendus compte que les envies et les besoins du fournisseur et du client convergeaient, et que les marchés publics centralisés posaient problème. Est-ce le cas dans d'autres domaines que l'éducation ? Comment, à terme, mettre en œuvre cette liberté et cette territorialisation à plus grande échelle ? Comptez-vous sur des outils législatifs et réglementaires ?

Mme Naomi Peres. En la matière, il est important d'« embarquer » tout de suite les ministères. Il est difficile de centraliser ces dynamiques dans une agence de l'innovation. Il a fallu du temps pour mettre au point cette stratégie et travailler avec tous les services du ministère de l'Éducation nationale et du ministère de l'Enseignement supérieur. Cela nécessite une forte volonté des ministres concernés.

Aujourd'hui, nous ne voulons plus débloquer des moyens du PIA, si nous n'avons pas répondu à la question : « que se passera-t-il si cela marche ? ». La réponse à cette question nécessite un engagement mutuel entre les ministères : les ministères doivent identifier les moyens qu'ils réorienteront et mobiliseront, si la stratégie d'innovation fonctionne. Ils doivent s'engager quant à leurs actions, si la preuve de concept est faite. Ensuite, il faut espérer que la ligne soit tenue. Cette discussion a eu lieu, y compris avec les opérateurs du ministère de l'Éducation nationale, comme le réseau Canopé.

Un budget comme le PIA donne une capacité d'action rapide pour mettre en place des pilotes et des expérimentations. Cela permet au ministère de prendre le temps de construire sa stratégie sur la base d'une expérimentation qui a fonctionné. Les ministères témoignent d'une certaine aversion au risque : il est très difficile de réussir à préserver leurs budgets d'innovation. En période de crise, les premiers budgets que l'on coupe dans les entreprises sont ceux alloués à la communication et à l'innovation. L'État a donc repris à sa charge ces postes de dépenses : le budget du PIA 4 est ainsi passé de 10 à 20 milliards d'euros. Le PIA permet cette respiration. Des envies s'expriment au sein des ministères : notre travail consiste à les trouver, à les réunir et à les entraîner. L'« agencisation » permet d'aller plus vite sans forcément produire des résultats plus transformants. Les moyens réglementaires ne nous appartenant pas, il nous faut donc convaincre par la preuve.

M. Philippe Latombe, rapporteur. Dans votre travail de mutualisation, quels rapports entretenez-vous avec le Haut-commissaire au Plan ? Vous intervenez à la fois sur la prospective et sur la mise en œuvre. Comment mutualisez-vous les idées ?

Quels domaines du numérique n'avons-nous pas investi alors que nous le devrions, d'autres pays étant, eux, en train de les investir ?

Mme Naomi Peres. Un des principaux services du Haut-commissariat au Plan est France Stratégie, un service du Premier ministre avec lequel nous travaillons de longue date. Notre temporalité n'est pas la même que celle du Haut-commissariat au Plan. Nous sommes une petite équipe. Par conséquent, nous construisons notre capacité prospective sur la base de travaux existants, et notamment ceux élaborés par France Stratégie. Nous entretenons par ailleurs beaucoup de liens avec eux au titre d'une autre de nos missions : l'évaluation socio-économique des grands projets d'investissement. Le Haut-commissariat rend visible un travail de prospective que nous pouvons intégrer. Lorsque nous construisons une stratégie à cinq ans, il est extrêmement intéressant de savoir quelle est la stratégie de l'État à dix ans. Nos travaux s'articulent donc assez naturellement.

Nous avons voulu construire un PIA qui ne soit pas préprogrammé à l'avance. Notre PIA est désormais désectorisé. Il est construit avec des grands outils d'intervention, de l'amont à l'aval, mais nous n'indiquons plus à l'avance quel montant du budget sera consacré aux

transports, à l'hydrogène ou à la cybersécurité. Nous disposons de moyens, nous avons construit une doctrine et des principes d'intervention, et nous les appliquons à différentes stratégies. Si demain, le Haut-commissaire au Plan identifie un sujet majeur de transformation publique qui nécessite des investissements dans l'innovation, le PIA peut intervenir. Nos travaux se répondent donc.

En ce qui concerne les secteurs du numérique, certaines stratégies sont déjà annoncées et une vingtaine, en cours d'élaboration, font l'objet de consultations publiques ou d'appels à manifestation d'intérêt. Ces stratégies en cours d'élaboration dans le numérique sont les suivantes : l'enseignement et le numérique ; la santé numérique ; la 5G et les technologies des réseaux de communications ; un complément à la stratégie d'intelligence artificielle concernant la confiance dans l'intelligence artificielle ; le *cloud* ; le verdissement du numérique ; la nanoélectronique à la suite du plan nano ; les transports pour le volet de digitalisation des mobilités ; la transition numérique des industries culturelles. Le numérique prend une très grande place dans le PIA 4 : indépendamment des sujets abordés d'un point de vue technologique, le numérique sera présent dans nombre des stratégies d'investissement que nous financerons. Le numérique est pour nous, à la fois, un secteur et un levier très transverses.

Tous ces domaines ont été identifiés après une large consultation. Si demain un domaine était identifié comme prioritaire – comme le quantique l'a été –, notre programme peut intervenir, du moment que l'on respecte sa doctrine et que l'on pense au déploiement des innovations. Il n'y a pas de restriction à cet égard.

M. Philippe Latombe, rapporteur. Que recouvre la stratégie relative à l'enseignement ?

Mme Naomi Peres. Je ne souhaite pas dévoiler les annonces prochaines. Nous pourrons vous faire connaître les actions conduites en préfiguration de cette stratégie, qui ont commencé dès 2020. En plus du dispositif des démonstrateurs territoriaux, nous avons œuvré à doter les universités de moyens pour hybrider les formations. Nous avons également couvert un volet de recherche, qui comprend la constitution de cohortes pour pouvoir suivre les élèves sur le long terme. Nous souhaitons transposer, dans l'éducation, la logique des grands équipements de recherche que sont les cohortes pour la santé. Nous avons également travaillé sur l'intelligence artificielle appliquée à l'éducation et ouvert un concours d'innovations pour débloquer des financements. Nous travaillons enfin énormément à la formation : nous avons travaillé sur les instituts nationaux supérieurs du professorat et de l'éducation (Inspé) du futur ; nous avons également développé la formation à distance des enseignants.

La stratégie « Éducation et numérique » expose aussi, en plus des investissements du PIA, les actions du ministère et de ses opérateurs pour déployer les innovations. Cette stratégie apporte une visibilité sur les actions à venir pour les trois ou quatre prochaines années, qu'il s'agisse des investissements du PIA en faveur de l'innovation et des actions de déploiement et de généralisation du ministère et de ses opérateurs.

M. Philippe Latombe, rapporteur. Votre démarche apporte des financements et des solutions technologiques. Comment le ministère vous accompagne-t-il par un mouvement de fond, permettant l'intégration de ces technologies dans les formations des professeurs ou dans la scolarité des élèves ? Avez-vous un effet d'entraînement sur les ministères ?

Mme Naomi Peres. Nous essayons d'avoir un effet d'entraînement. Nous évaluons beaucoup nos actions. L'effet d'entraînement se mesure différemment en fonction des secteurs. Il est assez nouveau, pour nous, d'intervenir dans l'éducation avec cette ampleur. Nous n'avions jamais pu, par le passé, construire une stratégie d'innovation avec le ministère.

Sur ce sujet, notre démarche ne peut fonctionner que s'il existe un très fort alignement avec la stratégie du ministère. Par exemple, nous finançons quatre Inspé du futur, à charge ensuite, pour le ministère, de généraliser les dispositifs qui auront fonctionné.

De manière générale, nous appliquons à la sélection de nos projets un critère de réplicabilité. Nous nous posons la question suivante : les projets que nous finançons ont-ils la capacité à être généralisés ? S'il s'agit d'une technologie, nous nous interrogeons sur la demande existante pour cette technologie et sur la capacité des industriels à l'insérer dans leurs processus de production.

Les projets territoriaux supposent de complètement renverser cette approche. Par l'action « Territoires d'innovation » par exemple, nous avons cherché des porteurs de projets aux idées novatrices. Nous avons donc identifié des sujets, aussi bien dans la santé que dans l'agriculture. Nous souhaitons accompagner les acteurs à agir différemment. Ce programme est novateur et il a été difficile à monter.

Notre logique pour convaincre de généraliser les innovations que nous finançons est la suivante :

– tout d'abord, associer le ministère, en amont, dans l'élaboration de la stratégie – cela est plus long car nous prenons le temps de nous mettre d'accord sur une feuille de route ;

– ensuite, démontrer que les solutions fonctionnent.

Nous avons la chance d'être rattachés au Premier ministre. Le PIA 4 est allé un cran plus loin : nous apportons désormais un soutien au déploiement en finançant des formations et de l'ingénierie de formation. Nous sommes prêts à aller jusqu'au bout de la preuve de concept. Une fois que cette preuve de concept est faite, il n'appartient plus au SGPI de la déployer. Parfois, il revient au marché de prendre le relais. Parfois, le ministère doit prendre le relais pour faire « sauter les derniers verrous ». Parfois, enfin, les opérateurs comme la Caisse des dépôts et consignations prennent le relais. Cela peut très bien fonctionner. Le premier financement est souvent le plus difficile – c'est pourquoi nous sommes là.

M. Philippe Latombe, rapporteur. Y'a-t-il des ministères ou des secteurs d'activité dans lesquels vous n'êtes jamais sollicités ? Ou à l'inverse, vient-on vous solliciter avec de nombreux projets – qui ne sont pas tous innovants – et êtes-vous obligés de faire un tri ?

Mme Naomi Peres. Le PIA 4 a beaucoup élargi notre champ d'intervention. Cela ne veut pas dire que nous interviendrons dans tous les domaines. Nous souhaitons avant tout élaborer une stratégie conjointe avant de lancer un appel à projets. Les situations sont très hétérogènes. Certains ministères sont très mûrs et l'élaboration d'une stratégie d'innovation peut aller très vite. Pour certains ministères, cette démarche est nouvelle : elle prend plus de temps – car il s'agit des ministères avec lesquels nous travaillions moins, le PIA ayant historiquement moins investi dans leurs secteurs d'intervention.

Il n'y a pas de ministère avec lequel nous ne travaillons pas du tout. En revanche, nous travaillons davantage avec certains ministères : le ministère de l'industrie et le ministère de la recherche sont de grands « clients ». Nous essayons même d'articuler nos interventions avec le ministère de la défense en matière de technologies duales. Nous ne travaillons en revanche pas beaucoup avec le ministère de la justice.

M. Philippe Latombe, rapporteur. Je m'interrogeais justement sur deux ministères : le ministère de la justice et le ministère de l'intérieur.

Mme Naomi Peres. Le PIA 4 est ouvert. Si un ministère présente une stratégie d'intervention qui procure des retombées en matière de transition écologique ou de résilience, le PIA peut intervenir. Nous avons souhaité renforcer encore davantage sa dimension interministérielle et ouvrir le champ à de nouveaux secteurs, dans la limite des conditions d'intervention du programme.

M. Philippe Latombe, rapporteur. Y a-t-il des sujets que nous n'avons pas abordés et que vous souhaiteriez porter à notre connaissance ?

Mme Naomi Peres. Je reviendrai sur la formation, qui est un domaine dans lequel le PIA a déjà beaucoup travaillé par le passé. L'intervention du PIA est très connue en ce qui concerne le regroupement d'universités. Nous avons également récemment conduit beaucoup d'investissements dans le champ de l'innovation pédagogique, par exemple, par les campus des métiers et des qualifications. Le PIA intervient aussi bien pour les masters et les thèses que pour l'ingénierie de formation professionnelle ou pour la formation initiale. Nous souhaitons renforcer cette dimension dans le PIA 4. L'enveloppe consacrée au soutien au déploiement s'élève à trois milliards d'euros sur cinq ans. Une bonne partie de ce budget concernera l'ingénierie de formation. Ce levier est extrêmement important.

M. Philippe Latombe, rapporteur. Comment articulez-vous l'action du PIA avec l'action menée au niveau européen ? Cela concerne à la fois la gestion des moyens et les orientations stratégiques. Couvrez-vous des domaines que l'Europe ne couvre pas, ou inversement ?

Mme Naomi Peres. Le PIA est intégré, pour une partie de ses crédits, dans le plan de relance. Le PIA porte ainsi la majeure partie du plan de relance dans le secteur du numérique. Le travail est en cours avec la Commission pour définir le contenu du plan de relance français : nous devons aligner les axes d'intervention en matière de numérique. Par ailleurs, nous travaillons au quotidien avec la direction générale du numérique, dont la mission principale est d'aligner les orientations de l'État sur celles de la Commission. L'alignement stratégique en matière de numérique est également très suivi par l'Élysée. Nous n'éprouvons donc pas de grande difficulté à comprendre les grandes orientations stratégiques dans ce domaine.

Nous devons néanmoins les mettre en œuvre. Nous avons travaillé en amont avec la Commission sur un appel à projets à destinations des universités européennes de recherche. Plutôt que de lancer un appel à projets français et un appel à projets européen, nous avons opéré de la manière suivante : puisque nous savons que le processus de sélection européen est extrêmement exigeant, nous nous sommes engagés à financer toutes les universités françaises retenues par la Commission. Nous avons travaillé en amont avec la Commission sur le cahier des charges et nous savons que leur processus de sélection est extrêmement exigeant, il est donc normal que nous nous alignions sur leur sélection. Nous pourrions dupliquer cette approche à des entreprises.

Nous travaillons également sur les régimes des *important projects of common european interest (IPCEI)* qui impliquent nécessairement deux pays au minimum. Nous travaillons sur plusieurs *IPCEI* avec l'Allemagne ; nous participons également à un *IPCEI* réunissant quatre pays sur le sujet du *cloud*.

De manière générale, la subsidiarité est une question intéressante. Considérant les volumes consacrés au numérique et les difficultés d'accès au marché européen, nous pourrions agir en subsidiarité, et décider de financer ce que l'Europe ne finance pas. Mais honnêtement, si les projets ne sont pas cofinancés par plusieurs États, je ne suis pas sûre que l'on puisse arriver à aligner les financements suffisants pour des projets numériques. Je ne sais pas si nous y aurions intérêt. Nous tentons plutôt de bien nous articuler avec l'action européenne et de simplifier au maximum les démarches pour les entreprises.

M. Clément Jakymiw. En ce qui concerne le partage des feuilles de route, nous nous posons systématiquement la question de l'articulation des dossiers qui nous parviennent avec le programme Horizon 2020. Nous devons comprendre comment les projets s'intègrent dans une dynamique de structuration des filières à l'échelle européenne, afin de soutenir des projets qui, à terme, pourront s'insérer sur le marché européen, parce qu'ils seront considérés par la Commission européenne. Cela est important. La notion de marché européen est critique dans le déploiement des entreprises en ce qui concerne le volet numérique. Nous nous posons donc systématiquement la question de l'articulation de la feuille de route nationale et de ses filières avec la feuille de route européenne, afin qu'il n'y ait pas de solution de continuité, mais qu'au contraire un biseau se crée, au niveau national, transnational et européen.

Mme Naomi Peres. J'ajouterai un élément sur le nouvel instrument French Tech Souveraineté. Nous y avons consacré des fonds propres. Les précédents PIA ont eu un vrai rôle de structuration du marché du financement, en particulier dans le numérique. Le PIA intervient en fonds de fonds pour la structuration du marché. Il intervient également en fonds direct en cas de faille de marché. Le nouvel instrument French Tech Souveraineté n'est pas un fonds d'investissement, il est une poche d'intervention à la main de l'État. Il permet, par exemple, de se défendre contre les comportements agressifs d'achats de start-up. Cette enveloppe d'intervention peut permettre de racheter des start-up, à la manière d'une petite agence des participations de l'État (APE) des entreprises technologiques. Nous avons donc renforcé l'arsenal des outils du PIA pour que nos pépites ne subissent pas la préemption d'un investisseur étranger.

Audition, ouverte à la presse, de M. le professeur Thibault Douville, professeur des universités, directeur du master Droit du numérique à l'Université Caen *Normandie*
(11 mars 2021)

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. Nous recevons M. le professeur Thibault Douville, professeur des universités en droit privé et directeur du master Droit du numérique à l'Université Caen Normandie.

Cette audition porte sur les aspects juridiques de la souveraineté numérique, s'agissant notamment de la protection des données personnelles. Plusieurs décisions sont intervenues à ce sujet ces derniers mois – la plus importante étant la décision *Schrems* II, rendue par la Cour de justice de l'Union européenne (CJUE) le 16 juillet 2020. Celle-ci invalide le *Privacy Shield*, c'est-à-dire la décision de la Commission européenne permettant le transfert de données par des entreprises européennes vers des pays tiers. Cette décision a suscité des doutes chez nombre d'acteurs, même si une recommandation du Comité européen à la protection des données est intervenue, depuis, pour préciser de quelle façon les entreprises pourraient, elles-mêmes, évaluer le cadre juridique externe afin de poursuivre correctement leurs transferts de données. Nous souhaiterons vous entendre également à propos des autres initiatives européennes en cours.

M. Philippe Latombe, rapporteur. Je souhaite vous questionner sur trois points en particulier.

Je souhaite d'abord vous interroger sur la définition de la souveraineté numérique. Ce sujet fait l'objet d'une attention croissante de la part des pouvoirs publics 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 vous appréhendez ce concept, en votre qualité de juriste, et quelle définition vous pouvez lui donner.

Ma deuxième interrogation concerne la décision *Schrems* II prise par la CJUE le 16 juillet 2020. De nombreux acteurs auditionnés, depuis le début des travaux de notre mission d'information, nous ont indiqué que cette décision avait créé beaucoup d'incertitudes. Le Health Data Hub a mandaté un cabinet d'expertise juridique pour en mesurer la portée exacte en ce qui concerne ses propres activités. J'aimerais donc que vous nous présentiez ses conséquences en droit et votre interprétation de sa portée.

Quelles sont les conséquences, pour la France, de l'arrêt de la CJUE du 2 mars 2021 concernant l'affaire *Prokuratuur*, dont les acteurs estiment qu'il pourrait poser des difficultés pour la bonne marche des procédures judiciaires françaises.

J'aimerais enfin aborder avec vous les différents projets de régulation du numérique et des données qui occupent l'actualité européenne ces derniers mois. Je pense en particulier au *Digital Services Act (DSA)*, au *Digital Market Act (DMA)* et au *Data Governance Act (DGA)*. Pensez-vous que ces initiatives s'orientent dans le bon sens ? Avez-vous des remarques ou des points d'alerte à nous communiquer sur ces projets qui n'ont pas encore fait l'objet du processus de trilogue ?

Pr Thibault Douville, professeur des universités, directeur du master Droit du numérique à l'Université Caen Normandie. La souveraineté numérique est un concept émergent en droit. Il ne fait pas l'objet, pour l'instant, d'une définition juridique. Comment la définir par référence au concept classique de souveraineté ? La souveraineté désigne le caractère suprême d'une puissance qui n'est soumise à aucune autre. Trois caractéristiques sont généralement mises en avant pour préciser sa définition. On s'attache tout d'abord au titulaire de celle-ci – qui est souverain ? On s'attache ensuite aux prérogatives mises en œuvre – quelle est la puissance souveraine ? On considère enfin la souveraineté comme une qualité constitutive de l'État : elle permet de distinguer l'État des autres organisations. Ce concept est donc étroitement dépendant d'une logique territoriale, qui pose difficulté dans l'environnement numérique.

Comment définir la souveraineté dans l'environnement numérique ? La souveraineté comme expression d'une puissance souveraine – c'est-à-dire la possibilité d'adopter des normes et de les faire appliquer dans l'environnement numérique – est un aspect admis de la souveraineté. De ce point de vue, l'État exerce une souveraineté sur l'espace numérique par les dispositions qu'il adopte, sous réserve des difficultés liées à la compétence territoriale.

La souveraineté numérique est, dans l'ordre externe, la capacité de l'État à demeurer indépendant. Ce deuxième aspect de la souveraineté numérique complète le premier : il existe, d'une part, l'aptitude à émettre des normes dans l'environnement numérique, et, d'autre part, son autonomie stratégique dans l'environnement numérique.

À mon sens, ces deux aspects permettent de définir la souveraineté numérique : elle recouvre un aspect normatif et un aspect lié à l'autonomie stratégique – économique, juridique et technologique. Ces deux aspects rejoignent, d'une certaine manière, la distinction classique entre la souveraineté interne et la souveraineté externe.

Le terme de souveraineté numérique n'est généralement pas admis en droit, pour une raison assez simple : Internet repose sur une logique initialement libertarienne. Ce réseau pourrait donc se passer d'État. Cette approche trouve son fondement dans la déclaration d'indépendance du cyberespace de 1996. Elle est aujourd'hui remise en cause par les acteurs d'Internet, puisque nous assistons à un mouvement de privatisation de ce réseau. L'émergence d'acteurs importants comme les géants du web américains – Google, Apple, Facebook, Amazon et Microsoft (GAFAM) – et chinois – Baidu, Alibaba, Tencent, Xiaomi (BATX) – met en exergue l'idée selon laquelle les États deviennent des colonies numériques. Il est vrai que la souveraineté réelle de l'État interroge, dès lors que des acteurs maîtrisent des données, émettent une monnaie, contrôlent les paiements, maîtrisent les places de marché, contrôlent la liberté d'expression en ligne et proposent des solutions d'identité numérique. Les différents modes d'expression de l'État sont ainsi petit à petit « mangés » par ces acteurs.

Il existe une production législative très importante pour encadrer le numérique, depuis une dizaine d'années, à l'initiative de l'Union européenne. Nous faisons face à un empilement très important de textes qui apportent des dispositions en matière de services de confiance, de protection des données personnelles et non personnelles, de protection des équilibres économiques. Nous assistons à une densification normative pour encadrer le numérique. Je ne suis pas persuadé que les réponses à ces enjeux soient nécessairement toujours juridiques. Il y a, à mon sens, un vrai problème de politiques publiques en matière de souveraineté numérique.

J'en veux pour exemple l'identité numérique, qui traduit l'aptitude des États à exercer leur souveraineté numérique. Elle constitue une clé pour transformer les services publics et pour développer la confiance dans les services en ligne. Du point de vue de l'État, ce service se développe très lentement avec France Connect Plus, qui n'est pas encore notifié à la

Commission et qui n'est pas encore interopérable – alors même que des acteurs privés prétendent proposer des solutions en la matière, comme Facebook avec ID Connect. L'État a pourtant naturellement vocation à proposer une solution d'identification électronique à ses citoyens, et ainsi favoriser l'émergence d'un socle de confiance en ligne et réaffirmer sa place dans l'environnement numérique.

La souveraineté numérique s'exprime au-delà du droit par des moyens suffisants, comme les effectifs de la Commission nationale de l'informatique et des libertés (CNIL) ou de la Plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS). Il existe une vraie question d'investissement humain et technique, ainsi qu'une nécessité d'investissement dans la recherche de technologies innovantes. Cela constitue de vraies difficultés pour les États, qui doivent investir suffisamment dans l'innovation pour conserver une longueur d'avance par rapport aux acteurs privés.

L'arrêt *Schrems* II est un arrêt fondamental en droit des données à caractère personnel. Cet arrêt était inattendu du point de vue de sa solution, car le contentieux qui a amené à l'arrêt *Schrems* II ne portait pas sur la validité de la décision d'adéquation *Privacy Shield*, mais sur le recours à des clauses contractuelles-types par Facebook pour transférer des données aux États-Unis.

Le contentieux ayant donné lieu aux arrêts *Schrems* I et II est assez ancien. L'autorité irlandaise de protection des données, amenée à se prononcer, a formulé, par deux fois, des questions préjudicielles qui ont conduit la Cour de justice à rendre un arrêt. Dans le cas de *Schrems* II, à l'occasion de l'appréciation de la validité des clauses contractuelles-types pour le transfert des données, la Cour de justice a jugé nécessaire de se prononcer sur la décision d'adéquation du *Privacy Shield*. Pour qu'un transfert de données à caractère personnel puisse avoir lieu d'Europe vers un pays tiers ou vers une organisation internationale, il faut s'appuyer sur une base juridique (comme une décision d'adéquation) permettant d'obtenir des garanties équivalentes à ce qui existe en droit de l'Union pour la protection des données, ou à défaut, sur des mécanismes beaucoup plus simples comme le consentement à un traitement de données pour des transferts ponctuels.

Dans l'arrêt *Schrems*, la Cour de justice a été amenée à apprécier la validité de la décision d'adéquation sur le point de savoir si les États-Unis présentaient ou non un niveau de protection des données équivalent à celui offert par le droit de l'Union. Elle a estimé que les États-Unis n'offraient pas cette protection équivalente. Elle s'est appuyée sur la protection du droit au respect de la vie privée garanti par l'article 7 de la Charte des droits fondamentaux, la protection du droit au respect des données à caractère personnel et son régime exprimé à l'article 8 de la Charte des droits fondamentaux et enfin, sur l'article 47 de la Charte des droits fondamentaux qui consacre le droit à un recours juridictionnel au titre des droits protégés par cette Charte.

Partant, la Cour de justice a été amenée à mettre en œuvre le contrôle habituel de proportionnalité. Elle s'est intéressée au but poursuivi par la législation américaine, à la nécessité de ce but et à la proportionnalité dans l'atteinte portée aux droits garantis par la Charte. À l'issue de cette analyse, la Cour de justice a estimé que la protection des données aux États-Unis ne présentait pas un niveau de garantie suffisant, car les personnes concernées ne bénéficient ni de droits effectifs et opposables, ni d'un droit à un recours juridictionnel. Elle a également jugé que le médiateur mis en place par les États-Unis, en tant qu'autorité chargée de protéger les données à caractère personnel des citoyens européens, ne présentait pas de garantie d'indépendance et ne disposait pas d'un pouvoir permettant d'adopter des dispositions contraignantes en matière de protection des données.

Par ce raisonnement, la Cour de justice a donné des indications importantes sur la manière d'apprécier le niveau de garantie équivalent présenté par une législation étrangère. Cela est important, car ce critère permet d'apprécier la validité d'une décision d'adéquation ou le caractère adéquat du recours à des garanties complémentaires, en l'absence d'une décision d'adéquation, comme des clauses contractuelles types ou des règles d'entreprise contraignantes. En rendant cet arrêt *Schrems*, la Cour de justice a donc donné la méthode : elle a précisé le niveau de protection des données requis en droit de l'Union, et donc requis d'un État tiers pour qu'une décision d'adéquation soit adoptée ou pour que des garanties appropriées soit adoptées pour compenser la différence de niveau de protection.

Pour les États-Unis, le recours à des clauses contractuelles-types ne permet pas de compenser la différence de niveau de protection, car celles-ci ne sont pas opposables à l'État américain et elles ne permettent pas, en elles-mêmes, d'accorder un recours juridictionnel aux citoyens européens, ni d'instituer une autorité de contrôle indépendante. En conséquence de cette décision, le transfert de données à caractère personnel vers les États-Unis est impossible. La législation américaine qui prévoit le contrôle et le stockage généralisé des données à caractère personnel transitant par les États-Unis rend difficilement possible l'adoption d'une nouvelle décision d'adéquation ou le recours à d'autres garanties appropriées. Le transfert des données vers les États-Unis est donc aujourd'hui prohibé. Le fait de procéder à un transfert de données entraîne une non-conformité au droit de l'Union, ce qui, en France, constitue une infraction pénale.

Cela cause un cataclysme dans les activités économiques. 65% de l'offre *cloud* est offerte par Amazon, dont une partie des serveurs se situe aux États-Unis. Dans le cas du Health Data Hub, Microsoft stocke des données en Europe, mais on sait que des opérations sur les données sont, pour partie, conduites grâce à un transfert temporaire *via* des serveurs américains. Ces situations causent potentiellement une non-conformité au droit de l'Union à la suite de l'arrêt *Schrems* II.

M. Philippe Latombe, rapporteur. Quelles sont les conséquences de cet arrêt pour les structures des entreprises ou des administrations qui utilisent des *clouds* américains ? Pour le Health Data Hub, le Conseil d'État a accordé à l'État un délai complémentaire au motif que les clés de chiffrement sont propriété de l'organisation qui collecte les données, qui est de droit européen. Il a été par ailleurs exigé, par contrat, que les données soient hébergées dans des serveurs en Europe. Est-ce suffisant aujourd'hui ?

Pr Thibault Douville. La conséquence de principe de cet arrêt est que la décision d'adéquation ne peut plus servir de fondement juridique pour le transfert de données à caractère personnel. Nécessairement, un autre fondement juridique doit être retenu pour procéder à ce transfert. Puisque la décision d'adéquation est invalidée, des fondements juridiques doivent présenter des garanties appropriées permettant de compenser la différence de niveau de protection. Il est ainsi admis qu'un transfert peut intervenir vers un pays tiers dans l'hypothèse où des mesures complémentaires sont adoptées. Le chiffrement des données constitue un exemple de mesure complémentaire pouvant être adoptée pour assurer une protection des données à caractère personnel de niveau équivalent. D'autres moyens existent, comme une pseudonymisation ou à une anonymisation des données. Si des mesures complémentaires peuvent être adoptées pour compenser la différence de niveau de protection, encore faut-il que ces mesures soient effectives. Le chiffrement des données est un moyen intéressant pour lever l'obstacle au transfert des données.

M. Philippe Latombe, rapporteur. Lors d'une précédente audition, IBM nous a expliqué ne pas être soumis au *Cloud Act* et n'avoir aucun problème d'extraterritorialité : IBM France est une filiale d'IBM Corporation, mais il s'agit d'une société de droit français qui

n'est, à ce titre, pas soumise aux règles extraterritoriales américaines. Le fait, pour une société de droit européen, d'entretenir un lien capitalistique majoritaire avec une société américaine assujettit-il la société à la réglementation américaine ? Si tel n'était pas le cas, le fait d'utiliser des algorithmes ou des solutions informatiques propriétés de la maison-mère aux États-Unis, assujettit-il la société à la réglementation américaine ?

Pr Thibault Douville. Je ne suis absolument pas spécialiste du *Cloud Act*, et par conséquent je me permettrais de ne pas répondre à votre question. Je procèderai à une vérification et vous apporterai une réponse écrite par la suite.

S'agissant de l'utilisation des moyens, toute la difficulté est de savoir comment ces moyens sont utilisés. Si des moyens de traitement de données sont utilisés dans le *cloud* et que ceux-ci supposent un transfert de données vers des serveurs hébergés aux États-Unis, la question se pose à la fois du transfert des données à caractère personnel vers un pays tiers et de l'application du *Cloud Act.*

Dans l'hypothèse du traitement des données dans le *cloud*, la question du maintien des mesures complémentaires, par exemple du déchiffrement des données, peut se poser. À cette occasion, la non-conformité au Règlement général sur la protection des données (RGPD) peut réapparaître, puisque les mesures complémentaires de protection des données seront levées pour un temps déterminé.

M. Philippe Latombe, rapporteur. La CJUE connaît une actualité forte sur ces sujets. L'arrêt *Prokuratuur* fait suite aux arrêts *Tele2* et *La quadrature du Net* suite à une question préjudicielle du Conseil d'État sur le stockage des métadonnées. Quels sont les impacts de ces arrêts sur le droit français ?

Pr Thibault Douville. Cette dynamique jurisprudentielle trouve son origine dans la directive européenne de mars 2006 sur la conservation des données de communications électroniques. Cette directive est intéressante car elle prévoit la conservation généralisée d'un certain nombre de données liées aux communications électroniques, qu'il s'agisse de données d'identification des utilisateurs ou de métadonnées. C'est ce qui est en cause dans la législation interne, notamment les dispositions du code des postes et des télécommunications électroniques et du code de la sécurité intérieure.

La Cour de justice a invalidé la décision de 2006 dans son arrêt *Digital rights* en affirmant l'interdiction du stockage et de la conservation généralisée de l'ensemble des données de connexion. Ce stockage et cette conservation sont, selon la Cour, disproportionnés par rapport aux buts poursuivis. Dès 2014, la Cour de justice mettait en avant l'ingérence dans le droit au respect de la vie privée et le non-respect des données à caractère personnel. Elle mettait en avant l'idée selon laquelle le texte n'opérait aucune différenciation entre les différents objectifs poursuivis par le législateur : la conservation des données était déconnectée du but poursuivi, soit de prévention d'atteinte à la sécurité publique ou de lutte contre la criminalité grave.

Postérieurement à l'invalidation de cette décision de 2006, la Cour de justice s'est à nouveau prononcée sur la question, cette fois au sujet de dispositions nationales par l'arrêt *Tele2* puis par l'arrêt *La quadrature du Net*, en reprenant des solutions similaires et en apportant des précisions quant à ces arrêts antérieurs. Elle mettait notamment en avant une échelle de mesures pouvant être adoptées selon le but poursuivi : lutte contre le terrorisme, lutte contre la criminalité grave ou protection de la sécurité publique. En fonction du but poursuivi, les mesures de conservation des données varient : elles peuvent être des mesures de conservation généralisée mais temporaire, des mesures de conservation ciblée et temporaire,

des mesures de conservation uniquement des données d'identification des utilisateurs. Les solutions apportées par les différents arrêts ne sont qu'une application de l'exigence de proportionnalité entre la protection des données, d'une part, et le but poursuivi, d'autre part.

En l'état, les dispositions internes sont remises en cause et supposent une réécriture. Cette réécriture ne me semble pas impossible : elle suppose de tenir compte du but poursuivi, qui varie en fonction de la gravité de l'infraction en cause.

Le récent arrêt *Prokuratuur* possède tout de même une spécificité. La Cour de justice se prononçait cette fois sur l'hypothèse dans laquelle des infractions peu graves auraient été commises – il s'agissait de vols pour des montants relativement réduits. Pour identifier l'auteur de ces vols, une juridiction estonienne avait permis la collecte et la conservation de l'ensemble des données concernant l'auteur des vols. La Cour de justice a considéré que la conservation généralisée des données de l'utilisateur permettait de dresser un profil de la vie privée de l'individu et était, là encore, disproportionnée par rapport au but poursuivi. La Cour de justice rappelle donc sa jurisprudence antérieure et la nécessité de cantonner les mesures de collecte et de conservation des données à la criminalité grave et à des menaces graves contre la sécurité publique. Cela n'interdit pas forcément l'ensemble des mesures de collecte ou de conservation des données, dès lors qu'elles sont ciblées et qu'elles ne permettent pas de dresser un portrait de la vie privée de l'individu. La portée donnée à la solution de cet arrêt est peut-être excessive : la Cour de justice n'interdit pas des mesures ciblées de conservation ou d'accès aux données mais la communication de données doit être limitée dans son étendue temporelle et matérielle.

Ces arrêts, depuis *Tele2* jusqu'au récent arrêt de mars 2021, viennent mettre en œuvre l'exigence de proportionnalité. Le législateur n'est pas interdit de mettre en place des mesures de conservation de données, mais ces mesures doivent être proportionnées par rapport au but poursuivi. Dès lors, il est étonnant que le législateur interne n'ait pas mis en œuvre l'exigence de proportionnalité en droit interne dès l'arrêt *Tele2*. Il aurait pu prévoir, par exemple, de rendre possible la conservation de l'ensemble des données d'identité des utilisateurs, de limiter la conservation de l'activité de l'utilisateur à certaines circonstances de lutte contre la criminalité grave et d'instituer un régime à paliers, selon la gravité des infractions ou du but de prévention.

M. Philippe Latombe, rapporteur. Au-delà des données personnelles, l'arrêt *Prokuratuur* questionne-t-il l'indépendance de la procédure ? L'arrêt de la Cour de justice indique que le ministère public ne présentait pas les garanties d'indépendance nécessaires pour demander la communication de ces informations. Est-ce un élément nouveau dont il faut tirer des conséquences ?

Pr Thibault Douville. Oui, cela est un élément nouveau. La Cour de justice ne s'était pas prononcée sur cet aspect dans les arrêts précédents. Sur le fondement de l'article 15 de la directive 2002-58, la Cour de justice s'oppose à une réglementation nationale donnant compétence au ministère public pour autoriser l'accès d'une autorité publique aux données relatives au trafic et aux données de localisation aux fins d'une instruction pénale. Elle pose l'exigence de l'intervention d'un juge indépendant pour autoriser l'accès aux données, le ministère public ne remplissant pas, dans le cas estonien, les conditions suffisantes d'indépendance. Cela est certainement également applicable au droit français : je pourrais imaginer que l'on confie la mission d'autoriser l'accès aux données au juge des libertés et de la détention, en raison de l'atteinte aux droits et libertés que cet accès va entraîner.

M. Philippe Latombe, rapporteur. Cela veut-il dire que cette décision serait également applicable au juge d'instruction en France ?

Pr Thibault Douville. Oui. Deux aspects ressortent de l'arrêt : la Cour de justice distingue bien, d'une part, l'autorité de poursuite et, d'autre part, la mission d'instruction. Ni l'un ni l'autre ne pourrait se voir confier cette prérogative, qui serait laissée à un tiers. Ce tiers pourrait être le juge des libertés et de la détention en France, qui présente les garanties d'indépendance requises pour adopter une mesure attentatoire au droit au respect de la vie privée ainsi qu'à la liberté d'expression, puisque les données recueillies au titre de la criminalité grave permettent de dresser un profil complet de la personne concernée.

M. Philippe Latombe, rapporteur. Quel impact peut avoir cet arrêt sur nos procédures en cours ? Le Conseil d'État a saisi la CJUE d'une question préjudicielle. Dans un mémoire, le gouvernement a fait état d'une inapplicabilité de la décision de la CJUE pour des raisons constitutionnelles. Qu'en pensez-vous ?

À la lumière de ce nouvel arrêt, les procédures en cours seraient-elles susceptibles d'être remises en cause ? Quelles mesures correctives faut-il donc prendre ?

Pr Thibault Douville. Je répondrai d'abord à l'argument de l'identité constitutionnelle de la France comme moyen d'échapper à cette jurisprudence et plus largement au régime applicable à la protection de la vie privée dans le cadre des communications électroniques. L'identité constitutionnelle de la France est une notion assez récente, découverte par le Conseil constitutionnel au début des années 2000. À l'occasion de la transposition en droit interne d'une directive communautaire, le Conseil constitutionnel a estimé, par une décision en date du 27 juillet 2006, que s'il n'appartenait qu'au juge communautaire de contrôler le respect de cette directive et des compétences définies par les traités, il a précisé que la directive pourrait faire l'objet d'un contrôle dans l'hypothèse où elle irait à l'encontre d'une règle ou d'un principe inhérent à l'identité constitutionnelle de la France. Plus tôt, dans une décision du 10 juin 2004, le Conseil constitutionnel avait évoqué l'idée de l'identité nationale inhérente aux structures fondamentales et politiques constitutionnelles de la France.

Cette notion pose un problème de définition. Nous avons bien du mal à identifier le contenu de l'identité constitutionnelle de la France : la langue, l'unicité du peuple, la laïcité peuvent naturellement en faire partie. La procédure pénale et la conservation des données à fins de prévention des infractions ou de lutte contre la criminalité relèvent-elles de l'identité constitutionnelle ? Doit-on considérer que l'exercice de la souveraineté pour garantir la sûreté publique est rattaché à l'identité constitutionnelle de la France ?

À mon sens, cela n'est pas le cas, pour deux raisons au moins. Tout d'abord, les dispositions relatives à la protection des données de communications électroniques font l'objet d'une européanisation depuis bientôt vingt ans. L'État français applique cette législation, sans avoir jusqu'à présent invoqué l'identité constitutionnelle de la France. Ensuite, du point de vue du droit de l'Union européenne, l'invocation de l'identité constitutionnelle de la France permettrait d'échapper à l'application du droit de l'Union. Cet élément pose question. Un certain nombre de matières ne relèvent pas du champ du droit de l'Union, comme par exemple la défense nationale. La lutte contre les infractions ou la criminalité, en revanche, fait l'objet d'une européanisation. J'ai du mal à imaginer, dans ce contexte, en quoi les dispositions internes en matière de procédure pénale et de conservation des données présentent une spécificité française. Enfin, la France sert de modèle et invoquer l'identité constitutionnelle nationale pour échapper à l'application de ces dispositions conduirait d'autres États à tirer parti de l'argument.

Je note un point important : pourquoi le droit de l'Union européenne et le RGPD ont-ils vocation à s'appliquer ? Le droit de l'Union s'applique car sont visées, à chaque fois, des exigences de conservation de données qui s'imposent aux acteurs des traitements de données.

C'est dans ce contexte que la Cour de justice a été amenée à se prononcer. J'ai du mal à concevoir que la législation interne pourrait être considérée comme distinctive par rapport au droit des autres États ou au droit de l'Union, et permettrait de justifier une forme d'exemption. Le Conseil constitutionnel n'a par ailleurs pas donné de définition générale de la notion d'identité constitutionnelle de la France, ce qui laisse la question en suspens.

Je répondrai maintenant à votre question sur les changements induits par cet arrêt en ce qui concerne la procédure pénale. L'arrêt *Prokoratuur* a une incidence en droit pénal interne, notamment du point de vue des actes d'instruction ou bien des actes d'enquête hors instruction. Pour l'instant, le juge des libertés et de la détention n'a pas vocation à autoriser la conservation ou l'accès aux données : un travail de réécriture serait donc à opérer de ce point de vue.

M. Philippe Latombe, rapporteur. Quelles seraient les conséquences d'une éventuelle acceptation par le Conseil d'État de l'argument de l'identité constitutionnelle de la France pour écarter le droit de l'Union ? Un de vos collègues professeur de droit a évoqué le risque de « balkanisation » du droit européen. Est-ce le vrai risque ?

Pr Thibault Douville. Il est évident qu'il existe un risque de balkanisation : suivre une telle approche peut conduire les autres États à adopter le même argument pour s'écarter du droit de l'Union, avec des champs d'application qui peuvent être variables. Pourquoi ne pas répliquer l'argument dans d'autres domaines ?

Il existe également un risque de conflit entre les juges. La Cour de justice pourrait tout à fait être amenée à se prononcer sur la position du Conseil d'État et à considérer que le droit de l'Union a vocation à s'appliquer à ces dispositions concernant la conservation et l'accès aux données de connexion. Cela créerait un problème de conciliation des positions entre l'ordre interne et l'ordre communautaire. Le fait d'évoquer l'argument de l'identité constitutionnelle de la France en la matière est absolument inédit.

Le sujet pourrait également être traité à l'occasion de la révision de la directive qui constitue le futur Règlement *e-privacy*. Il serait possible d'introduire directement dans le Règlement *e-privacy* un certain nombre de dispositions prévoyant la conservation de données de connexion à certaines conditions et dans certains buts de prévention du terrorisme ou de lutte contre la criminalité grave, ce qui permettrait de donner un socle européen à ces dispositions. La Cour de justice pourrait tout à fait être amenée à contrôler la validité de ce texte à l'aune de la Charte des droits fondamentaux et il ne faudrait donc pas que ce texte présente de disproportion. L'exigence de proportionnalité conduit à raisonner en escalier : plus l'on descend des marches de gravité, moins les données qui peuvent être conservées sont importantes.

M. Philippe Latombe, rapporteur. Cela nous permet d'échanger sur les trois projets de directives en cours. Selon vous, ces directives sont-elles bien calibrées et atteignent-elles leur but ?

Pr Thibault Douville. La proposition de règlement *DSA*, qui constitue une réforme de la directive sur le commerce électronique et le statut des intermédiaires techniques, est très intéressante. Tout en maintenant l'acquis communautaire en matière d'intermédiaires techniques (c'est-à-dire le principe d'irresponsabilité pour les hébergeurs et les fournisseurs d'accès à Internet), la proposition pose un cadre juridique, à plusieurs niveaux, en ce qui concerne la modération du contenu. Le texte s'applique aux prestataires de services intermédiaires, puis aux prestataires de services intermédiaires ayant la qualité de plateforme

en ligne, puis aux grandes plateformes en ligne, avec des obligations différentes pour chaque sous-qualification.

Le *DSA* propose d'instituer un régime de modération des contenus par les plateformes en ligne. Son apport est très intéressant puisqu'il vise, à la fois, à lutter contre certains contenus illégaux ou illicites par rapport aux conditions générales d'utilisation des services et à garantir la liberté d'expression. Nous savons que l'équilibre est difficile à trouver. Le *DSA* propose un mécanisme intéressant, alliant des exigences concernant les notifications et les instructions de communication de données par les autorités compétentes, d'une part, et des mécanismes de recours interne, de règlement des différends, d'évaluation des risques systémiques présentés par les grandes plateformes en ligne quant à la liberté d'expression, d'autre part.

Certains aspects de ce mécanisme peuvent néanmoins poser difficulté. Le premier aspect problématique est politique : la régulation des contenus va d'abord peser sur des acteurs privés, la modération relèvant des plateformes. L'institution d'une autorité de contrôle indépendante – le Conseil supérieur de l'audiovisuel (CSA) pour la France – est une proposition intéressante, mais elle s'inscrit dans une logique de régulation.

Un point technique peut par ailleurs être bloquant : le recours à des traitements automatisés pour procéder à la modération des contenus. Le *DSA* prévoit une exigence de transparence. La question de la transparence algorithmique soulève une vraie difficulté. Ne faudrait-il pas mettre en place des tests plus poussés des algorithmes dans des situations déterminées, ou par rapport à des types de propos déterminés ? On avance souvent l'idée d'une forme d'analyse d'impact algorithmique, mais il n'est pas certain que cela soit suffisant.

L'internalisation du mécanisme de recours est intéressante – il s'agit d'un mécanisme de règlement interne des différends dans l'hypothèse de suppressions de comptes ou de contenus. Là encore, le règlement interne a vocation à être indépendant, mais relève de la sphère privée. Nous assistons à une forme de marginalisation du juge dans le cas des atteintes à la liberté d'expression et cela peut poser problème. Il est, de plus, proposé de mettre en place un mécanisme de règlement extra-judiciaire des différends, en cas d'insatisfaction quant à la décision de règlement interne adopté. Cet empilement de mécanismes n'est pas forcément satisfaisant et risque d'être très long. Il peut être intéressant de maintenir une procédure judiciaire rapide pour qu'une juridiction se prononce sur un conflit lié à l'absence de modération d'un propos ou à la suppression d'un propos. La marginalisation du juge me surprend, avec la désignation du CSA comme autorité de contrôle. Le recours contre une décision du CSA relève du Conseil d'État et non du juge judiciaire, garant des libertés individuelles. En tant que juriste privatiste, cette décision m'interroge.

Le projet de loi renforçant le respect des principes de la République va à mon sens dans le bon sens, proposant une forme d'introduction anticipée du *DSA* : il permettra d'expérimenter par avance le système du *DSA* et de bénéficier d'un retour d'expérience qui pourra être intéressant lors des négociations sur le texte.

M. Philippe Latombe, rapporteur. Dans les futures négociations, les pays européens sont-ils d'accord sur les contenus qui seront soumis à cette réglementation ? Les pays européens ont-ils la même interprétation de ce qu'est la liberté d'expression ?

Pr Thibault Douville. C'est en effet une question centrale. Nous le voyons déjà en matière de droit au déréférencement et de droit à la protection des données personnelles. Les conceptions de la liberté d'expression varient. Les plateformes en ligne ont une interprétation autonome et globale de la liberté d'expression, qui répond à des critères différents des nôtres. Il n'est pas prévu que le *DSA* définisse une liste des propos illégaux. Au regard de l'état de

son droit, chaque État membre va être amené à définir le caractère illicite de certains propos. Nous faisons donc face à un risque d'éclatement ou de fragmentation de la manière dont sera apprécié le caractère illicite de certains propos. Avec un mécanisme comme le *DSA* instituant la compétence du prestataire en la matière, il y a un risque que l'appréciation des propos varie en fonction des opérateurs.

M. Philippe Latombe, rapporteur. Le RGPD a mis en place un fonctionnement dans lequel toutes les autorités de contrôle nationales de type CNIL travaillent ensemble sous la direction d'un chef de file. Le *DSA*, lui, ne prévoit pas de tel mécanisme. Chaque pays conduira donc sa propre interprétation ?

Pr Thibault Douville. On peut imaginer une coopération entre les autorités de contrôle – cela est dans la logique de l'instrument. Mais effectivement, le texte ne prévoit pas de mécanisme instituant une autorité de contrôle chef de file avec un mécanisme de règlement des conflits entre autorités (dans le RGPD, ce rôle est confié au Comité européen). Il y a donc un vrai risque de fragmentation de la manière dont la liberté d'expression est appréciée dans l'Union européenne, ainsi qu'un risque de définition variable des contenus illicites, au sens des conditions générales d'utilisation des acteurs.

En revanche, il ne faut pas oublier que la Charte des droits fondamentaux promeut la liberté d'expression et garantit la protection de la vie privée et des données à caractère personnel. Les autorités nationales s'inspireront naturellement tant de la jurisprudence de la Cour de justice que de celle de la Cour européenne des droits de l'Homme. Cet acquis apportera quelques garanties dans la mise en œuvre de ces mécanismes.

M. Philippe Latombe, rapporteur. Les conditions générales d'utilisateurs ne sont pas spécifiquement visées dans le *DSA*. Ne devrions-nous pas récupérer de la souveraineté sur ce sujet ? Il s'agit de réglementations privées s'appliquant à l'ensemble des utilisateurs. Les États n'ont-ils pas le devoir de s'y intéresser et de les réguler ?

Pr Thibault Douville. Le *DSA* ne prévoit en effet pas l'encadrement des conditions générales d'utilisation, au-delà d'une exigence de transparence et de la nécessité de préserver la liberté d'expression – cela demeure très vague.

À titre individuel, les utilisateurs pourront toujours se prévaloir d'une atteinte à leur liberté d'expression résultant de l'application des conditions générales d'utilisation. On peut imaginer que certaines conditions générales d'utilisation prohibant certains propos soient contraires à la liberté d'expression : la clause pourrait alors être déclarée illicite car contraire à l'ordre public, et frappée de nullité partielle.

À titre plus général, est-il possible d'imaginer un mécanisme de contrôle des conditions générales d'utilisation ? On pourrait dresser un parallèle avec le mécanisme de contrôle des clauses abusives en droit de la consommation. Il pourrait être intéressant d'intégrer dans le *DSA* un mécanisme similaire de contrôle visant à encadrer ou à limiter la liberté d'expression sur les plateformes, afin de déterminer les frontières du licite et de l'illicite dans ces clauses. Cela est tout à fait imaginable. En la matière, le mécanisme de contrôle des clauses abusives est un bon exemple qu'il serait possible de dupliquer.

Le *DGA* constitue une proposition très intéressante qui vise à faciliter le partage des données. Le texte considère que les données constituent une infrastructure qu'il est possible et souhaitable de mobiliser pour différents usages et en vue de différentes finalités. Le *DGA* propose donc la mise en place de services de partage des données à travers les *data hubs*. La difficulté de ces plateformes est la confiance des utilisateurs, aussi bien ceux détenant les

données que ceux qui pourraient les réutiliser, à la fois, quant aux jeux de données et à la protection du secret et aux finalités de la réutilisation. L'instrument européen cherche à répondre à cet enjeu de confiance. Il promeut certains services nouveaux, comme la mise à disposition de données à caractère personnel en faveur de réutilisateurs ou la mise en place de services de coopératives de données.

Au-delà de son affirmation de principe, très intéressante, beaucoup de questions se posent. Le partage des données demeure facultatif et volontaire. La question de la qualité des données partagées se pose : nous avons besoin d'un référentiel en matière de fraîcheur, de format, de contenu et des finalités de réutilisation des données. Les *data hubs* mis en place ne sont pas toujours une réussite : il demeure un écart entre l'affirmation politique et économique de la création d'un *data hub* et les réutilisations effectives de données. Il n'est pas certain, pour l'heure, que les *data hubs* aient trouvé leur public.

Je relève un constat final intéressant : les acteurs concurrents de l'État (les GAFAM et les BATX) collectent des données et les conservent pour améliorer leurs services et dégager de nouvelles connaissances. L'état du droit de l'Union, en revanche, ne va pas dans le sens d'une affirmation du partage des données. Par exemple, le Règlement européen *Platform to business* de 2019 vise à rétablir l'équilibre entre plateformes et entreprises utilisatrices et pose une exigence de transparence, quant au partage de données, en faveur des utilisateurs. On peut donc se poser la question de savoir si la simple mise en place d'un cadre de confiance pour le partage des données est suffisante afin de tirer parti des données collectées. Il pourrait être important également de diffuser une culture de la donnée à destination des acteurs économiques et des citoyens, afin de favoriser l'utilisation des données et de développer des solutions techniques qui permettent leur valorisation – celles-ci ne sont pas forcément disponibles actuellement.

Le texte est donc intéressant pour le cadre de confiance apporté, mais je ne suis pas certain qu'il réussira à atteindre son objectif qui est de favoriser la mise en place d'une économie de la donnée.

M. Philippe Latombe, rapporteur. Le texte ne réussira pas à atteindre son objectif car vous pensez qu'il n'apporte pas assez de confiance ?

Pr Thibault Douville. Cela n'est pas forcément dû à la confiance. L'instrument du *data hub* est intéressant, mais ce qui pose difficulté est de savoir pourquoi des détenteurs de données les mettraient à disposition de réutilisateurs. Dans quel but le feraient-ils ? Pourquoi des personnes mettraient-elles à disposition leurs données à caractère personnel ? Dans quel but le feraient-elles ? Il n'est pas certain que l'offre corresponde à la demande. Imaginons par exemple qu'un industriel récolte des données à l'occasion de sa production et qu'il cherche à les mettre à disposition d'autres acteurs. Quels autres acteurs seraient intéressés ? Il se pose un problème de correspondance entre collecteurs de données, d'une part, et réutilisateurs de données, d'autre part.

S'agissant de l'économie de la donnée, la plupart des transferts de données à caractère onéreux interviennent, aujourd'hui, dans le cas d'activités commerciales publicitaires. Il y a un alignement des intérêts des collecteurs de données et des réutilisateurs en la matière. Du point de vue industriel, cela est plus difficilement le cas. Je ne sais pas si mettre en place des plateformes de confiance, mettant en relation des collecteurs et des réutilisateurs, est la solution pour faciliter la réutilisation des données. Au-delà de l'instrument, se pose la question du marché : il existe un problème de marché et de circuit de la donnée.

M. Philippe Latombe, rapporteur. Quels sont les sujets juridiques auxquels nous devrions nous intéresser maintenant au regard des nouvelles technologies émergentes ? Je pense notamment à l'intelligence artificielle ou au quantique. En ce qui concerne l'intelligence artificielle, par exemple, des questions se posent sur la propriété intellectuelle d'algorithmes produits par l'intelligence artificielle. Devons-nous dès maintenant créer un cadre, ou devrons-nous nous adapter au fur et à mesure des avancées technologiques ?

Pr Thibault Douville. C'est une question fondamentale. Je me permettrai, pour débuter, un parallèle avec la *blockchain*. Il y a eu, en matière de *blockchain*, une volonté politique très forte de consacrer un cadre juridique, afin de favoriser l'émergence de la *blockchain* et de servir de modèle à l'échelle de l'Union européenne. Aujourd'hui, on se rend compte que le cadre mis en place a favorisé des initiatives, qui sont bloquées pour des raisons réglementaires, notamment de certifications. Nous avons assisté à un mouvement de mobilisation des énergies pour s'emparer de ces outils, et, aujourd'hui, un ralentissement en raison de contraintes réglementaires.

Le fait d'adopter des normes permet-il vraiment de faire émerger des initiatives et de prendre de l'avance ? Cela est vraiment discutable. Nous pouvons partir du principe que le premier cadre défini permet de servir de modèle, d'asseoir la confiance des utilisateurs et de favoriser l'investissement – cela est vrai : cela a été le cas pour l'utilisation de la *blockchain* en matière financière. Inversement, la mise en place d'un cadre juridique est un frein pour des acteurs qui sont encore à la recherche de solutions techniques.

L'intelligence artificielle reste, pour l'heure, des algorithmes sous maîtrise humaine. La question des créations peut trouver une réponse sur le fondement du droit actuel de la propriété intellectuelle ou par d'autres mécanismes contractuels. Je ne sais donc pas si la mise en place d'un cadre juridique est le meilleur moyen d'encourager les initiatives en la matière. Il demeure cependant des questions importantes sur lesquelles le législateur pourrait se pencher, comme la mise en place d'un cadre pour l'audit des algorithmes ou la transparence des algorithmes. Cette question très intéressante n'est pas réglée et mériterait de l'être. S'il s'agit d'adopter un texte pour mettre en place des règles très générales sur l'intelligence artificielle, la question de la pertinence de ce cadre se pose.

En matière de souveraineté juridique, une question actuelle pose difficulté : il s'agit de l'identité numérique. Je ne comprends pas que nous ne disposions pas de moyens d'identification électronique, que l'État ne se réapproprie pas l'identité électronique, que l'identité numérique ne soit pas ouverte aux fournisseurs de services afin de favoriser son adoption, que l'on ne se saisisse pas de ce moyen pour opérer une transformation de l'État et des services publics permettant le déploiement de services de confiance, comme la signature électronique qualifiée, l'horodatage qualifié, la lettre recommandée électronique qualifiée – sous réserve évidemment de la protection des personnes exclues du numérique.

Parmi les actions concrètes immédiates, l'identité numérique est à mes yeux une clé de la transformation numérique de l'État et de la souveraineté de l'État. L'État est le détenteur naturel de l'identité de tous ses concitoyens : il a le monopole de l'émission des titres d'identité. Ce sujet est au croisement des dispositions législatives, réglementaires et de l'investissement public. Le déploiement d'une identité numérique étatique permettrait d'opérer une transformation de l'État en mettant le citoyen au cœur de la transmission de ses données entre administrations. Ceci apporterait aux citoyens une plus grande confiance dans le déploiement du numérique et permettrait de développer de nouvelles technologies : le recours au *deep* pour les services financiers, par exemple. Ce sujet est urgent à mes yeux.

Votre mission d'information s'intéresse principalement aux usages et aux services. Il pourrait être intéressant, pour le législateur, de s'intéresser à l'infrastructure. Il s'agit de se demander si l'infrastructure numérique n'a pas vocation à relever, dans une certaine mesure, de services publics. Cela concerne l'hébergement de données – avec des garanties d'indépendance, par exemple – et les réseaux. L'ouvrage récemment publié par Thibault Verbiest et Jonathan J. Attia, « *Un nouvel Internet est-il possible ?* » raisonne sur la couche de l'infrastructure. Il propose d'intégrer à la norme des protocoles Internet TCP/IP de nouvelles fonctionnalités d'identification, de certification de contenus, de transferts de données, qui permettraient à l'État et au citoyen de retrouver une certaine maîtrise sur leurs usages. Cette approche a été peu développée jusqu'à présent. Les directives européennes s'attachent davantage à réguler les usages ou le marché.

M. Philippe Latombe, rapporteur. Notre mission d'information ouvrira une séquence pour traiter du sujet de l'identité numérique. Mme Christine Hennion et M.Jean-Michel Mis ont déjà remis un rapport à ce sujet. Leurs recommandations n'ont pas été mises en œuvre.

Pr Thibault Douville. Ce rapport formulait d'excellentes propositions. Nous disposons de France Connect Plus et une notification à la Commission devrait en principe intervenir cet été. La question est vraiment celle de l'ouverture du système à des fournisseurs de services privés pour permettre au citoyen de s'en emparer. Une vraie communication doit être faite à ce sujet.

M. Philippe Latombe, rapporteur. En ce qui concerne la *blockchain*, vous avez évoqué la partie financière et la volonté marquée dans la loi relative à la croissance et la transformation des entreprises, dite loi PACTE, d'avancer à ce sujet. La réglementation par décret a, par la suite, bloqué les intermédiaires financiers. Mais la *blockchain* permet aussi l'horodatage et l'inscription au registre. Certains pays sont très en avance et ont adopté des réglementations internes pour donner une force probante à la *blockchain*. Où en est la France et quelles mesures devons-nous adopter en urgence ?

Pr Thibault Douville. Un rapport et plusieurs propositions parlementaires sont intervenus à ce sujet. Votre collègue, M. Jean-Michel Mis, avait proposé, à l'occasion de la loi PACTE, d'introduire dans le code civil une disposition visant à donner une force probante aux enregistrements sur une *blockchain*.

Je formule à ce sujet plusieurs remarques. Le déploiement de la technologie de la *blockchain* demeure limité en dehors des cryptomonnaies ou des actifs numériques. Cela étonne, dès lors que la *blockchain* est connue et commence à être maîtrisée par tous. Du point de vue des usages, la *blockchain* pose la question de la conservation de l'information, de son intégrité et de sa datation. Elle ouvre la possibilité de la digitalisation de l'activité contractuelle par les *smart contracts*.

En ce qui concerne la force probante, la consécration d'une forme d'intégrité des données pourrait être intéressante. Le code civil permet d'ores et déjà d'utiliser une signature électronique avancée qui permet de garantir l'identité du signataire et de faire le lien entre la signature et l'acte. Il est possible à des prestataires de services de confiance de combiner leurs services avec des services de *blockchain* privés. La question de la consécration de la force probante sur des *blockchains* publiques se pose : elle pourrait être intéressante, au moins s'agissant d'une présomption quant à la datation de l'enregistrement et quant à l'intégrité de l'information, mais non une présomption quant à l'identité de celui ou celle ayant enregistré l'information – car cet élément ne peut pas faire l'objet d'un contrôle s'agissant d'une *blockchain* publique, sauf si un intermédiaire intervient pour délivrer des clés d'identification.

Il pourrait être intéressant de réfléchir à l'intégration d'un régime de *smart contracts*. L'autonomisation d'un certain nombre de contrats a vocation à intervenir, s'agissant des clauses contractuelles pouvant faire l'objet d'une mise en œuvre automatique, comme, par exemple, les conditions suspensives d'obtention d'un prêt. Le *smart contract* ne serait-il alors qu'une déclinaison de clauses contractuelles dans la *blockchain*, ou peut-on imaginer un contrat entièrement codé ? Cette seconde option poserait des questions de transparence, de compréhension par les parties et d'expression du consentement par les parties. Dans un premier temps, on pourrait imaginer la consécration de l'utilisation de *smart contracts*, c'est-à-dire d'exécution automatique de contrats sur une *blockchain*. Cela permettrait de lever un certain nombre d'incertitudes quant à l'inexécution éventuelle du contrat, mais pose, dans le même temps, des problèmes en ce qui concerne sa suspension éventuelle. Cela soulève beaucoup de questions qui mériteraient une vraie réflexion.

Le prochain congrès annuel des notaires aura pour thème l'homme, le numérique et le droit. Les notaires proposeront notamment un premier clausier de *smart contracts*, sur des opérations simples (conditions suspensives, terme d'un contrat, paiement d'une somme d'argent), qui ne requièrent pas d'information ou d'exécution extérieure de la part d'une personne. Cela pose une première brique de réflexion intéressante.

En France, en ce qui concerne les faits juridiques, un enregistrement sur une *blockchain* peut parfaitement être invoqué devant une juridiction, en vertu du principe de non-discrimination des documents électroniques instauré par le Règlement européen eIDAS. Une révision du Règlement eIDAS est envisagée, notamment pour y intégrer les *blockchains*. Jusqu'à présent, le Règlement eIDAS traite de l'identification électronique et des services de confiance, qu'il envisage de manière centralisée. Il est envisagé d'intégrer la *blockchain* dans ce Règlement : cela poserait davantage de questions pour les *blockchains* publiques que pour les *blockchains* privées.

En France, contrairement à la Belgique, nous n'avons pas profité de l'adaptation du droit français au Règlement eIDAS pour intégrer un statut des prestataires de confiance ou des tiers de confiance numériques. Il pourrait être intéressant de le faire. J'en veux pour exemple la consécration du coffre-fort numérique comme service de confiance en France. Le pouvoir réglementaire n'a pas indiqué qui peut proposer un service de coffre-fort numérique et quel est son statut. Il pourrait être intéressant de consacrer un régime général, peut-être dans le code de commerce, de l'activité de services de confiance en ligne. Cette activité pourrait être entendue soit de manière restrictive (c'est-à-dire tous les services de confiance au sens du Règlement eIDAS ou ajoutés par le législateur interne), ou bien plus largement : le tiers de confiance pourrait être celui qui propose des services de confiance ou la certification d'information par voie électronique. Cela peut être intéressant à l'occasion du déploiement des *blockchain* qui proposent des services de conservation d'actifs numériques, en rattachant les prestataires de services d'actifs numériques à cette catégorie des tiers de confiance.

Cela ferait apparaître un acteur qui bénéficierait d'un statut sur lequel le législateur pourrait s'appuyer pour de nouveaux usages à consacrer par la suite : des garanties financières de responsabilité, de respect des données à caractère personnel, de cybersécurité, qui seraient variables selon la qualité du tiers de confiance. On pourrait par exemple imaginer que les notaires puissent être tiers de confiance pour la certification et l'authentification d'information. On pourrait également imaginer que les prestataires de services qualifiés au sens d'eIDAS bénéficient de ce statut pour les services donnés. Cela permettrait d'agréger un certain nombre d'acteurs sous une qualification unique. Le législateur pourrait ensuite consacrer de nouveaux services de confiance se rattachant à cette catégorie de tiers de confiance bénéficiant d'un régime unitaire.

M. Philippe Latombe, rapporteur. Vous ne préconisez pas de créer une profession juridique réglementée spécialisée ? D'autres pays européens l'ont fait.

Pr Thibault Douville. Derrière la notion de « confiance en ligne » se cache une multitude de services possibles. Il existe les services de confiance au sens classique, c'est-à-dire au sens du règlement eIDAS. La Poste, dans le cadre de la délivrance de moyens d'identification électroniques, exerce, elle aussi, une activité de confiance. Ce service de confiance de vérification d'identité n'est pas consacré par le législateur – il est rattaché à un référentiel de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Pour permettre le déploiement des *smart contracts*, les notaires pourraient eux aussi exercer une activité d'authentification d'information en ligne. Il serait donc intéressant de disposer d'un statut unique de prestataire de services de confiance, dont les titulaires pourraient être habilités à proposer un service d'authentification de documents, aussi bien que de vérification d'identité. Cette catégorie a vocation à être adaptable en fonction du service de confiance proposé par les différents professionnels.

En consacrant la notion de prestataire de services de confiance ou de tiers de confiance, on pourrait associer à cette qualification un ensemble d'obligations communes de transparence, de responsabilité, de certification. Cette qualification bénéficierait de l'ensemble de l'acquis interne et européen, tout en permettant d'ouvrir de nouveaux usages par la suite. Un service de confiance d'authentification de documents est fondamental pour le déploiement des *blockchain* : il permettrait d'ajouter une présomption d'intégrité et de validité des informations enregistrées sur une chaîne de bloc. Nous avons besoin d'une catégorie.

M. Philippe Latombe, rapporteur. L'État travaille à sa numérisation et a besoin de plus en plus de données. Pour le contrôle fiscal par exemple, Bercy a souhaité pouvoir aspirer les données des réseaux sociaux. À l'occasion de l'examen du projet de loi sur la sécurité globale, la question du stockage des images filmées par les drones a également été débattue. Pensez-vous que l'État a aujourd'hui une suffisante culture de la donnée ?

Pr Thibault Douville. C'est une question difficile. Tout dépend des ministères et des services concernés. L'État mène une politique volontaire d'*open data* – c'est-à-dire d'ouverture des données – depuis bientôt vingt ans et cela commence à porter ses fruits. Un service public de la donnée a été créé et l'on constate aujourd'hui la mise à disposition d'un certain nombre de bases de données.

Votre question porte peut-être davantage sur les données que l'État collecte et traite dans ses activités. Ces données sont-elles valorisées et pourraient-elles l'être davantage ? Une récente initiative du ministère de la justice donne des clés de compréhension à ce sujet. Le décret DataJust de mars 2020 vise à mettre en place un traitement automatisé de données à caractère personnel. Un algorithme, établi à partir de décisions judiciaires, permet, par exemple, d'établir un barème d'indemnisations en matière de dommages corporels, de faire de la prospective et de l'analyse de moyens des juridictions, d'informer les justiciables concernant leurs droits et, potentiellement, l'indemnisation à laquelle ils peuvent prétendre. Cela favoriserait la mise en place de mécanismes de règlement extrajudiciaire des litiges. Cette initiative du ministère de la justice consiste à valoriser des données existantes, avec un objectif d'ordre à la fois opérationnel, prospectif, d'information et de pédagogie auprès des citoyens.

Ce modèle peut être dupliqué. La prospective et l'analyse de données peuvent, évidemment, être utiles à l'État – l'État le fait d'ailleurs déjà dans certains ministères et a vocation à le faire davantage. Cette initiative est également le moyen, pour l'État, de garder la main sur ses données et d'éviter que des acteurs privés ne s'en emparent. Les *legal tech*, par exemple, développent leurs activités sur des données judicaires : par son initiative, le ministère

de la justice propose un service étatique et garde ainsi la main sur ses données. L'utilisation et la valorisation des données sont également un moyen de favoriser la confiance. La crise du COVID a montré que l'ouverture des données sanitaires était un très bon moyen de donner aux citoyens une prise sur l'évolution de la situation sanitaire. Plusieurs cas de réutilisation de données ouvertes par l'État ont ainsi été salués.

Les moyens posent problème dans la valorisation de la donnée. Nous en sommes toujours là. Nous avons créé le Health Data Hub ; il aurait été possible de prévoir une modernisation et une uniformisation des systèmes d'information des hôpitaux pour permettre une valorisation des données stockées localement, mais la difficulté est l'éclatement des suites logicielles utilisées dans les différents services des hôpitaux. En matière judiciaire, la même difficulté se pose : l'absence de rénovation du parc informatique et l'absence de matériel suffisant et à jour bloquent le développement de nouveaux usages. La mise à disposition de l'*open data* des données en matière judiciaire est aujourd'hui bloquée par la constitution de bases de données progressives. Nous sommes confrontés à un vrai problème d'investissement dans les politiques numériques, ainsi que de normalisation, d'uniformisation et de rénovation numérique de l'État. Cela bloque un certain nombre d'initiatives que l'État pourrait lancer et cela est dommage.

M. Philippe Latombe, rapporteur. La culture de la protection de la donnée fait-elle partie de la culture de l'État, ou l'État doit-il l'acquérir ? Avez-vous des recommandations à partager en matière de protection des données ?

Pr Thibault Douville. L'État est actif en matière de protection des données. La loi de programmation militaire 2013-2019 a été, par exemple, la première à créer la catégorie des opérateurs d'importance vitale pour protéger les systèmes d'information et les données. L'État est par ailleurs actif par le cadre juridique mis en place, par exemple, concernant la sécurité des données de santé qui font l'objet d'un hébergement. Il existe une vraie politique étatique en matière de protection des données. De ce point de vue, il me semble que l'État est assez proactif, aussi bien en matière de protection des données que de cybersécurité.

Il est plus surprenant peut-être de constater la défiance que les citoyens peuvent entretenir à l'égard de l'État quant à la manière dont il traite les données et aux finalités poursuivies par ces traitements. Le projet Alicem en est un exemple concret : le traitement de données visait à permettre la création d'un moyen d'identification électronique sur un *smartphone*. Il a provoqué des réactions assez vives en raison des risques que le système poserait quant à la protection des données à caractère personnel, notamment en raison du stockage centralisé d'un certain nombre de données. L'État devrait peut-être mettre en œuvre une politique pour minimiser les données traitées afin de favoriser la confiance des citoyens. Était-il par exemple nécessaire, dans le projet Alicem, de prévoir un stockage centralisé des données à des fins d'authentification compte tenu des usages possibles du moyen d'identification électronique ? L'État devrait peut-être développer une politique de minimisation des données pour favoriser la confiance des citoyens. Il me semble que la quantité ou le volume des données traitées, par l'État, peut créer une difficulté pour les citoyens. La meilleure protection des données est la minimisation. La meilleure anticipation du risque cyber est la minimisation des données traitées.

La collecte massive des données génère un risque. Il est tout à fait possible de modifier, par voie réglementaire ou législative, la finalité de l'utilisation des données pour transformer l'objet du traitement. C'est en cela que le raisonnement sur la finalité du traitement n'est pas forcément satisfaisant à lui seul. Une mise en œuvre du principe de minimisation des données constitue une vraie protection complémentaire des droits et libertés. La minimisation

constituait le principe de base du RGPD, et l'on se focalise aujourd'hui davantage sur les finalités poursuivies que sur la minimisation des données.

La transformation numérique de l'État est un point fondamental en ce qui concerne la souveraineté. La place de l'État dans l'environnement numérique a vocation à se renforcer : l'État est très présent hors numérique, mais quelle est sa place dans l'environnement numérique ? Il y a toute sa place. Pour cela, l'État a certainement vocation à remettre le citoyen au cœur de ses données et au cœur de son identité ainsi qu'à minimiser les données traitées, afin de redonner une certaine prise au citoyen sur l'activité de l'État en matière numérique et à lui redonner confiance. Il est aberrant que les citoyens aient, en France, davantage confiance en Facebook ou Google qu'en l'État pour traiter leurs données.

M. Philippe Latombe, rapporteur. Y a-t-il des sujets que nous n'avons pas abordés et que vous souhaitez évoquer ?

Pr Thibault Douville. Nous avons, je crois, couvert l'essentiel des questions. Je vous enverrai une réponse écrite sur le périmètre d'application du *Cloud Act* aux filiales d'entreprises américaines.

Audition, ouverte à la presse, de M. Julien Nocetti, docteur en sciences politiques, chercheur associé à l'institut français des relations internationales (Ifri) et enseignant-chercheur en relations internationales et études stratégiques aux Écoles de Saint-Cyr Coëtquidan *(11 mars 2021)*

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. Pour évoquer les enjeux géopolitiques de la souveraineté numérique, nous avons le plaisir de recevoir M. Julien Nocetti, docteur en sciences politiques, chercheur associé à l'institut français des relations internationales (Ifri) et au centre Géopolitique de la Datasphère (GEODE), qui vient d'ailleurs d'obtenir le label d'excellence du ministère des Armées. Enseignant les relations internationales et les enjeux numériques aux Écoles militaires de Saint-Cyr Coëtquidan, ses travaux portent notamment sur la diplomatie du numérique et l'intelligence artificielle, sur l'évolution de la cyber-conflictualité – avec une expertise de longue date sur la Russie – et sur les rapports entre États et grandes plateformes du numérique. Sur l'ensemble de ces sujets, M. Nocetti participe régulièrement à des conférences internationales et multiplie les interventions dans les médias français et étrangers.

M. Philippe Latombe, rapporteur. Je vous interrogerai sur trois points.

Quel sens peut revêtir la notion de souveraineté numérique, abordée sous l'angle géopolitique et diplomatique ? Nous avons échangé à de multiples reprises — c'est une question-type que je pose régulièrement en début d'audition – sur ce concept, que l'on peut définir comme une forme d'autonomie stratégique ou décisionnelle. J'aimerais donc savoir comment vous appréhendez cette notion et comment elle contribue à remodeler les relations internationales.

Le deuxième point se rapporte aux enjeux de cyberdéfense et de cybersécurité et à leurs conséquences géopolitiques. Comme vous le savez, ce sujet est prégnant au niveau national, comme en témoignent les nombreuses cyberattaques relayées par la presse, mais également au niveau international, comme l'affaire SolarWinds. La Commission européenne a défini une stratégie en matière de cybersécurité, qui doit soutenir le développement de capacités de cyberdéfense et l'établissement d'une politique internationale de cyberespace ouverte et cohérente. La France et l'Europe sont-elles prêtes à faire face à l'importance croissante de ces enjeux ? Comment percevez-vous les nombreux projets de régulation du numérique portés au niveau européen, comme les directives *Digital Services Act (DSA)*, *Digital Markets Act (DMA)* ou *Data Governance Act (DGA)* ?

Enfin, en ce qui concerne la diplomatie numérique française et européenne, notre mission d'information a auditionné l'ambassadeur pour le Numérique, M. Henri Verdier, ainsi que l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP), qui participe aux travaux des organismes internationaux traitant de ces sujets. La France se distingue-t-elle des autres pays en confiant la coordination de la défense de ses intérêts à un acteur dédié ? Plus globalement, comment peut-on qualifier le positionnement de la diplomatie numérique française ?

M. Julien Nocetti, docteur en sciences politiques, chercheur associé à l'institut français des relations internationales (Ifri). Je vous remercie de m'avoir invité à m'exprimer sur ces enjeux que vous venez d'esquisser, qui sont absolument passionnants, éminemment

complexes, très évolutifs et qui mobilisent votre mission d'information. En guise de préambule, je me permets de préciser que je dirige aussi, depuis peu, la chaire Cybersécurité de Rennes School of Business, au sein de l'une des plaques territoriales de la cybersécurité en France.

Mon propos liminaire reprendra naturellement les questions que vous m'avez adressées. Il sera nécessairement partiel, eu égard à la diversité de ces grands enjeux de souveraineté numérique, quitte à créer une forme de frustration qui, je l'espère, sera aussi réduite que possible.

En lien avec votre première interrogation, je débuterai par une série de constats relatifs à cette souveraineté numérique – qui est ardemment souhaitée et rarement satisfaisante pour nous en Europe – et à ses enjeux, avant de m'attarder sur des enjeux plus immédiats et plus prégnants.

D'abord, le concept de souveraineté numérique n'a pas émergé partout au même moment. En Europe, et en France en particulier, le lien entre la souveraineté des États et l'ère de foisonnement numérique a commencé à être évoqué dès la fin des années 2000. Sans surprise, nous constatons une montée en puissance de ce concept à l'occasion des révélations d'Edward Snowden, avant que l'emprise des grandes plateformes américaines du numérique ne vienne nous révéler crûment, et de manière progressive, nos propres failles en matière de souveraineté.

La souveraineté numérique n'est pas toujours pareillement comprise – permettez-moi cette litote – dans les différentes zones du globe, ce qui induit d'y prêter un regard plus global et plus géopolitique. Des États comme la Chine et la Russie – mais non eux seuls – ont pensé, de très longue date, la souveraineté numérique sous le prisme de la souveraineté de l'information, avec l'idée que les contenus produits et échangés sur le web comptaient tout autant, sinon plus, que l'infrastructure physique. Cette différence peut sans doute nous paraître « lointaine » car relevant d'une autre culture politique, mais il s'agit précisément du biais que nous devons éviter.

J'en arrive à un sujet que nous avons peut-être occulté ces derniers temps. Les grandes plateformes du web, que nous connaissons tous, ont été conçues pour défaire l'autoritarisme et défendre la démocratie. Pourtant, nous vivons aujourd'hui une séquence où la contrainte pesant sur le respect de la vie privée en ligne – et la tyrannie de la transparence qui peut aussi en découler – suggère une forme d'alignement progressif des pratiques de nos États démocratiques sur celles des régimes autoritaires. Je ne dresse évidemment pas des tables d'équivalence, mais cette tendance est clairement d'actualité depuis cinq ou six ans.

Dans ce contexte, le sujet de la souveraineté numérique constitue, depuis longtemps, une ligne de fracture dans la gouvernance internationale de l'espace numérique, avec des États – je les ai mentionnés – ayant pour eux le mérite de la constance de leurs positions. C'est un point que nous avons certainement sous-estimé les années précédentes, avant que ne se renforce, en Europe et en France en particulier, notre propre appareil diplomatique en matière de numérique.

Nous observons, par ailleurs, que l'enjeu de la souveraineté numérique est parfois exploité, par les États que j'ai mentionnés, à des fins stratégiques et de politique étrangère. Il est d'ailleurs frappant de relever, soit dit en passant, que certains médias russes – que nous connaissons bien depuis 2017 – n'ont aucun complexe à instrumentaliser ce sujet de la souveraineté numérique, ou plutôt l'absence de souveraineté numérique en Europe, avec en contrepoint les différents scandales d'espionnage qui ont émaillé la vie politique et stratégique

européenne depuis une dizaine d'années. La souveraineté numérique est donc une thématique qui est aussi exploitée à nos propres dépens, et nous devons nécessairement prêter attention à cette dimension dans l'élaboration de doctrines et pour peser dans ce domaine.

De surcroît – c'est peut-être un lieu commun –, cette thématique est devenue indissociable de l'effet systémique produit, d'abord, par les géants américains Google, Apple, Facebook, Amazon et Microsoft (GAFAM), mais également par les géants chinois Baidu, Alibaba, Tencent et Xiaomi (BATX). Nous connaissons bien le phénomène de grignotage – certains diraient de dépeçage, mais je n'irais peut-être pas jusque-là aujourd'hui – des prérogatives souveraines des États par ces acteurs. Je n'insisterai pas outre mesure sur ce point, mais je citerai quelques exemples en guise d'illustration. À l'heure actuelle, le meilleur cadastre au monde est l'outil Google Maps. Pour sa part, Facebook détient probablement plus de données sur ses utilisateurs que n'en possédera jamais l'état-civil. Sur le plan monétaire, le projet Libra porté par Facebook pourrait, à terme, prendre de vitesse l'Union africaine dans son ambition de relier les États africains par le biais d'une monnaie unique. En matière de sécurité, de plus en plus de géants du numérique ont développé des capacités pour parer aux cyberattaques. Enfin, dans une perspective plus diplomatique, certains de ces géants aiment à se comparer aux acteurs diplomatiques traditionnels. Je ne mentionnerai aucun nom, mais ce phénomène est clairement visible sur la scène internationale.

Il me semble qu'il existe une forme de contradiction entre le phénomène de territorialisation du cyberespace, qui est renforcé par des considérations de souveraineté, et la position des GAFAM en tant que signes hors-sol de la puissance américaine. Ce point important n'est pas toujours bien mesuré en Europe occidentale, et plus particulièrement en France. Notre manière de penser les relations internationales et la géopolitique repose sur l'idée d'espace, de frontière, de territoire. Pourtant, nous assistons aujourd'hui à un phénomène de déspatialisation, qui dépasse le numérique, mais qui le concerne très nettement. Il existe déjà une réalité du rapport de pouvoir dématérialisé, qu'il est très difficile de juridiciser. Toutefois, les dirigeants américains ont eu le génie d'être les premiers à l'appréhender. Avant même la chute du mur de Berlin en 1989, ils ont compris qu'ils allaient perdre le contrôle effectif de l'espace, mais qu'ils pourraient exercer leur pouvoir et leur puissance en maîtrisant les signes hors-sol. Nous en avons vu la première manifestation dans les révolutions monétaristes et financières, dont il n'est pas question aujourd'hui, puis dans le développement du numérique, d'Internet et de l'économie globale.

L'exercice du pouvoir américain – et la mondialisation qui en découle depuis plusieurs décennies – se caractérise également par l'existence de courts-circuits, sur lesquels se fonde, en grande partie, cette puissance numérique américaine. Dans cette logique, la construction originelle basée sur l'espace est court-circuitée par d'autres éléments. En effet, ce pouvoir repose sur la maîtrise et le contrôle de différents signes, notamment monétaires et numériques, qui permettent aux Américains d'exercer une forme de souveraineté sur tous les autres domaines d'activité, mais aussi sur tous les autres pays. Pour maîtriser les signes, tout doit passer par le territoire américain. À cet égard, la question des données illustre parfaitement mon propos. Si vous ne deviez retenir qu'un seul chiffre, sachez que 90 % des données produites sur le continent européen transitent, à un moment, par le territoire américain. Je pense que c'est un paramètre que nous devons bien mesurer.

Au-delà du cas américain, nous devons bien appréhender l'évolution extrêmement rapide de cette notion de souveraineté numérique et des enjeux qu'elle charrie. En 2021, la souveraineté numérique est très différente de la souveraineté numérique que nous commencions à appréhender en 2010 ou en 2014, un an après l'affaire Edward Snowden. À l'époque, lorsque l'on évoquait la notion de souveraineté numérique, les débats se

focalisaient essentiellement sur une seule question : qui contrôle Internet ? Aujourd'hui, les enjeux sont extrêmement différents, puisque la question dépasse le champ numérique traditionnel – infrastructures, Internet, web, etc. Par conséquent, nous devons urgemment élargir notre propre focale en y incluant les technologies critiques. L'intelligence artificielle, la 5G et l'informatique quantique ne peuvent pas être occultées de notre conception de la souveraineté numérique, tout comme l'enjeu de l'approvisionnement en composants critiques, sur lequel je reviendrai dans quelques instants. Je pense également à la maîtrise d'algorithmes sensibles. Ces problématiques sont d'une très grande complexité lorsqu'elles s'intercombinent. Je vous laisse donc imaginer à quel point toute ambition de souveraineté numérique est vertigineuse.

Je viens d'évoquer un point particulier, sur lequel j'apporterai quelques développements, et auquel les médias prêtent de plus en plus d'attention. Il s'agit des semi-conducteurs. Cet aspect a été occulté durant des années, avant d'animer l'actualité à la faveur ou à la défaveur des tensions sino-américaines et des différents décrets adoptés par Donald Trump à partir de mai 2019. Les semi-conducteurs sont aujourd'hui absolument fondamentaux et centraux dans ces ambitions de souveraineté numérique. Le sujet n'est pas nouveau, mais il s'est amplifié à mesure de notre dépendance accrue à ces composants, et à mesure que nous prenions conscience de la complexité des chaînes de valeur globales des semi-conducteurs. Nous dépendons d'acteurs américains pour leur conception et leur design, d'acteurs taïwanais pour la fonderie et leur production physique, mais aussi d'acteurs chinois, britanniques ou singapouriens pour d'autres volets de ces chaînes de valeur. Ces composants technologiques revêtent logiquement une dimension géopolitique extrêmement forte, ainsi qu'une dimension économique majeure au regard de leur prolifération et de l'industrie très globalisée qui les entoure. L'enjeu est également stratégique. En effet, si nous avons surtout tendance à aborder la dimension civile et commerciale de ces semi-conducteurs, qui innervent nos smartphones et autres produits informatiques, nous ne devons pas en oublier les enjeux critiques en termes de supériorité militaire pour les décennies à venir.

La question des semi-conducteurs induit donc des enjeux de souveraineté numérique et technologique extrêmement puissants. Par cet aspect, la dimension industrielle est intimement liée à la dimension géopolitique. C'est par le biais de ce composant qui paraissait initialement anodin – le semi-conducteur – que nous mesurons aujourd'hui toute la complexité et toute l'interdépendance de nos chaînes de valeur. Dans ce domaine, l'Europe dispose d'une faible marge de manœuvre, du moins pour le moment. Ses acteurs – Infineon, NXP, STMicroelectronics – demeurent relativement modestes en termes de taille. En outre, le climat stratégique autour de la 5G – dont les semi-conducteurs constituent l'ossature la plus avancée – nuit à l'homogénéité de vues entre Européens et à la prise de décision.

Comme vous l'évoquiez, l'Europe cumule des faiblesses déjà bien identifiées en matière de souveraineté numérique, qu'il s'agisse de facteurs internes ou externes. En interne, citons l'insuffisante intégration du marché numérique, les problématiques de financement de l'innovation, les divergences politiques entre États membres, etc. À l'extérieur, l'Europe s'expose de plus en plus à des stratégies de puissance prédatrices et éprouvées. J'ai déjà évoqué, dans le cas des États-Unis, une longue tradition combinant puissance financière, puissance technologique, mais aussi attraction des GAFAM – par le biais d'un écosystème extrêmement performant – et extraterritorialité du droit américain. Du côté de la Chine, la célérité et le centralisme de la prise de décision, conjugués à une absence totale de considérations éthiques en interne, expliquent pourquoi cette spécificité chinoise parvient à acquérir quelques avantages en matière stratégique, au détriment de l'Europe.

Vous avez également évoqué l'idée d'autonomie stratégique qui, à mon sens, vient s'entrechoquer avec cette notion de souveraineté numérique. Ce concept d'autonomie stratégique, extrait du champ lexical de la défense française depuis l'époque du général de Gaulle, a fait son entrée dans la politique européenne, y compris dans différents documents d'orientations stratégiques de l'Union européenne en matière de sécurité et d'affaires étrangères. Le problème est que les États membres ne soutiennent pas tous le développement d'une autonomie stratégique européenne, tandis que ses partisans ne s'accordent ni sur ce qu'elle recouvre ni sur le niveau d'ambition stratégique que l'Europe devrait acquérir et mettre en œuvre dans le domaine numérique. À cet égard, l'attitude à adopter vis-à-vis des États-Unis demeure une divergence fondamentale, tandis que les risques qu'une autonomie stratégique européenne pourrait faire peser sur les relations transatlantiques – particulièrement sur les sujets de défense – demeurent un véritable point de crispation

Le contexte actuel en matière de numérique s'avère donc assez particulier pour l'Europe. À la lecture d'une Europe perçue comme une « colonie numérique » s'oppose une approche plus nuancée mettant en avant le volontarisme de l'actuelle Commission européenne en matière de protection numérique ou d'intelligence artificielle. Nous avons d'ailleurs affaire à une Commission européenne qui se veut *« géopolitique »*, selon les propres mots de sa présidente. Pourtant, plusieurs signaux contradictoires sont envoyés depuis quelques mois.

D'un côté, nous retrouvons l'activisme bien connu du commissaire au marché intérieur, qui se superpose d'ailleurs aux différentes initiatives du Portugal, qui préside actuellement le Conseil de l'Union européenne. Je songe notamment à différentes initiatives intéressantes relatives aux câbles sous-marins, qui font suite à des propositions en matière de *cloud* et de semi-conducteurs, avec un accent très marqué – j'insiste sur ce sujet – sur les infrastructures critiques. Ce point majeur témoigne bien de l'évolution de l'Europe dans son appréhension du phénomène et de sa dépendance vis-à-vis d'infrastructures maîtrisées par des puissances extérieures.

D'un autre côté, la stratégie dite *« boussole numérique 2030 »* récemment publiée s'avère relativement décevante. Pour être tout à fait franc, l'on n'y décèle pas, loin de là, une tonalité géopolitique faisant transparaître une réelle ambition de souveraineté numérique, même si le terme y est employé, quoiqu'à une seule reprise. Par ailleurs, d'autres déclarations et d'autres formes de rhétorique brouillent quelque peu le message de la Commission européenne. Je fais ici référence à une récente lettre ouverte adressée par la chancelière allemande et les premières ministres estonienne, finlandaise et danoise à Ursula von der Leyen, qui nous fait penser que ce concept de souveraineté numérique masque des logiques d'interdépendances devenues un véritable marqueur de notre époque, en dépit des stratégies dites *« de découplage »* que les États-Unis tentent d'imposer « avec force » depuis quelque temps.

Pour en revenir à votre première question relative à la définition de la souveraineté numérique, je rappellerai d'abord que beaucoup s'y sont déjà essayés, et que je ne suis donc pas certain de pouvoir y apporter une contribution fondamentalement nouvelle. Néanmoins, en lien avec cette logique d'interdépendances, la souveraineté numérique pourrait consister à pouvoir choisir nos interdépendances. Par cette formule, je sous-entends l'idée de choix, de stratégies, de moyens, de capacités, mais également l'idée que nous évoluons dans un contexte global d'interdépendances. Nous devons bien mesurer que certaines approches de la souveraineté numérique édictées ou martelées au cours de la dernière décennie ont pu parfois sembler cantonnées à des logiques nationales extrêmement réductrices, sans doute caricaturales, qui occultaient complètement le fait que notre monde demeurait extrêmement

globalisé et soumis à des logiques d'interdépendances, en dépit des formes de nationalisme technologique auxquelles nous avons pu assister du côté chinois comme du côté américain.

Nous évoluons aussi dans un contexte particulier, comme je l'indiquais précédemment, de par la récente élection de Joseph Biden à la présidence des États-Unis, qui vient nécessairement trancher avec les quatre années de la présidence de Donald Trump. Le moment est sans doute paradoxal pour nous autres Européens. Cette présidence Trump, ô combien chaotique et problématique à certains égards, nous a tout de même réveillés, en nous donnant enfin l'occasion d'affronter nos propres vulnérabilités et nos propres failles dans le domaine numérique et le domaine technologique au sens large. Avec la présidence Biden, nous risquons d'en revenir à ce vieux consensus transatlantique et d'en oublier nos propres divergences vis-à-vis de certaines thématiques numériques, d'abord, sur les enjeux de fiscalité, mais aussi sur les enjeux de transferts des données, qui constituent précisément, depuis des années, l'une des pierres majeures d'achoppement entre l'Europe et les États-Unis. De la part de cette administration Biden, nous devons peut-être nous attendre à une forme de géoéconomie très brute, qui ne tranchera pas nécessairement avec la présidence Trump, mais qui sera enveloppée de multilatéralisme très poli.

Je pense à l'instant à un autre paramètre à prendre en compte sur cette thématique du numérique. Qu'il s'agisse des questions de cybersécurité, d'échanges de données, de droits de l'homme, etc., nous devons nous attendre à interagir avec des interlocuteurs américains très expérimentés. Certains d'entre eux occupaient déjà des postes à haut niveau sous la présidence de Barack Obama. Surtout, ces interlocuteurs sont extrêmement compétents. Il s'agit évidemment d'un aspect tranchant avec la présidence Trump, durant laquelle certains postes à responsabilités au sein de la haute administration américaine étaient parfois restés vacants. Aujourd'hui, ces postes sont pourvus et occupés par des individus à l'expertise extrêmement riche. Cette dimension ne doit pas être sous-estimée, du côté européen, lorsque nous cherchons à échanger avec nos alliés et à leur faire passer nos propres messages.

J'en termine sur ce propos introductif, qui m'a permis de répondre brièvement à une partie de vos questions liminaires. Comme vous le sous-entendiez, ces enjeux sont bien plus vastes. Par exemple, je n'ai pas eu l'occasion d'évoquer, dans mon propos, l'enjeu du capital humain, qui est certainement l'un des aspects les plus sous-estimés de ces enjeux de souveraineté numérique. C'est aussi en évitant la fuite des cerveaux et en formant massivement ses propres experts que l'Europe pourra s'affranchir de sa tutelle numérique. À cet égard, trois enjeux se superposent : l'enjeu de la formation, que nous venons d'évoquer ; l'enjeu de la rétention de nos cerveaux ; l'enjeu de la captation. C'est sur cet enjeu humain que la question du numérique prend une dimension quasi géopolitique, d'autant que nous l'avons trop longtemps sous-estimé, alors que les États-Unis peuvent s'enorgueillir d'une expérience extrêmement riche en la matière. Si l'Europe ambitionne de peser dans ce domaine et de s'affranchir, au moins partiellement, de ces formes de tutelle que je viens d'évoquer, elle doit nécessairement et urgemment répondre à cet enjeu de formation au long cours.

M. Philippe Latombe, rapporteur. S'agissant des semi-conducteurs et du volet matériel dans son ensemble, vous indiquiez que l'Europe était quelque peu à la traîne – en tout cas, je l'ai compris ainsi – et que les Américains avaient pris de l'avance. Pour faire écho à vos propos sur la nouvelle administration américaine, Joseph Biden a initié un grand plan sur les semi-conducteurs afin de rapatrier la production aux États-Unis, mais également pour chercher des solutions d'avenir. Est-ce à dire que les Américains ont aujourd'hui peur de l'émergence chinoise sur le marché des semi-conducteurs ? Devons-nous nous attendre à une nouvelle guerre sino-américaine sur ce segment en particulier, et considérer que les tensions avec Huawei n'étaient que les prémices de prochaines étapes conflictuelles ? Dans ce cas,

comment l'Europe peut-elle s'affranchir de ce conflit pour ne pas se retrouver prise entre deux feux, autrement dit entre les États-Unis et la Chine ?

M. Julien Nocetti. Ces questions recouvrent à nouveau des enjeux éminemment politiques, dont les impacts se feront ressentir jusqu'en Europe. D'abord, il est amusant de constater que cette problématique des semi-conducteurs émerge après deux ou trois années de tensions extrêmement vives entre Américains et Chinois. À l'origine, ce sont surtout les enjeux de propriété intellectuelle et de cybersécurité qui caractérisaient ces tensions. L'intelligence artificielle s'est ensuite retrouvée au cœur de la rivalité sino-américaine, au point de cristalliser un certain nombre de peurs – notamment de déclassement – chez les Américains, eu égard à la montée en puissance de la Chine. Plus récemment, le dossier de la 5G a provoqué un regain de tensions entre les deux acteurs, avec notamment les performances internationales de la société Huawei. De ce point de vue, l'enjeu des semi-conducteurs est particulièrement intéressant. Comme je l'indiquais précédemment, cet enjeu fut très longtemps occulté, surtout par les Européens, mais aussi par les Américains, qui n'avaient peut-être pas mesuré les ambitions chinoises d'autonomisation technologique en la matière.

Sans revenir en détail sur la stratégie de Pékin, différents plans ont été annoncés par les dirigeants chinois dans le domaine des technologies et des semi-conducteurs. Le plus fameux, *« Made in China 2025 »*, consiste à acquérir une forme de souveraineté, disons de maîtrise, sur la plupart des technologies dites critiques. Plusieurs technologies clés ont ainsi été identifiées comme extrêmement vitales pour l'avenir de la Chine. En l'occurrence, les semi-conducteurs avancés, notamment ceux intégrant de l'intelligence artificielle, sont perçus comme à l'avant-garde de ce que la Chine doit maîtriser et produire massivement. Pourtant, du côté chinois, l'objectif est loin d'être atteint. Malgré les montants faramineux parfois avancés par les autorités de Pékin, la Chine ne maîtrise pas, à ce stade, les composants les plus sophistiqués, dont la miniaturisation est poussée à son paroxysme et qui peuvent être intégrés au sein des produits et des services les plus sensibles. De ce point de vue, les Chinois affichent encore, aujourd'hui, un déficit de souveraineté.

Du côté américain, la situation est paradoxale. Certains acteurs comme Qualcomm, Apple et Intel jouissent d'une forme de leadership sur certaines parties de la chaîne de valeur des semi-conducteurs, en particulier dans leur design. En revanche, les Américains ne maîtrisent pas l'ensemble du spectre et dépendent de chaînes de valeur tout à fait globalisées, comme je l'indiquais précédemment. C'est d'ailleurs pour cette raison que le géant américain Nvidia a tenté, l'été dernier, de racheter le britannique ARM, qui est extrêmement avancé dans la construction de semi-conducteurs. L'accord a semble-t-il capoté pour diverses raisons. Néanmoins, cette tentative montre bien que les Américains sont devenus extrêmement susceptibles sur cet enjeu des semi-conducteurs et cherchent à mettre certains de leurs alliés sous pression, notamment en Asie. Je pense notamment à Taïwan, qui revient en force dans cette géopolitique des technologies, et qui héberge notamment la société TSMC, leader mondial de la fonderie et de la production de ces composants. Durant sa présidence, Donald Trump a cherché à relocaliser, sur le territoire américain, précisément en Arizona, une partie de la production de TSMC. J'ignore si l'accord sera ou non maintenu par l'administration Biden, mais force est de constater que cet enjeu fut véritablement, durant plusieurs années, au centre de l'agenda bilatéral sino-américain et des tensions géopolitiques en matière de technologies.

De son côté, l'Europe commence à mesurer l'intérêt de cet enjeu. Il est tout à fait logique, d'ailleurs, que l'actuelle présidence portugaise du Conseil de l'Union européenne l'ait inscrit dans les premières lignes de son agenda politique.

M. Philippe Latombe, rapporteur. De nombreuses cyberattaques ont été attribuées à la Russie. Depuis quelque temps, et encore très récemment, la plupart des cyberattaques sont attribuées aux Chinois. Est-ce un révélateur de leur positionnement ou de leurs oppositions géopolitiques ? Voici quelques années, les Russes avaient été mis en cause pour le virus Petya. De leur côté, les Nord-Coréens avaient été accusés d'avoir lancé des cyberattaques sur le sol américain. Très récemment, l'attaque subie par Microsoft a été attribuée à des Chinois. S'agit-il donc d'un révélateur ou d'un bon thermomètre de la géopolitique et des antagonismes caractérisant l'univers du numérique ?

M. Julien Nocetti. Il s'agit effectivement d'un révélateur extrêmement éclairant. Par le passé, les Américains avaient déjà attribué quelques attaques à la Chine. Durant la présidence de Barack Obama, ces tensions et ces attributions étaient demeurées, sinon en sourdine, du moins relativement discrètes par rapport aux attributions formulées sous la présidence de Donald Trump. Les attributions publiques constituent d'ailleurs – nous basculons dans une autre thématique – un point extrêmement sensible de cette géopolitique.

Les Américains ne se privent absolument pas d'attribuer publiquement des cyberattaques. Au contraire, la France s'y montre plutôt réticente, pour différentes raisons, principalement parce que les capacités d'attribution reposent sur des traces techniques détectables et sur des capacités de renseignement. De fait, lorsque vous attribuez une attaque, vous révélez en partie vos propres capacités de renseignement. Nous comprenons donc les réticences de la France dans ce domaine. En revanche, les Américains appliquent une politique d'attribution publique systématique, dite du *« name and shame »*, qui a débuté à la fin du mandat de Barack Obama, avec notamment différentes attaques attribuées à la Russie à l'occasion de la campagne présidentielle de 2016. Plus largement, les exemples nord-coréens jalonnent les présidences américaines successives. Souvenons-nous notamment de la cyberattaque ayant ciblé Sony Pictures en 2014, qui avait conduit Barack Obama à réagir publiquement à la télévision américaine pour attribuer cette attaque importante au régime de Pyongyang.

Sous l'administration Trump, les attributions publiques sont allées *crescendo*. Si ces attributions émanaient initialement de la Maison-Blanche, le processus d'attribution a graduellement été marqué par une forme de décentralisation. Les attributions n'émanaient plus nécessairement de Donald Trump ou de ses conseillers, mais du département de la Justice pour les mises en accusation et du département du Trésor pour les sanctions adoptées vis-à-vis de certains hackers, groupes criminels ou autres.

Avec Joseph Biden, nous devons nous attendre, malgré une volonté d'apaisement qui sera recherchée avec la Chine, à une politique du coup pour coup sur ces questions de cybersécurité, et à une stratégie de représailles systématiques contre ces velléités chinoises de tester les États-Unis. Nous le savons, les Américains sont amplement testés depuis quelque temps. Nous en avons vu la première manifestation avec l'attaque dirigée contre SolarWinds, qui fut pour partie attribuée à la Russie, tandis que certains acteurs chinois auraient également effectué quelques intrusions au sein des systèmes compromis. Je pense également à cette attaque subie par la Floride, dont les systèmes d'approvisionnement en eau auraient été compromis par l'intervention de pirates informatiques. Plus récemment, nous avons tous en tête l'attaque dirigée contre Microsoft Exchange par le biais de pirates chinois.

Aux États-Unis, cette tradition d'attributions publiques des attaques relève aussi d'une logique d'envoi de signaux : envoyer des signaux de dissuasion et/ou de coercition et empêcher que tel ou tel acteur ne se livre à des attaques répétées et plus conséquentes en termes de dégâts. S'il est probable que cette tendance se poursuive aux États-Unis, reste à savoir si cette systématisation des attributions se répercutera, à long terme, chez les alliés européens.

Au Royaume-Uni, on observe depuis quelque temps une forme de mimétisme et d'alignement, avec de multiples cyberattaques attribuées à la Russie. Le reste de l'Europe est, quant à lui, marqué, sur ce plan également, par des divergences de politiques et de conceptions sur l'attribution ou la non-attribution de cyberattaques. À ce stade, aucun consensus ne semble véritablement se dégager. L'un des points fondamentaux suscitant le plus de débats est d'ailleurs l'enjeu du *« hack back »*, ou piratage en retour, qui confère aux acteurs privés un rôle important en matière de représailles. Ce sujet ne fait absolument pas consensus et se prête parfois aux chamailleries des différents États européens au sein des enceintes de discussion communautaires.

M. Philippe Latombe, rapporteur. Si l'attribution de cyberattaques ou le fait d'y répondre s'apparente à l'envoi d'un signal, c'est bien qu'il existe une diplomatie numérique. En tout cas, cette diplomatie numérique existe assurément du côté des États-Unis, de la Russie et de la Chine. Où en est la diplomatie numérique européenne ? En France, nous disposons d'un ambassadeur pour le numérique, mais où l'Europe se situe-t-elle dans ce mouvement de plaques diplomatique ? Avons-nous une voix qui compte et une véritable diplomatie numérique ? Dans le cas contraire, comment pourrions-nous la construire ?

M. Julien Nocetti. S'agissant de la diplomatie numérique à l'échelle européenne, je resterais relativement mesuré. Bien que relevant des prérogatives du Service européen pour l'action extérieure (SEAE), ces compétences s'exercent encore aujourd'hui selon une logique géographique. En outre, ce paramètre numérique est scindé entre les différentes compétences des commissaires. Le commissaire au marché intérieur a son mot à dire sur certains aspects de diplomatie numérique, ce dont il ne se prive pas, comme en témoignent, depuis le mois de décembre, les différentes stratégies et déclarations formulées en matière de souveraineté et de réponse, vis-à-vis des États-Unis ou de la Chine. Néanmoins, le commissaire à l'innovation et le commissaire à la concurrence – bien évidemment – jouissent également de prérogatives en matière de diplomatie numérique.

Dans une logique plus diplomatique, les États membres européens conservent évidemment leurs compétences. Je relativiserai donc toute réalité ou toute consistance d'une diplomatie du numérique européenne, qui ne « fait pas le poids », pour l'instant, face aux deux acteurs américain et chinois prenant en étau l'Union européenne. Ce champ relève encore aujourd'hui des politiques nationales, avec des niveaux de maturité sans doute différents entre États européens.

M. Philippe Latombe, rapporteur. En lien avec ma précédente question, comment situez-vous les Anglais, qui ont quitté l'Union européenne ? Sur cet échiquier mondial, la petite plaque qu'est le Royaume-Uni se rapprochera-t-elle plutôt des Américains ou se maintiendra-t-elle plutôt dans notre environnement ? Je pense notamment à la protection des données, sachant que le Règlement général sur la protection des données (RGPD) ne sera plus applicable au Royaume-Uni à partir du 1er juillet 2021. Les Britanniques doivent ainsi décider, avant le mois de juin, quel modèle adopter en matière de protection des données. Conserveront-ils l'ancien modèle du RGPD ou entameront-ils une transition vers le modèle américain ? Ce sujet peut-il être source de difficultés ? Sait-on si le Royaume-Uni aurait fait des émules auprès d'États membres qui souhaiteraient se rapprocher des Américains ?

M. Julien Nocetti. Il s'agit d'une question relativement sensible. Avant le Brexit, la diplomatie numérique britannique était assez pléthorique, et le Royaume-Uni était sans doute l'acteur européen le plus consistant dans ce domaine, sans doute par mimétisme vis-à-vis du partenaire américain, mais aussi par connaissance de ces thématiques et par une plus grande maturité sur ces enjeux et sur la défense des intérêts britanniques en la matière. Cette consistance était particulièrement visible sur la plaque bruxelloise, avec des intérêts

britanniques – notamment en matière de commerce et de protection des données – savamment défendus par les officiels de la Couronne, mais aussi une habileté à fonctionner en réseau avec des sociétés de conseil – ou autres – extrêmement efficaces dans la défense de ces intérêts et des approches promues par les Britanniques. Tout ne disparaîtra pas avec la transition et le départ du Royaume-Uni des instances communautaires, puisque le pouvoir britannique disposera toujours d'experts et de relais à Bruxelles.

Quoi qu'il en soit, le contexte numérique britannique est également très particulier, dans le sens où la crise de la COVID-19 a jeté une lumière assez crue sur les dépendances du Royaume-Uni en matière numérique et sur les choix de Londres vis-à-vis de la Chine. Ce dossier a suscité des débats extrêmement animés et placé le Premier ministre Boris Johnson en position parfois délicate. À l'été 2020, le Royaume-Uni a fait le choix assumé de moins chercher à s'attirer les faveurs de Pékin et contracter avec des sociétés technologiques chinoises. Mécaniquement, depuis neuf mois, l'on observe un retour vers l'allié américain, qui pourrait augurer d'un possible alignement des planètes entre Londres et Washington. D'ailleurs, avec l'élection de Joseph Biden, le discours vis-à-vis des Britanniques se voudra plus conciliant que sous la présidence de Donald Trump, durant laquelle les relations anglo-américaines étaient assez chaotiques malgré les déclarations d'amitié répétées de Donald Trump à Boris Johnson.

M. Philippe Latombe, rapporteur. S'agissant de l'espace numérique en tant que tel, les interactions et la diplomatie s'effectuent aujourd'hui dans un espace numérique ouvert. N'assistons-nous pas, progressivement, à une forme de régionalisation d'Internet ? D'un côté, les Chinois se calfeutrent derrière une muraille de Chine et entendent totalement maîtriser leur propre marché, notamment pour des raisons sociétales de contrôle de la population. D'un autre côté, les Américains sont hégémoniques sur leur marché, au point de ne laisser place à personne d'autre. Dans ce contexte où l'Europe serait le point de rencontre de ces deux grosses plaques régionales – je dirais même de ces châteaux forts – quasiment inattaquables, n'aurions-nous pas intérêt à trouver une troisième voie pour nous protéger ?

M. Julien Nocetti. C'est un point intéressant, dans la mesure où cette idée de troisième voie – sur laquelle je travaille actuellement – n'est pas nouvelle. Si l'on en retrace la généalogie, cette notion de troisième voie est surtout mise en avant depuis l'affaire Edward Snowden. À l'origine, certaines propositions politiques ont pu sembler farfelues ou décalées. En 2013, la proposition d'Angela Merkel de mise en place d'un Schengen de l'Internet avait suscité une série d'incompréhensions politiques à différents niveaux, avant d'être balayée d'un revers de main par les Américains. Je songe également aux stratégies d'évitement d'une ultra-dépendance aux câbles sous-marins contrôlés par des sociétés américaines. La question n'est donc pas nouvelle, puisque ces propositions pouvaient être envisagées, à l'époque, comme une forme de troisième voie permettant à l'Europe de se positionner entre cette vision très libertarienne à la californienne – bien que soutenue par le pouvoir fédéral – et cette vision techno-autoritaire à la chinoise.

Depuis, l'accent a fortement été mis sur les valeurs, en particulier avec l'adoption du RGPD en mai 2018. Loin de moi l'idée de critiquer ce point précis de la diplomatie numérique des États européens. Cela dit, alors que la diplomatie numérique à l'européenne se place uniquement sur la défense des valeurs, en particulier de l'éthique en matière de données et d'intelligence artificielle, les deux blocs américain et chinois n'ont absolument aucune pudeur à s'affranchir de ce type de considérations et à s'inscrire dans des logiques de puissance assez classiques. Je ne souhaite absolument pas relativiser ou mettre sous le tapis ce type de politique éminemment louable. Est-ce toutefois suffisant pour être en mesure de peser sur la scène

internationale ? Est-ce suffisant pour entrer dans une démarche plus soutenue de souveraineté numérique ? Je n'en suis pas totalement certain.

Un choix est à opérer dans cette logique de troisième voie. Doit-elle impliquer une démarche plus proactive en matière numérique ou devons-nous nous reposer sur la défense d'une vision spécifique du numérique, qui nous classerait à part sur cette carte numérique internationale ? Ces questions demeurent ouvertes. En tout état de cause, nous parvenons à un tournant dans cette approche de troisième voie. Dans d'autres régions du monde, en Asie du Sud-Est, dans le sous-continent indien, en Afrique, au Moyen-Orient, les approches et les politiques américaines et chinoises s'entrechoquent et s'affrontent, tandis que l'Europe est parfois très absente. Nous devons donc veiller à ne pas rester invisibles ou en retrait sur notre piédestal de la défense d'un monde libre et débarrassé de ses contingences les moins réjouissantes. Ces éléments semblent peut-être abstraits, mais je suis convaincu que toute réflexion ultérieure sur cette idée de troisième voie devrait nous amener à penser le type de modèle que nous souhaiterions défendre.

M. Philippe Latombe, rapporteur. Vous avez souligné, à plusieurs reprises, que les Américains avaient pris conscience de l'inéluctabilité des problèmes d'espace, et qu'ils s'étaient pleinement engagés dans le numérique pour contrebalancer cette évolution. Si l'on se réfère au premier sens de la notion d'espace, à savoir l'Espace, situé au-delà de la surface de la Terre, nous observons que les Américains lancent, *via* des acteurs privés, des constellations de satellites pour être en capacité de communiquer partout sur tous les points du globe – c'est un autre projet d'Elon Musk. De notre côté, le commissaire européen souhaite lui aussi lancer sa propre constellation. Nous suivons ainsi les évolutions proposées par les Américains ou les Chinois, en nous efforçant de rattraper notre retard. D'après vous, avons-nous la possibilité, sur un certain nombre de technologies, de prendre de l'avance et d'être suffisamment proactifs pour assumer un leadership sur ces technologies indispensables à l'avenir ?

M. Julien Nocetti. Cette question est presque vertigineuse. Vous avez à juste titre évoqué cette forme de suivisme et d'approche défensive de l'Union européenne, notamment en matière de numérique ou de cybersécurité. Différents éléments peuvent pourtant nous apporter un peu d'espoir ou donner matière à réfléchir. Je pense ici aux différentes initiatives récemment avancées en matière de 6G. Dans la mesure où nous sommes encore dans une phase embryonnaire de déploiement de la 5G, parler de 6G pourrait sembler très abstrait. Pourtant, des réflexions et des projets très concrets ont déjà été initiés dans ce domaine.

De fait, si l'Europe pouvait s'engouffrer dans des niches – certes étroites – d'excellence, il s'agirait plutôt de niches intégrant une dimension normative et de standards. On doit bien comprendre que la plupart des tensions numériques et technologiques des quatre ou cinq dernières années ont étroitement associé des enjeux de normes et standards. Auparavant, ces enjeux relevaient de processus de régulation extrêmement techniques. Aujourd'hui, ils ont pris une dimension géopolitique extrêmement puissante. Dans ce domaine, les Européens ont également pris conscience de leur propre retard. La 5G a évidemment jeté une lumière assez crue sur cette réalité, notamment du côté américain, puisque nous avons compris que les Américains ne maîtrisaient pas tout le spectre de la technologie 5G. En Europe, la situation est quelque peu différente, avec des acteurs comme Nokia ou Ericsson disposant de leurs propres savoir-faire.

Quoi qu'il en soit, des niches d'excellence sont nécessairement à prendre du côté européen. Dans certains domaines comme la cybersécurité, l'identité numérique ou l'algorithmie, l'Europe dispose de savoir-faire de pointe et de pépites, avec des expertises personnelles et collectives – centres de recherche, laboratoires, start-up – extrêmement

pointues. De fait, pour répondre indirectement à votre question, l'Europe pourrait se montrer plus proactive en assurant la défense et la protection de tels acteurs face à des stratégies prédatrices extrêmement classiques. Nous devons investir des niches d'excellence susceptibles de réduire notre dépendance à d'autres acteurs extra-européens, tout en nous donnant la capacité de protéger nos propres acteurs. Comme l'actualité l'a récemment montré, certains acteurs majeurs de la cybersécurité ont été rachetés par des concurrents étrangers. Différentes pistes doivent donc être explorées dans ce domaine.

M. Philippe Latombe, rapporteur. Peut-on superposer, sur les plaques du numérique, des plaques liées à la défense physique ? Obtient-on des développements numériques et de l'expertise numérique grâce aux besoins de l'industrie militaire et de défense ? Nous savons que les Chinois investissent massivement dans le naval afin de rattraper leur retard sur les Américains. En ont-ils profité pour catalyser sur le numérique et acquérir des avantages dans ce domaine ? Dans le même esprit, le réinvestissement de l'Espace par les Américains a-t-il permis l'émergence de filières numériques plus fortes ? Les deux sujets sont-ils nécessairement liés ou sont-ils décorrélés ?

M. Julien Nocetti. Les deux sujets ne sont absolument pas décorrélés. L'histoire récente des États-Unis témoigne d'ailleurs des liens étroits tissés entre l'écosystème numérique national et le complexe militaro-industriel. C'est notamment pour cette raison que l'on fait de plus en plus souvent référence, aux États-Unis, au complexe militaro-numérique. Cette expression ne relève aucunement du fantasme et a été employée à maintes reprises par quantité d'auteurs.

En Chine, une stratégie de mimétisme a été initiée à partir du début des années 2010, avant de monter en puissance à partir de 2015 avec les différentes ambitions nationales édictées en matière de cybersécurité, d'intelligence artificielle, d'autonomisation technologique, etc. On observe d'ailleurs, davantage du côté chinois que du côté américain, avec les différences de régime que l'on connaît, le caractère totalement assumé des collaborations entre le parti-État, les structures de l'Armée populaire de libération et les différents acteurs de l'économique numérique nationale. Ces différents acteurs numériques sont ainsi très fortement incités à collaborer avec les structures militaires. Une expression chinoise consacrée parle même de *« fusion civilo-militaire »*, traduisant l'idée que toute avancée dans le domaine civil commercial en matière de numérique doit aussi bénéficier à l'armée, aux structures militaires et aux services de renseignement.

L'imbrication entre les deux dimensions est donc extrêmement forte du côté chinois. C'est d'ailleurs l'un des éléments qui peut nous faire réagir si l'on considère l'exportation plus soutenue de ces acteurs chinois en Europe, en Afrique ou ailleurs, et qui explique en partie les très vives réactions des différentes administrations américaines.

M. Philippe Latombe, rapporteur. Quelle est la position de la France au sein de l'Europe ? Quel est notre rôle ? Sommes-nous suffisamment ou insuffisamment moteurs en la matière ? Disposons-nous d'une vision trop franco-française des enjeux ? Comprenons-nous bien les contraintes et les volontés de nos voisins ? Comment sommes-nous perçus par nos partenaires européens ?

M. Julien Nocetti. La question est évidemment très vaste. J'évoquais précédemment le concept d'autonomie stratégique et sa réappropriation partielle par la « bulle bruxelloise », par le biais de certaines initiatives technologiques et numériques. Or ce concept est bien issu du contexte stratégique français. De fait, cette idée d'autonomie stratégique numérique a pu être perçue, par certains États européens à Bruxelles, comme une volonté française d'être,

sinon hégémonique, du moins beaucoup plus présent dans le débat, quitte à essayer d'en imposer les termes. Certains de nos partenaires européens le ressentent ainsi.

Par ailleurs, nos partenaires observent également que la France mène, surtout depuis 2017, une diplomatie de la conférence très soutenue en matière de numérique, avec la succession – presque chaque année – d'évènements internationaux. Je pense ici aux évènements TechForGood et VivaTech, ainsi qu'aux réceptions d'acteurs de la Tech et de patrons américains à Versailles ou à Paris. Scénarisés en grande pompe, ces évènements sont parfois observés avec une forme d'amusement chez certains de nos voisins, qui y voient surtout une volonté de la France de se mettre en avant, au détriment d'une approche plus collective et plus européenne. Je ne fais ici que retranscrire une partie du regard de certains partenaires, qui est assez présente en Allemagne et en Italie, où cette mise en avant de la France suscite parfois quelques critiques.

N'oublions pas, cependant, que la France a été motrice vis-à-vis de certains processus, notamment dans l'Appel de Christchurch. Formulées dans la foulée de l'attentat de 2019, les propositions de la Première ministre néozélandaise sur la nécessité de lutter contre les discours de haine en ligne avaient été relayées par la présidence française, avec une dimension européenne, ce qui avait été positivement perçu par nos partenaires.

Un autre élément m'amènerait peut-être à réagir de manière plus nuancée. Je pense ici à la diplomatie de la cybersécurité, avec l'Appel de Paris, qui associe différents partenaires étatiques, privés et associatifs, et qui est sans doute l'élément majeur de cette diplomatie numérique à la française. *In fine*, cet Appel de Paris de novembre 2018 a bénéficié d'un insuffisant service après-vente, si je puis parler crûment. Cet effort pourrait pourtant être soutenu. D'ailleurs, différentes commissions et différents groupes de travail s'efforcent aujourd'hui de prolonger les propositions de l'Appel de Paris. Néanmoins, en échangeant avec des officiels et des experts extra-européens, on comprend que les propositions françaises formulées dans l'Appel de Paris demeurent peu connues et qu'elles n'ont guère été relayées après l'évènement de novembre 2018.

De fait, la diplomatie de la conférence conduite par la France traduit aussi une stratégie d'affichage qui n'est pas toujours suivie d'effets. Cet aspect de notre politique pourrait donc être plus soutenu et plus efficient, sachant que la diversité des enjeux traités dans ces multiples initiatives et évènements requiert des moyens qui, parfois, font aussi défaut à l'ensemble de l'appareil diplomatique français.

M. Philippe Latombe, rapporteur. Le RGPD est une création européenne, dont l'impact fut assez fort au sein de l'Union européenne – pour les entreprises, les collectivités, etc. – comme à l'extérieur de l'espace communautaire. Est-ce un outil dont nous devons tirer des leçons pour étendre notre diplomatie et notre influence ? S'agit-il d'un bon exemple, ou considérez-vous que ce qui a fonctionné pour le RGPD ne fonctionnera pas pour d'autres sujets ?

M. Julien Nocetti. Le RGPD constitue à la fois un bon et un mauvais exemple de cette affirmation de l'Union européenne en matière numérique. Il est un bon exemple dans le sens où il entre dans le champ classique des politiques extérieures de l'Union européenne, qui souhaite s'affirmer en tant que puissance par la norme et par le droit. Je fais ici référence à un ouvrage de Zaiki Laïdi, qui présentait l'Union européenne comme puissance normative par excellence. En l'occurrence, on s'est rendu compte que ce RGPD avait « parlé » bien au-delà de nos propres frontières et que certains acteurs – y compris certains États américains – l'avaient lu avec un très grand intérêt, au point d'être allègrement discuté en Chine.

Néanmoins, nous ne devons pas nous reposer sur nos lauriers européens et sur cette mise en avant de nos propres valeurs en matière de données personnelles et de fonctionnement de l'économie numérique en général. En effet, dès l'origine, le RGPD a été amplement contourné par certaines dispositions, notamment par le fameux *Cloud Act* américain, que votre mission d'information n'a certainement pas manqué de questionner durant ses auditions. Cette affirmation européenne est évidemment très positive en ce sens qu'elle participe d'un *soft power* et d'un rayonnement évidemment bienvenus, qui nous font dire que l'Europe compte aussi dans la diplomatie numérique, mais elle est loin d'être suffisante. J'en reviens à l'une de mes précédentes réponses, à savoir que nous devrions chercher à peser de manière plus classique en mesurant bien les rapports de force régissant le champ numérique.

M. Philippe Latombe, rapporteur. Devrions-nous assurer l'extraterritorialité partielle de notre droit, à l'instar des Américains ?

M. Julien Nocetti. Il s'agit également d'une question aux enjeux multiples. Dans la mesure où les Américains utilisent sans fard leur droit à des fins de politique étrangère et à des fins stratégiques, il paraîtrait naturel que l'Europe puisse aussi se doter de moyens juridiques à la hauteur des ambitions qu'elle formule pour son propre avenir numérique, telles qu'elles sont précisées dans le document *Boussole numérique 2030*. De même, dans la mesure où les sanctions internationales constituent désormais l'un des outils privilégiés de la géopolitique, il paraîtrait nécessaire de pouvoir se doter d'instruments d'extraterritorialité.

M. Philippe Latombe, rapporteur. Historiquement, l'extraterritorialité américaine a notamment débuté avec le dollar, qui a permis d'imposer des sanctions à des pays comme l'Iran. Elle a ensuite été étendue au champ économique *via* des possibilités de sanctions contre des banques européennes. Cette extraterritorialité, qui s'est matérialisée dans le conflit économique avec les Chinois, notamment pour les systèmes d'exploitation des smartphones et les semi-conducteurs, pourrait-elle nous impacter à terme ? Pourrions-nous également en être victimes à court terme ? Malgré cette notion d'alliance avec les États-Unis, seraient-ils capables de nous l'imposer de la même manière ? Les sentez-vous en capacité d'agir ? Existe-t-il un véritable risque dans ce domaine ?

M. Julien Nocetti. Le risque est toujours présent. Néanmoins, ma réponse comporte une part de spéculation. Il est toujours extrêmement délicat de se positionner. Lors de la dernière décennie, et notamment sous la présidence de Barack Obama, l'alliance avec les partenaires traditionnels des États-Unis était de rigueur. Pourtant, c'est bien à ce moment qu'ont été votées des sanctions ciblant notamment certaines banques françaises ou certains acteurs de l'énergie, non pas en rapport avec la Chine, mais en rapport avec l'Iran. *In fine*, peu importe le camp politique de l'actuel président américain, puisque ce sont d'abord et avant tout les intérêts nationaux américains – tels qu'édictés par la Maison-Blanche – qui primeront. Le risque politique de sanctions demeure donc très fort et pourrait bien viser les Européens dans certains secteurs critiques. Sous la présidence de Donald Trump, différentes manœuvres et menaces de sanctions ont été brandies à l'encontre de certains acteurs européens. Ericsson a par exemple subi des sanctions en raison de liens supposés avec l'Iran, dans un contexte où les tensions avec Huawei étaient au plus fort, et où le conseil d'administration de Nokia était en plein renouvellement. Ces manœuvres géoéconomiques témoignent donc d'une utilisation sans fard et sans complexe de tous ces outils de politique étrangère. Sanctions et mesures extraterritoriales font partie de l'arsenal américain, dans une logique totalement assumée, indépendamment du parti politique dont est issu le locataire de la Maison-Blanche.

M. Philippe Latombe, rapporteur. France Digitale a attaqué Apple en justice pour des pratiques anti-concurrentielles, arguant du fait qu'il est impossible d'échapper à son monopole, étant entendu qu'Apple est propriétaire à la fois du système d'exploitation et de la

plateforme d'achat des applications. Parallèlement, des questions sur la taille des GAFAM commencent à émerger aux États-Unis. S'agit-il d'une question qui se pose réellement ? S'agit-il simplement d'une menace de circonstance ou s'agit-il d'une voie dans laquelle même les Américains devront rentrer ?

M. Julien Nocetti. La question de la régulation des GAFAM est aussi très sensible aux États-Unis. Je suppose que vous avez en tête le rapport de David Cicilline rendu public à l'automne dernier, du nom de ce député américain porteur de ce rapport très conséquent sur le démantèlement – c'était l'une des conclusions phares du rapport – des géants du numérique, qui fait suite à un travail parlementaire très fouillé sur les pratiques des *Big Tech*. On se rend bien compte que les différentes menaces pesant sur les GAFAM sont évoquées avec plus de bruit qu'en Europe ou dans d'autres régions du monde. Peut-être est-ce en interne et par le pays dont sont originaires ces acteurs que pourraient venir les menaces les plus sérieuses. De même, nous avons tous ici en tête les différentes auditions du patron de Facebook, Mark Zuckerberg, par le Congrès américain. Nous l'avons vu répondre, penaud et parfois livide, aux différentes accusations parfois véhémentes des parlementaires américains.

Cette tendance n'est pas à sous-estimer, car elle ne relève pas seulement d'une scénarisation. Sans nier l'existence d'une part d'affichage politique en interne, il existe indéniablement une insatisfaction par rapport à ce que ces géants du numérique sont devenus. Cette insatisfaction n'est pas nécessairement partagée par toutes les tendances politiques, mais l'aile la plus à gauche du parti démocrate soutient des positions extrêmement virulentes vis-à-vis de ces acteurs, comme en témoignent notamment les propositions de démantèlement soutenues par Elisabeth Warren. La plupart de ces propositions n'ont que très peu de chances d'aboutir, en l'absence de consensus bipartisan sur la majorité des thématiques numériques.

Cela dit, l'enjeu le plus saillant sur lequel ces acteurs pourraient être attaqués est celui du respect de la concurrence, que le législateur américain a toujours à cœur, suite à des décennies de pratiques déjà éprouvées dans ce domaine. Il ne serait pas surprenant qu'un acteur comme Facebook, aussi majeur soit-il, finisse par être scindé, pour des raisons concurrentielles, mais aussi politiques, en plusieurs entités, sachant que ce sujet fait l'objet de discussions répétées au sein même des États-Unis. En tout état de cause, cette possibilité ne relève pas du simple fantasme.

Il conviendra donc de scruter, avec l'installation progressive de la nouvelle administration, l'expression de différentes tendances en son sein. La vice-présidente Kamala Harris ne disposera-t-elle pas d'une voix politique plus importante d'ici un ou deux ans ? Personne ne le sait à l'heure actuelle, mais qui nous dit que son propre regard sur les GAFAM ne va pas l'emporter ? Nous savons qu'elle nourrit plutôt, de par son expérience d'élue californienne, une forme de proximité avec la défense des intérêts de ce secteur, qui est au demeurant tout à fait classique. Quoi qu'il en soit, nous sommes à un moment charnière. L'administration Biden va désormais se concentrer sur des questions de politique intérieure, et il est vrai que cette insatisfaction et ce poids politique démesuré acquis par les GAFAM ne laisseront pas d'autres choix au législateur américain que d'agir dans les quatre ans à venir.

M. Philippe Latombe, rapporteur. Ne sont-ils pas en train de recréer d'autres formes de conglomérats aussi puissants, par exemple en confiant à Elon Musk l'activité spatiale, la reconquête industrielle automobile américaine et la distribution de réseaux Internet par satellites ? *In fine*, n'est-ce pas l'histoire sans fin des États-Unis que de détruire d'importants conglomérats – de type Standard Oil – pour en créer d'autres en parallèle ? Devons-nous nous y habituer ? Avec les Chinois qui construisent eux-mêmes leurs propres conglomérats, nous nous retrouvons aujourd'hui avec les GAFAM d'un côté et les BATX de l'autre, mais nous

pourrions tout aussi bien, à l'avenir, retrouver de grands complexes industriels et numériques américains à la Elon Musk et leurs équivalents chinois.

M. Julien Nocetti. La question est éminemment complexe et politique. D'ailleurs, parmi les nombreux exemples américains, vous avez omis de mentionner Amazon.

M. Philippe Latombe, rapporteur. Bien sûr, j'aurais pu citer Amazon.

M. Julien Nocetti. Cette omission est très intéressante. Bien souvent, lorsque l'on évoque ces grands acteurs du numérique, il existe – j'ignore pourquoi – une forme d'impensé vis-à-vis d'Amazon, alors que c'est peut-être l'acteur sinon le plus menaçant, du moins le plus tentaculaire de ces GAFAM. Amazon est devenu la place de marché par excellence et fait peser des risques très concrets au plan macroéconomique et microéconomique, impactant les questions d'équilibre des territoires au sein de ses différents pays d'implantation.

Comme vous l'avez justement décrit, nous faisons face à un mouvement de reconstitution d'acteurs monopolistiques. L'exemple d'Elon Musk avec Tesla et SpaceX est très clair. Nous pourrions aussi parler de Facebook et de ses ambitions – qui ont été discrètement annoncées – de production de semi-conducteurs. De même, Google et Facebook sont très présents, depuis quelques années, dans le tirage de câbles sous-marins. Nous avons donc affaire à des acteurs qui ne se contentent plus du tout d'être la grille de lecture sur le monde de la jeunesse connectée – pour Facebook – ou le moteur de recherche incontournable sur le web – pour Google, puisque ces acteurs entendent également maîtriser l'infrastructure. Cette quête passe par différentes ambitions dans divers secteurs. À ce titre, le spatial est sans doute le secteur qui nous révèle le côté le plus ambitieux – voire mégalomane – de leurs aspirations. Pour sa part, l'Europe dispose d'assez peu de moyens pour répondre à cet enjeu.

M. Philippe Latombe, rapporteur. Devons-nous chercher à agréger des acteurs pour leur permettre d'atteindre une taille critique ? Dans la compétition de demain, pourrons-nous survivre avec des entreprises de taille intermédiaire (ETI) face aux grands groupes construits par nos concurrents – j'emploie à dessein le terme *« concurrents »*, et non le terme *« adversaires »* ? Je précise que ma question couvre aussi bien le volet économique que la logique de stratégie d'influence.

M. Julien Nocetti. Dans la mesure où les équivalents de Facebook, Google et consorts n'existent pas en Europe, et dans la mesure où il serait inutile de les imiter, nous devrions plutôt privilégier des logiques d'intégration au sein de grands groupes déjà présents dans les différents secteurs industriels : défense, aéronautique, ferroviaire, etc. C'est plutôt à partir de ces grands groupes que nous devrions penser l'intégration de différentes capacités numériques au sens large. Du moins, c'est par ce type d'acteurs – je ne mentionnerai aucun nom aujourd'hui – que les Européens pourront peser à l'international. Ce n'est pas par le biais d'un éventuel Google européen – toutes les tentatives en la matière ont échoué – que l'Europe pourra essayer de défendre ses positions, mais par l'adaptation des grands acteurs industriels traditionnels. En tout cas, c'est ainsi que je vois les ambitions européennes se matérialiser.

M. Philippe Latombe, rapporteur. Dans une vision prospective, à quoi ressemblera le numérique d'ici cinq ou dix ans ? Aurons-nous franchi de tels paliers technologiques que ce que nous connaissons aujourd'hui ne sera plus du tout d'actualité à moyen terme ? Ou serons-nous dans la continuité de ce qui existe aujourd'hui ? *In fine*, à quoi devons-nous nous préparer, et quelle étape suivante devrions-nous d'ores et déjà commencer à intégrer ?

M. Julien Nocetti. Comme je l'évoquais dans mon propos liminaire, nous devons bien mesurer l'accélération phénoménale à laquelle nous avons été confrontés depuis à peine dix

ans. En l'espace de quelques années, la décennie 2010 a été marquée par le franchissement de certaines étapes vertigineuses en matière de numérique et de technologies. Ce rythme effréné va-t-il se poursuivre à horizon de cinq ou dix ans ? De la réponse à cette question dépendront un certain nombre de paramètres.

Je pense d'abord à un paramètre souvent négligé, qui a pu être rappelé par les patrons de Google ou Microsoft, à savoir nos capacités d'adaptation à nous, citoyens du monde entier, à la magnitude et à la vélocité de ce changement technologique numérique. Il ne s'agit pas de paroles en l'air, mais d'un sujet extrêmement concret. En Europe, et surtout aux États-Unis, où les fractures au sein de la société sont plus nettes et plus mesurables, une partie des insatisfactions prend forme dans les conséquences des changements technologiques. Les principaux thèmes des campagnes présidentielles américaines de 2016 et de 2020 – migrations, travail, rapport à la mondialisation, etc. – étaient très étroitement liés aux conséquences de la numérisation des sociétés, de l'évolution des modes de travail et de tous ces bouleversements technologiques à l'œuvre dans nos sociétés globalisées.

Bien que nous ayons tendance à occulter ce paramètre socio-économique, nous devrons le suivre de manière très stratégique et très politique dans les cinq à dix années à venir, sachant que ces changements technologiques suivent un rythme très véloce, qui plus est avec une extension du champ numérique. Je mentionnais précédemment l'ampleur prise par les questions et les enjeux de l'intelligence artificielle, des réseaux 5G déployés à grande échelle, qui impliqueront des enjeux de libertés fondamentales à l'ère numérique, des enjeux de surveillance – que nous avons malheureusement pu mesurer depuis la crise sanitaire – et des enjeux stratégiques, au sens où les grands acteurs de cette planète technologique n'auront aucune pudeur à s'affranchir des règles de bon comportement et défendront leur propre pré carré et leur propre stratégie. Je ne le dis pas pour m'inscrire dans une posture pseudo-réaliste, mais pour tenter de dessiner une lecture qui se distancie d'une certaine forme d'ingénuité par rapport à ces enjeux. Nous sommes bien dans une logique de rapports assez bruts, et tous les phénomènes que nous pouvons observer depuis quelques années seront nécessairement amplifiés dans les années à venir. Il s'agit donc d'acquérir une compréhension extrêmement fine de ces enjeux, en particulier – c'est l'objet de votre commission et de vos travaux – de ces enjeux de souveraineté extrêmement puissants.

M. Philippe Latombe, rapporteur. Vous considérez que le numérique modèle la société, mais pas nécessairement au même rythme pour tout le monde, ce qui peut générer, au-delà de la fracture numérique en tant que telle, une fracture sociale ou sociétale liée au numérique. L'opposition manifestée en France à l'encontre de la 5G et du développement de cette nouvelle technologie en est-elle un exemple ou relève-t-elle simplement de l'épiphénomène ? Pensez-vous qu'une partie des sociétés s'opposeront à ce rythme de transformation ? Quelles en seraient les conséquences géopolitiques et géostratégiques, notamment du côté chinois ou américain ? Aux États-Unis, la dernière élection présidentielle nous permet de mesurer globalement l'étendue du rapport de force. Du côté chinois, hormis quelques révoltes à Hong Kong, le phénomène est difficile à mesurer. S'agit-il également d'une menace pour Pékin ? Comment le pouvoir chinois perçoit-il cet enjeu ? Va-t-il ralentir le rythme de transformation de la société chinoise, ou au contraire l'accélérer pour obliger tout le monde à suivre ?

M. Julien Nocetti. Je répondrai en deux temps, en tenant compte des deux dimensions que vous avez évoquées. Je mets de côté la Chine, sur laquelle je reviendrai dans quelques instants, pour commencer par ce premier enjeu plus sociétal. *In fine*, un développeur de San Francisco partage davantage de points communs avec un fondateur de start-up de Bangalore, un capital-risqueur de Londres ou un hacker de Saint-Pétersbourg qu'avec ses propres

concitoyens du Midwest américain. Bien entendu, il s'agit de l'exemple américain, qui est très particulier. Néanmoins, les mêmes fractures territoriales, urbaines et géographiques sont à l'œuvre en France, ainsi qu'au Royaume-Uni, où les fractures sont encore plus marquées qu'en France. Ces fractures sont profondément travaillées par le numérique, par notre dépendance au numérique et par l'emprise de certains acteurs, à commencer par Amazon. C'est un paramètre sur lequel je souhaite mettre l'accent.

Pour ce qui est de la Chine, nous exerçons, depuis notre continent européen, un regard très distancé et sans doute très monolithique et très vertical sur cette Chine numérique. Deux paramètres sont à prendre en compte.

D'abord, les plans quinquennaux et les grandes ambitions et stratégies chinoises en matière d'intelligence artificielle, de numérique ou de semi-conducteurs ne sont pas tous couronnés de succès. Pékin recourt aussi à une stratégie déclaratoire très visible, à laquelle nous donnons beaucoup d'échos, et qui est relayée par les États-Unis, qui en développent une forme d'anxiété. Malgré tout, certains grands plans chinois – notamment dans l'industrie automobile – ont échoué, témoignant ainsi de l'absence de certitudes quant à la réussite de ces grandes ambitions chinoises, qui se heurtent parfois à l'absence de capital humain et d'expertise dans certains domaines de pointe. J'en reviens ici à cette dimension humaine que nous avons longtemps occultée sur les enjeux de numérique, notamment dans le domaine de la cybersécurité.

En outre, la Chine est épisodiquement marquée par l'émergence de contestations. Il est difficile d'y voir parfaitement clair, mais le pouvoir chinois fait parfois face à des foyers de contestation liés à une crise écologique, un accident ferroviaire, sans compter les évènements très particuliers de Hong Kong, dont l'impact fut retentissant. En tout état de cause, le numérique sert aussi aux citoyens chinois, qui ont développé une forme d'ingéniosité en tentant de contourner les mots et termes censurés, et qui emploient tout un vocable dédié afin de contourner cette grande muraille et ce pare-feu à la chinoise, dont le caractère monolithique est effectivement indéniable. Ne sous-estimons donc pas les réponses et les capacités de mobilisation des populations chinoises face aux initiatives très verticales de Pékin.

M. Philippe Latombe, rapporteur. Nous consacrerons une partie de nos auditions à l'éducation et à la formation, de même qu'au sujet plus global du capital humain. Nous avons bien compris le point que vous avez soulevé, notamment en matière de cybersécurité, et nous dédierons une partie de nos auditions à cette thématique de formation, un élément clé du numérique consistant à disposer d'acteurs et d'experts en capacité de produire du numérique.

Audition, ouverte à la presse, de MM. Julien Groues, directeur général, et Stéphan Hadinger, directeur technique, d'Amazon Web services (AwS) *(18 mars 2021)*

Présidence de M. Jean-Luc Warsmann, président.

M. le Président Jean-Luc Warsmann. Nous recevons ce matin les représentants d'Amazon web services (AWS) France : M. Julien Groues, directeur général, M. Stephan Hadinger, directeur technique, M. Laurent Tari, directeur juridique, M. Lionel Benatia, directeur des affaires publiques et Mme Charlotte Baylac, chargée des affaires publiques.

AWS est une filiale d'Amazon née en 2006 et spécialisée dans les services de *cloud computing*, dont elle était, fin 2019, le premier fournisseur français avec 39 % des parts de marché. Vous nous indiquerez l'évolution de ce chiffre depuis. À l'époque, le *cloud* Microsoft détenait 19 % de parts de marché et Google cloud, 9 %.

Nous avons à vous poser de nombreuses questions sur la protection des données face au *Cloud Act*, les tendances du marché actuelles et la numérisation des entreprises françaises, dont beaucoup font appel à vos services.

M. Philippe Latombe, rapporteur. En introduction, j'évoquerai trois sujets sur lesquels nous souhaiterions vous entendre.

D'abord, que recouvre pour vous la notion de souveraineté numérique ? Les pouvoirs publics y consacrent une attention croissante depuis la crise sanitaire. Nous avons entendu, lors de nos auditions, plusieurs définitions de cette notion, que certains rapprochent d'une forme d'autonomie stratégique ou décisionnelle. Je suis curieux du regard qui est le vôtre en tant qu'entreprise américaine implantée en Europe.

Ensuite, comment voyez-vous le marché actuel du *cloud* ? Comment anticipez-vous son évolution, ces prochaines années ? Votre regard sur les pratiques des entreprises privées et des acteurs publics clients de vos solutions nous intéresse également. Quels sont leurs besoins et leurs attentes ? Ceux-ci ont-ils évolué depuis la crise sanitaire ? Pourriez-vous aussi nous parler de l'initiative GAIA-X, dont vous êtes membre, visant à garantir le mutlicloud, la sécurité des données et l'interopérabilité des services ?

Enfin, nous aimerions échanger avec vous sur les différentes initiatives européennes de régulation du numérique, comme le *Digital Services Act (DSA)*, le *Digital Markets Act (DMA)* ou le *Data Governance Act (DGA)*. Comment vous positionnez-vous par rapport à ces différents projets de régulation ?

Que pouvez-nous nous dire de l'enjeu que constitue la protection des données, dans un contexte où l'extraterritorialité du droit américain risque de mettre à mal le respect des garanties offertes par le droit européen ? Comment interprétez-vous le *Cloud Act* dans le cas d'une demande de transmission de données par les autorités américaines ? Qu'est-ce qu'a changé l'arrêt *Schrems* II dans les relations avec l'Europe ?

M. Julien Groues, directeur général d'AWS France. C'est un honneur pour nous de prendre la parole devant vous aujourd'hui. Je propose qu'une fois rappelé brièvement qui nous sommes et ce que nous faisons en France et en Europe, nous évoquions la manière dont AWS joue son rôle dans le renforcement du leadership numérique de l'Union européenne.

Nous nourrissons la conviction que les entreprises françaises doivent avoir la liberté de choisir où elles stockent leurs données, d'en contrôler le contenu et de changer de fournisseur si elles le souhaitent, en optant pour celui qui met à leur disposition la meilleure technologie, dans un cadre compétitif. Cette liberté de choix nous apparaît comme un besoin fondamental de nos clients. Nous ne devons pas la limiter sous peine de freiner ainsi leur innovation.

Je suis convaincu que le *cloud* AWS rend plus souveraines les organisations françaises et européennes, c'est-à-dire plus autonomes, plus compétitives, plus innovantes et mieux sécurisées.

Après plus d'une décennie à développer une application web évolutive, Amazon.com, en tant que détaillant, a pris conscience de sa compétence acquise dans l'exploitation d'infrastructures technologiques et de grands centres de données. L'entreprise s'est alors lancée dans une mission plus vaste : servir de nouveaux clients (développeurs et entreprises) en leur fournissant des services web pour créer des applications sophistiquées et évolutives. Par coïncidence, nous fêtons cette semaine le quinzième anniversaire d'AWS.

Le terme de *cloud computing* désigne la fourniture à la demande de ressources informatiques facturées à l'usage. Au lieu d'acquérir puis d'entretenir leur propre centre de données ou leurs serveurs, des organisations utilisent, en fonction de leurs besoins, des technologies et des services informatiques. On peut comparer le *cloud computing* à la fourniture d'électricité, dans la mesure où les entreprises clientes pressent en quelque sorte un interrupteur pour accéder à des services qu'elles peuvent cesser d'utiliser à tout moment, d'un simple clic de leur part.

AWS assure la gestion et le maintien, dans un environnement sécurisé, d'une infrastructure technologique, à laquelle accèdent les entreprises pour développer rapidement leurs propres applications, celles-ci ne payant que pour la partie de l'infrastructure qui leur est utile.

Nous fournissons, partout dans le monde, à la demande, plus de deux cents services liés à la puissance de calcul, au stockage, aux bases de données, à l'Intelligence artificielle, à l'Internet des objets, aux solutions hybrides, etc.

Au cours du dernier trimestre 2020, AWS a réalisé un chiffre d'affaires de 12,7 milliards de dollars, en hausse de 28 % par rapport à l'année précédente, ce qui porte le chiffre d'affaires annualisé à 51 milliards de dollars.

Depuis dix ans, nous accélérons nos investissements en France pour accompagner nos clients locaux. Nous avons ainsi ouvert, en 2017, en France, une région de *data centres* : à savoir, plusieurs ensembles de centres de données, disponibles pour tous nos clients souhaitant stocker leurs données sur le territoire français ou bénéficier d'une faible latence pour leurs applications.

En France, les équipes d'AWS aident ces clients et partenaires de toute taille (dont les intégrateurs de systèmes et les éditeurs de logiciels indépendants) à passer au *cloud* afin de bénéficier de ces avantages. Nous comptons en France des dizaines de milliers de clients actifs. Nous travaillons avec les deux tiers des entreprises du Next40 et avec plus de 80 % de celles du CAC40. Le recours au *cloud* s'est désormais imposé comme norme permettant aux entreprises de se concentrer sur leur cœur de métier et de réduire leur dette technique.

Il présente cinq avantages principaux :

– l'agilité (la capacité d'allouer rapidement d'importantes ressources en cas de besoin en activant des milliers de serveurs en quelques minutes) ;

– la réduction des coûts (Veolia évalue l'économie liée à la migration de ses bases de données vers le *cloud* à 40 % de ses coûts d'exploitation *ERP*) ;

– l'élasticité (au lieu de fonctionner presque constamment en surcapacité pour faire face aux pics d'activité, nos clients ne payent que pour ce qu'ils consomment réellement) ;

– la capacité d'innovation (qui augmente à proportion de la baisse du coût de l'échec) ;

– la faculté de déployer instantanément des solutions partout dans le monde.

Deux autres raisons poussent un nombre croissant de nos clients à se tourner vers le *cloud* AWS :

– la réduction de l'impact écologique ;

– la sécurité des données et des applications.

En 2020, le *cloud computing* s'est avéré plus important que jamais : il a permis aux entreprises françaises de s'adapter et de limiter les dommages économiques d'une crise sanitaire inattendue. AWS a accompagné ses clients dans la continuité de leurs opérations, la réduction de leurs coûts informatiques, l'invention de nouveaux *business models*, ou encore la croissance de leur activité.

La question de la souveraineté numérique réside au cœur de notre mission d'entreprise. Au-delà de la capacité à réguler le cyberespace et la sphère numérique, la souveraineté numérique suppose d'atteindre une autonomie stratégique dans la sphère numérique, conjuguée à une compétitivité technologique renforcée.

Selon nous, être souverain en matière numérique, c'est avant tout maîtriser les outils qui permettent des choix technologiques autonomes, le développement et le déploiement des capacités et des infrastructures numériques stratégiques, comme l'a expliqué la commissaire européenne Margrethe Vestager.

Notre action en ce sens s'articule autour de trois axes :

– garantir le plus haut niveau de sécurité et de protection des données ;

– respecter la souveraineté de ces données ;

– fournir un accès aux technologies les plus avancées.

M. Stéphan Hadinger, directeur technique d'AWS France. La sécurité et la protection des données sont des piliers de la numérisation de l'économie française et européenne. Rien ne compte plus pour AWS que de protéger les données de ses clients. Nous avons travaillé dur, année après année, pour nous conformer aux normes internationales reconnues.

Nous avons ainsi été le premier fournisseur de *cloud* en 2016 à recevoir la certification C5 en Allemagne. Nous pouvons aussi nous targuer d'une certification

« hébergement de données de santé » (HDS) en France et « *Esquema nacional de seguridad* » (ENS) en Espagne. AWS adhère au code de conduite du *Cloud Infrastructure Services Providers in Europe* (CISPE), une association professionnelle de fournisseurs de *cloud* en Europe, permettant à leurs clients d'évaluer la conformité de leur fournisseur de *cloud* au Réglement général sur la protection des données (RGPD). Nous participons, qui plus est, dans chaque pays européen, à des travaux visant à améliorer la sécurité de nos clients.

Nos nombreuses certifications internationales couvrent l'intégralité de nos clients. Indépendamment de leur taille et de leur secteur d'activité, ils bénéficient de l'ensemble des contrôles requis pour toutes les données personnelles, bancaires ou de santé, même s'ils n'opèrent pas dans ces domaines. En somme, AWS démocratise les technologies de sécurité les plus avancées.

Dans un centre de données classique, un tel niveau de sécurité nécessite un investissement tant financier qu'humain difficile à maintenir dans le temps. Nous l'avons vu avec les affaires récentes de rançongiciels contre les hôpitaux. Ces programmes malveillants s'attaquent d'abord aux organisations dotées des moyens sécuritaires les plus faibles. Le *cloud* d'AWS met à portée de ses clients la meilleure protection contre les dénis de service, l'accès à des systèmes de détection d'intrusion basés sur l'intelligence artificielle et la possibilité de chiffrer les données qu'ils stockent, sans que cela impacte leur performance. Aujourd'hui, certaines entreprises craignent que le chiffrement massif de leurs données ne s'avère difficile ou coûteux. Ce n'est pourtant pas le cas sur le *cloud* AWS où, à titre d'exemple, Engie chiffre plus de 90 % de ses données.

Vous nous avez demandé dans votre questionnaire comment nous anticipons les risques d'incendie. Je suppose que la question est liée aux récents événements de Strasbourg. Nous avons une pensée pour les équipes de cette entreprise qui reste mobilisée pour ses clients, et ne cachons pas notre admiration pour les pompiers intervenus sur le terrain.

Tous les centres de données AWS sont équipés de systèmes de détection (de fumée notamment) et d'extinction des incendies (par l'eau ou par le gaz), placés dans les salles serveurs ainsi que les zones techniques avoisinantes. Dans le cas (rarissime) d'un incendie, les données des clients AWS resteraient accessibles, du fait de l'architecture des régions d'AWS. Celles-ci sont composées d'au moins trois zones de disponibilité, c'est-à-dire trois centres de données. En France, nos trois zones de disponibilité (toutes trois en Île-de-France) sont physiquement séparées les unes des autres et se trouvent dans des zones de risques (quand c'est le cas) différents. Chacune d'elles est conçue pour fonctionner avec un haut degré de fiabilité, indépendamment des autres. Leur interconnexion permet aux clients d'architecturer leurs applications de manière à ce que celles-ci basculent automatiquement d'une zone à l'autre sans solution de continuité.

Un exemple concret illustre cette résilience de nos services. Nous avons lancé, voici quinze ans, un service de stockage en ligne : Amazon S3. Les données y sont répliquées automatiquement dans l'ensemble des zones de disponibilité. Six copies sont ainsi effectuées dans trois centres physiquement séparés.

Au-delà de ces aspects techniques, nous proposons une approche complète en termes de sécurité et de protection des données. Nous respectons la souveraineté des données européennes et comprenons que la liberté de choix soit un besoin fondamental de nos clients. Cette liberté revêt plusieurs formes :

– d'abord celle d'une liberté de mouvement. Ce sont les clients AWS, propriétaires de leurs données, qui décident de leur lieu de stockage et de qui sera autorisé ou non à y accéder. Ils gardent aussi la possibilité de les chiffrer, de les déplacer ou de les supprimer ;

– la réversibilité se réfère à la liberté de changer de fournisseur. Elle implique un compromis entre le coût initial de création d'un système et son coût futur de transfert vers un autre acteur. Nous avons contribué à de nombreuses initiatives, telles que le code de conduite sur le portage des données et le changement de fournisseur de *cloud (Switching Cloud Providers and Porting Data SWIPO)*, facilité par la Commission européenne dans le Règlement sur la libre circulation des données non personnelles. Techniquement, AWS propose de nombreuses solutions basées sur des logiciels libres (en open source), de telle sorte qu'il est peu complexe pour nos clients de transférer ou de répliquer leurs données hors du *cloud* AWS. Nous les y aidons d'ailleurs, car tous les services de synchronisation que nous proposons permettent l'exportation des données ;

– nos clients sont libres de travailler avec des acteurs locaux. Au-delà des services natifs d'AWS, notre *cloud* permet la mise en place de solutions de type OpenStack, reconnues par le gouvernement français. Nos clients peuvent aussi faire appel à des partenaires français ou européens (Atos ou Devoteam) jouant le rôle de tiers de confiance. Ces sociétés proposent des mesures de sécurité spécifiques au *cloud* AWS, incluant un second niveau de chiffrement des données avec une gestion des clés externalisée. Elles utilisent des boîtiers cryptographiques exploités en dehors des centres de données AWS.

La possibilité pour les clients d'AWS de changer de fournisseur quand ils le souhaitent nous force quotidiennement à toujours leur proposer les meilleurs services en répondant au mieux à leurs besoins.

Nos clients demandent surtout qu'AWS se conforme à la réglementation européenne et au RGPD, ce qui est le cas depuis que ce Règlement a été mis en place. Bien sûr, nous nous adaptons aux évolutions de la réglementation : nous avons récemment renforcé nos engagements contractuels suite à l'arrêt *Schrems* II, en allant au-delà de ce qu'il imposait. Nos nouveaux engagements s'appliquent automatiquement à l'ensemble de nos clients soumis au RGPD, que leurs données soient stockées ou non dans l'Espace économique européen, par le biais d'un addendum consultable en ligne dans nos conditions de service. Nous nous engageons concrètement à :

– notifier à nos clients les demandes d'accès émanant d'entités gouvernementales, européennes ou non ;

– contester ces demandes dès qu'elles entrent en conflit avec la législation européenne ou celle d'un État membre de l'Union européenne, ou qu'un motif de contestation légitime apparaît ;

– au cas où nous serions malgré tout contraints de divulguer ces données, n'en révéler qu'une quantité minimale.

Vous nous avez demandé si notre statut de filiale française ou européenne d'une entreprise américaine nous plaçait hors du champ d'application du *Cloud Act*. Selon notre analyse, le *Cloud Act* s'applique à tous les fournisseurs de services de communication électronique et d'informatique à distance soumis à la juridiction des États-Unis, y compris les filiales européennes de sociétés américaines telles qu'AWS et AWS EMEA SARL.

La plupart des sociétés étrangères opérant aux États-Unis (parce qu'elles y ont une filiale, une succursale, des salariés, ou simplement des clients) sont elles aussi soumises à la juridiction des États-Unis. Soulignons que le *Cloud Act* ne donne pas au gouvernement américain un accès illimité aux données détenues par les fournisseurs de *cloud*.

Habituellement, AWS utilise les outils à sa disposition pour contester les demandes émanant des États-Unis, portant sur une société domiciliée hors de leur territoire. Nous publions d'ailleurs des rapports dressant la liste de telles demandes. Au second semestre 2020, nous n'avons pas livré au gouvernement américain une seule donnée détenue par une société implantée hors des États-Unis.

L'adaptation constante à la réglementation s'inscrit dans l'ADN d'AWS, et c'est dans cet esprit que nous envisageons les législations européennes *(DMA, DSA, DGA)* qui devraient être bientôt promulguées.

Pour renforcer sa souveraineté numérique, l'Union européenne a besoin de règles cohérentes et applicables tenant compte des spécificités des services de *cloud*. Ces règles doivent éviter d'entraver l'innovation et laisser le choix aux clients. Nous partageons l'objectif de la Commission européenne de faire de l'Europe une économie ouverte et numérisée.

M. Julien Groues. La meilleure façon de garantir le succès des entreprises européennes et donc, leur souveraineté, consiste à leur donner accès à la technologie la plus avancée. Les clients ayant migré vers AWS disposent d'à peu près trois fois plus de fonctionnalités, qu'ils fournissent 42 % plus rapidement à leurs propres clients. L'accélération de notre rythme d'innovation permet, *in fine*, à nos clients d'augmenter leur marge de manœuvre financière ou humaine.

Les services *cloud* d'AWS proposent aux organisations publiques et privées une large gamme de services d'intelligence artificielle et d'apprentissage automatique. AWS met ces techniques entre les mains de développeurs, experts ou non en Intelligence artificielle, pour qu'ils créent grâce à elles des robots de conversation, des solutions de recherche automatisée d'enfants disparus dans des bases de données d'images, des méthodes d'analyse et de prévision des besoins de maintenance, de détection de défaillances potentielles dans des chaînes de fabrication ou encore de détection de fraudes dans les transactions financières.

La souveraineté passe aussi par les compétences. Voilà pourquoi AWS soutient de nombreux programmes éducatifs dans les universités françaises. Nous faisons en outre bénéficier des start-up de crédits et d'un soutien technologique. Nous soutenons jusqu'aux personnes éloignées de l'emploi. AWS re/Start utilise ainsi le *cloud* comme un levier de réinsertion et de reconversion professionnelle. Nous travaillons avec des associations locales, des centres de formation et des entreprises partenaires, accueillant les bénéficiaires du dispositif.

Choisir le *cloud*, c'est en outre, à nos yeux, saisir une opportunité responsable et durable de lutter contre le changement climatique. Nous nous engageons à exploiter nos infrastructures le plus durablement possible. Nous avons cofondé en 2019 *The Climate Pledge*, nous engageant à être net zéro carbone dans toute l'entreprise d'ici 2040. Nous sommes en voie d'alimenter notre infrastructure *cloud* mondiale avec 100 % d'énergie renouvelable d'ici à 2025, soit cinq ans plus tôt que l'objectif initialement fixé.

Nous avons économisé plus de 300 000 tonnes d'émission de CO_2 par an, ce qui équivaut à planter 400 millions d'arbres, soit 5,7 arbres par Français. Une étude récente a montré que le passage au *cloud* AWS permet de réduire l'empreinte carbone jusqu'à 88 % ;

notre infrastructure étant trois à quatre fois plus efficace sur le plan énergétique que le centre de données médian.

En conclusion, j'insisterai sur la nécessité de ne pas juger une entreprise sur le lieu d'implantation de son siège social mais sur les garanties qu'elle offre aux citoyens et aux organisations françaises.

Ces derniers mois, et cela m'inquiète, nous avons vu des entreprises ralentir leur mouvement vers l'innovation à cause d'une mauvaise compréhension des réglementations numériques. Il ne faudrait pas que s'ouvre une nouvelle fracture numérique. La sécurité et la protection des données sont la base de la numérisation de l'économie. Nous sommes prêts à la soutenir. C'est là notre rôle.

M. Philippe Latombe, rapporteur. Nous avons reçu la semaine dernière IBM France qui nous a déclaré, en tant que société de droit français, ne pas être soumise au *Cloud Act*. Les divergences d'interprétation sur ce point des grands fournisseurs de services informatiques, de droit américain à l'origine, interpellent forcément nos concitoyens.

Qu'en est-il du *Foreign Intelligence Surveillance Act (FISA)* ? Comment pouvez-vous aujourd'hui matériellement garantir, au-delà d'une pétition de principe, à des sociétés ou des administrations européennes que le gouvernement fédéral américain n'accédera à aucune de leurs données et que ces données sont stockées en permanence sur le sol européen sans que, pour des motifs de sauvegarde, de vérification ou d'entretien des serveurs, elles migrent en tout ou partie vers le sol américain ?

M. Julien Groues. Selon notre interprétation juridique du *Cloud Act*, et bien que nous manquions d'expérience, au vu des rares demandes reçues dans ce cadre, celui-ci s'applique à tous les fournisseurs de services de communication et de services informatiques à distance, y compris les entreprises américaines disposant de filiales à l'étranger. Nous estimons qu'il s'applique, de même, aux filiales des sociétés étrangères opérant aux États-Unis.

Pour autant, ce *Cloud Act* ne donne pas au gouvernement américain un accès illimité aux données. Des contrôles sont mis en place. Nous accordons la priorité à la confidentialité et à la protection des données de nos clients *via*, notamment, leur chiffrement. Seuls nos clients possèdent aujourd'hui les clés de chiffrement de leurs données, sans lesquelles celles-ci sont inexploitables.

M. Stephan Hadinger. Quand l'un de nos clients choisit de stocker ses données dans une région, à savoir une zone métropolitaine, nous nous engageons à ne pas les déplacer. Il est le seul à pouvoir en prendre la décision. Notre certification allemande C5 résulte d'un contrôle précis de ce point. Les données, même répliquées ou sauvegardées, ne migrent pas vers l'étranger.

Nous proposons à nos clients des briques technologiques en self-service. Ce sont donc eux qui contrôlent la localisation de leurs données en décidant, ou non, de les répliquer d'un pays à l'autre.

Le chiffre que j'ai avancé tout à l'heure de zéro donnée transmise au gouvernement américain me semble éloquent. Il atteste l'efficacité de nos mesures de protection (de chiffrement, notamment) face aux demandes. La possibilité pour nos clients de recourir à des mesures de protection additionnelles auprès d'autres fournisseurs (Atos ou Devoteam) leur assure un niveau de contrôle supplémentaire de leurs données.

M. Philippe Latombe, rapporteur. Vous ne répondez pas tout à fait à ma question sur le *FISA*, mais nous y reviendrons. J'aimerais vous entendre à propos de deux affaires à l'origine d'une polémique en France. D'abord, celle des données de Doctolib, apparaissant en clair à un moment de la chaîne. Que pensez-vous des inquiétudes qui ont pu en résulter ?

Votre partenariat avec Bpifrance a suscité beaucoup de critiques. Les comprenez-vous ? Comment en tenez-vous compte ? Par quels arguments factuels les contrez-vous ? Comment percevez-vous, à la lumière de ces deux exemples, l'attitude générale vis-à-vis des *clouds* américains, dont vous faites partie ?

M. Julien Groues. Nous devons aujourd'hui continuer d'informer sur le fonctionnement du *cloud* AWS, sa sécurité, la mise en place de clés de chiffrement et la création d'infrastructures et d'applications extrêmement sécurisées. Les formations et l'apprentissage de ces technologies revêtent une importance cruciale, puisque c'est grâce à eux que le fonctionnement de nos services devient intelligible. Nous passons beaucoup de temps à expliquer à nos clients comment se doter des meilleurs moyens de sécuriser leurs données et, lorsqu'ils le demandent, nous les aidons à architecturer leurs applications en ce sens.

Nous offrons à nos clients (dont Doctolib et Bpifrance) la possibilité d'utiliser les meilleures technologies au meilleur prix tout en protégeant leurs propres clients. Le 17 février, nous avons ajouté un addendum à nos accords de *data processing*, renforçant nos engagements sur le traitement des demandes d'accès aux données. Dans sa décision du 12 mars, le Conseil d'État a examiné ce qu'impliquait, notamment par rapport au RGPD, notre statut de filiale d'un groupe américain, soumise à des lois américaines. Le Conseil d'État a estimé de son devoir de vérifier le niveau de protection des données personnelles en tenant compte de nos garanties juridiques et techniques. Selon lui, nos engagements contractuels contribuent à une protection suffisante des données face à des demandes émanant du gouvernement américain, en plus des mesures de chiffrement prises par nos clients.

Nous devons continuer en ce sens. Il ne faudrait pas que certaines situations freinent aujourd'hui l'innovation. Nous sommes persuadés que, techniquement et juridiquement, nos clients disposent grâce à nous de solutions sécurisées.

Le choix d'AWS par Bpifrance a fait du bruit. Le projet portait sur la mise en place des prêts garantis par l'État. Nous y avons vu une excellente nouvelle pour les dizaines de milliers d'entreprises ainsi soutenues pendant la crise. Quelques inexactitudes ont été énoncées quant au fonctionnement et à la sécurisation de l'application. Bpifrance conserve aujourd'hui la propriété et le contrôle intégraux de ses données. C'est elle qui décide où et comment celles-ci sont stockées et qui y a accès. Par souci accru de sécurité, Bpifrance chiffre en outre ses données, en mouvement et au repos, et conserve le contrôle absolu des clés de chiffrement, sans lesquelles ses données sont inexploitables.

M. Philippe Latombe, rapporteur. Doctolib vous a choisi parce que vous étiez hébergeur de données de santé

M. Julien Groues. Il faudrait leur poser la question, mais je pense que cela faisait partie de leurs critères de sélection.

M. Philippe Latombe, rapporteur. Étonnamment, le Conseil d'État a considéré les données de Doctolib comme des données personnelles mais non à caractère sensible car elles n'étaient pas, selon lui, des données de santé. Nous interrogerons la CNIL sur son

interprétation de ces données ; les différentes catégories de données ne bénéficiant pas du même niveau de protection.

Au-delà des prêts garantis par l'État, il a été question d'un partenariat entre AWS et Bpifrance. Comment percevez-vous le retournement de l'opinion vis-à-vis des géants du numérique américains ? Cette sorte de défiance généralisée vous semble-t-elle totalement infondée ? Viendrait-elle de votre taille ?

M. Julien Groues. Il convient de distinguer la réalité de sa perception. Nos clients se disent ravis de travailler avec nous. Les développeurs adorent utiliser nos technologies pour développer mondialement des solutions innovantes.

Malgré la tendance, en France, à les regrouper, ces sociétés de technologie sont très différentes les unes des autres. Il faut se méfier des simplifications : certaines s'occupent de réseaux sociaux, d'autres, de publicité *via* la recherche, d'autres encore, de création de téléphones et d'applications. Opérant sur des marchés différents, elles apportent des contributions différentes à la valeur.

Le cœur de métier d'AWS reste la fourniture de services *cloud*. Nous investissons énormément en France. Depuis quelques années, nous avons ouvert des bureaux à Paris, Lyon, Toulouse, Nantes, Lille. Nous recrutons chaque année un grand nombre de personnes et servons des dizaines de milliers de clients.

Nous allons poursuivre nos efforts pour accompagner nos clients et les former à l'utilisation des technologies du *cloud*. Celles-ci ont permis aux entreprises françaises de passer au télétravail très rapidement sans solution de continuité. Certains de nos clients ont migré vers le *cloud* en quelques jours sans que leur activité en soit impactée. Ils ont réduit leurs coûts ; leurs techniciens restant dès lors libres de travailler au développement de nouvelles applications. Nous avons répondu aux besoins en puissance de calcul ou en espace de stockage de fournisseurs de cours en ligne, par exemple.

Selon moi, il faut continuer ce processus de formation et d'accompagnement. Les polémiques s'éteindront alors rapidement.

M. Philippe Latombe, rapporteur. On reproche, à AWS, mais non à elle seule, ses méthodes commerciales : vous fournissez facilement des vouchers et, bien que la réversibilité ne pose techniquement pas de problème, du fait de vos conditions tarifaires, il est moins cher de déposer des données chez AWS que de les récupérer.

D'autres critiques vous reprochent un lobbying actif, voire agressif. Le revendiquez-vous ? L'assumez-vous ? Estimez-vous nécessaire de modifier votre fonctionnement pour remédier à une telle perception ? GAIA-X visait à l'origine la création d'un *cloud* souverain européen. Votre appartenance à une telle initiative soulève des questions.

M. Julien Groues. Je reviendrai d'abord sur la partie commerciale de votre question. Aujourd'hui, nous comptons en France des dizaines de milliers de clients. Ils utilisent nos services à la demande et reçoivent une facture mensuelle de ce qu'ils ont consommé, ni plus ni moins, en fonction d'une liste de tarifs publiée sur Internet. Ce sont eux qui choisissent les services qu'ils utilisent et la quantité de données qu'ils stockent. Aucun contrat d'engagement ne les lie à nous. En termes de réversibilité, on ne peut pas faire mieux.

Aucun contrat (de licence ou autre) ne bloque nos clients dans nos infrastructures. Nous appartenons d'ailleurs à des groupes, évoqués par M. Stephan Hadinger, facilitant les

transferts. La plupart de nos technologies sont basées sur de l'open source, ce qui facilite le basculement vers d'autres *clouds*.

Nos clients souhaitent surtout rapidement innover et donc bénéficier dans les meilleurs délais des technologies les plus récentes. On constate, en France et dans le reste du monde, un basculement massif des entreprises de systèmes propriétaires avec licences vers de l'open source. Elles réalisent ainsi des économies tout en renforçant la sécurité de leurs infrastructures, dès lors plus puissantes.

Nos pratiques commerciales bénéficient à nos clients. Loin de les retenir prisonniers de contrats, nous travaillons quotidiennement pour leur donner envie de nous rester fidèles.

L'initiative GAIA-X permet à nos yeux d'associer les entreprises, le monde de la science et de la politique à la définition des standards des nouvelles générations d'infrastructures de données, à la fois ouvertes, transparentes et sécurisées. Nous souhaitons créer ensemble un écosystème numérique ouvert et compétitif de données. Nous avons rejoint GAIA-X pour aider nos clients à continuer d'accélérer l'innovation autour de la donnée. Comme nombre de nos clients y participaient déjà, il nous a semblé logique de les accompagner. Nous œuvrons dans quatre groupes de travail sur :

– les besoins en architecture et en software ;

– les infrastructures opérationnelles ;

– le stockage et le calcul dans le *cloud* ;

– les réseaux et les transferts.

Nous nous concentrons aussi sur les certifications.

M. Philippe Latombe, rapporteur. Vous avez fait part de votre crainte qu'une fracture numérique se creuse, à cause des réticences de certaines entreprises à faire appel à vos services, parce que vous ne seriez pas souverains. Avez-vous conscience que votre taille effraie ? Vous et vos collègues d'origine américaine faites figure d'« ogres ». Cette peur que vous suscitez vient-elle selon vous de votre chiffre d'affaires colossal, propre à donner l'impression que vous tuez la concurrence en vous assurant un monopole ?

M. Julien Groues. Gartner estime entre 5 et 7 % la part de l'informatique dans le *cloud* en France. Toujours selon Gartner, AWS détiendrait 45 % à 47 % de parts de marché dans le *cloud*, un secteur où œuvrent énormément d'acteurs. Les clients peuvent, soit choisir leur *cloud provider*, soit continuer à construire leurs propres centres de données avec des fournisseurs de hardware ou de software. Nos partenaires souhaitent accéder aux meilleures technologies pour en tirer profit. Depuis le lancement d'AWS, voici plus de quinze ans, plus de 80 baisses de prix de nos services ont été constatées, or nous n'en avons interrompu aucun.

M. Philippe Latombe, rapporteur. Je me livre à un rapide calcul : AWS représente 51 milliards de dollars de chiffre d'affaires annuel. Votre objectif consiste-t-il à garder votre part (45 % à 47 %) de ce marché en pleine croissance ?

M. Julien Groues. Notre objectif est de continuer à écouter nos clients et leur fournir le meilleur de la technologie pour qu'ils continuent d'inventer de nouveaux modèles d'affaires. Les start-up comme les grandes entreprises mènent à bien, rapidement, des innovations qui

transforment positivement notre manière de travailler autant que notre mode de vie. Notre culture d'entreprise consiste à les accompagner en ce sens.

M. Philippe Latombe, rapporteur. Comprenez-vous que cela fait peur ? En cas de triplement des entreprises dans le *cloud*, votre chiffre d'affaires exploserait, dépassant éventuellement le budget d'un certain nombre d'États.

M. Julien Groues. Je ne sais pas si cela fait peur. Tant que nous resterons complètement transparents sur nos activités, nous pourrons continuer d'accompagner tout l'écosystème du *cloud* dans sa transformation.

M. Philippe Latombe, rapporteur. Pourriez-vous nous en dire plus sur la partie formation ?

M. Julien Groues. Nous ambitionnons de former tous ceux qui le souhaitent aux technologies du *cloud*. Certaines de nos formations visent les entreprises, véritables viviers de talents en France. Nous aidons leurs employés à s'approprier les technologies du *cloud* pour mieux innover. Nous touchons aussi les intégrateurs, entreprises de services du numérique (ESN), à qui nous transmettons les compétences en matière de bonnes pratiques et de sécurité nécessaires à l'accompagnement de leurs propres clients. Nous formons aussi les étudiants en informatique de manière à ce qu'ils arrivent sur le marché de l'emploi, prêts à contribuer à la transformation des entreprises françaises. Enfin, le *cloud* offre une fantastique opportunité aux personnes éloignées de l'emploi d'apprendre un métier. Nous avons créé voici dix-huit mois le programme re/Start en France. Nous assurons, par cohortes, des formations certifiantes de trois mois, avec Simplon, aux technologies du *cloud* et aux *soft-skills* qui débouchent, grâce à nos partenaires, sur des embauches.

M. Philippe Latombe, rapporteur. Intervenez-vous, dans ce type de formation, sous la marque AWS ? Le nom de votre entreprise y apparaît-il ?

M. Julien Groues. Oui. Nous assurons auprès des enseignants, dans les universités, des formations validées par des certifications, professionnelles ou non, allant de la compréhension du fonctionnement du *cloud* aux meilleures pratiques de sécurité. Dans ce cadre, nous intervenons sous notre nom ou *via* des partenaires certifiés se revendiquant comme des formateurs AWS.

La souveraineté, pour les entreprises et les organisations que nous accompagnons, c'est la possibilité d'explorer de nouveaux marchés et de gagner en compétitivité en bénéficiant du meilleur de la technologie afin de se réinventer en servant au mieux leurs clients.

M. Philippe Latombe, rapporteur. J'apprécierais que vous m'apportiez par écrit une réponse, que j'annexerai au rapport, sur le *FISA*.

Audition, ouverte à la presse, de MM. Olivier Esper, chargé des relations institutionnelles, et Fenitra Ravelomanantsoa, responsable des affaires publiques, de Google France
(18 mars 2021)

Présidence de M. Philippe Latombe, rapporteur.

M. Philippe Latombe, président et rapporteur. Nous recevons les représentants de Google France : M. Olivier Esper, chargé des relations institutionnelles, et M. Fenitra Ravelomanantsoa responsable des affaires publiques.

Google est une entreprise américaine de services technologiques, fondée en 1998 par Larry Page et Sergueï Brin. Filiale de la société Alphabet depuis 2015, elle est présente sur le marché des moteurs de recherche, des applications (avec Android) et du *cloud*, par l'intermédiaire de Google cloud.

Son positionnement avantageux sur ces segments se situe au cœur de notre réflexion, en lien avec notre préoccupation légitime de protection de la souveraineté numérique nationale et européenne.

Pourriez-vous nous indiquer ce que recouvre pour vous la notion de souveraineté numérique ? Les pouvoirs publics y portent une attention croissante depuis la crise sanitaire. Certains l'apparentent à une forme d'autonomie stratégique ou décisionnelle. Quel regard portez-vous, en tant qu'important acteur américain des marchés des moteurs de recherche, des systèmes d'exploitation et du *cloud*, sur les diverses définitions qui lui ont été données ? Comment voyez-vous aujourd'hui le marché du *cloud* ? Comment anticipez-vous son évolution au cours des prochaines années ? Quel regard portez-vous sur les pratiques des entreprises privées et des acteurs publics clients de vos solutions ? Quels sont leurs besoins et attentes ? Ont-ils évolué avec la crise sanitaire ?

J'aimerais aussi vous entendre sur l'initiative GAIA-X, dont vous êtes membre, qui vise à garantir le multicloud, la sécurité des données et l'interopérabilité des services.

Comment, en outre, vous positionnez-vous par rapport aux initiatives européennes de régulation du numérique *(Digital Services Act, Digital Markets Act et Data Governance Act)* ?

J'aimerais enfin vous entendre à propos des enjeux liés à la protection des données, dans un contexte où l'extraterritorialité du droit américain pourrait menacer les garanties offertes par le droit européen. Qu'impliquent selon vous le *Cloud Act* et l'invalidation du *Privacy Shield* par l'arrêt *Schrems* II de la Cour de justice de l'Union européenne (CJUE), notamment en cas de demande de transmission de données par les autorités américaines ?

M. Olivier Esper, chargé des relations institutionnelles Google France. Je commencerai par vous présenter rapidement les activités de Google en France avant que mon collègue ne vous parle du *cloud*, qui vous intéresse plus particulièrement.

Google emploie en France un peu moins de 1 500 personnes basées pour la plupart à Paris. Ce chiffre a doublé depuis trois ans. L'entreprise, en phase d'investissement, a ouvert, en septembre 2018, en plus de son centre de recherche et développement employant déjà des ingénieurs, un centre de recherche en intelligence artificielle. Sa création a été annoncée par le PDG de Google au côté du Président de la République en janvier 2018 à l'occasion du premier sommet Choose France destiné aux investisseurs étrangers.

Ce nouveau centre regroupant une centaine d'ingénieurs a noué des liens avec l'écosystème de la recherche en France par le financement d'une chaire à l'école polytechnique ainsi que par un partenariat avec le *PaRis Artificial Intelligence Research InstitutE* (PRAIRIE) et l'Institut national de recherche en informatique et en automatique (INRIA).

L'activité de Google en France s'axe, en second lieu, autour de la numérisation des entreprises. Nous contribuons à leur présence en ligne par un programme de sensibilisation et de formation baptisé « atelier numérique de Google ». Il cible en priorité les petites entreprises, puisque c'est souvent là que le bât blesse dans la transformation numérique de l'économie. Il vise aussi les étudiants et les chercheurs d'emploi. Lancé en 2012 avec les chambres de commerce et d'industrie, les universités, Pôle emploi et les missions locales, il a déjà formé plus de 500 000 personnes. Il a notamment aidé de nombreux commerces à s'adapter aux confinements lors de la crise sanitaire en passant au « *click and collect* ».

Un partenariat s'est noué dans ce cadre, l'an dernier, avec la Fédération française des associations de commerçants. Exclusivement nomade jusqu'en 2019 (des équipes de Google sillonnaient alors la France), notre programme se déploie désormais aussi depuis quatre ateliers numériques physiquement implantés à Rennes, Saint-Etienne, Montpellier et Nancy.

Une formation à la cybersécurité est venue le compléter l'an dernier, là encore à destination des petites entreprises, en partenariat avec le groupement d'intérêt public cybermalveillance.gouv.fr, que nous avons rejoint, et la fédération de l'e-commerce et de la vente à distance (Fevad). Nous comptons développer dans le même esprit un *massive open online course* (MOOC) en ligne pour toucher encore davantage d'entrepreneurs.

M. Fenitra Ravelomanantsoa, responsable des affaires publiques Google France. Après une présentation de Google cloud, j'aborderai les tendances dans l'utilisation du *cloud computing* sur lequel nous souhaitons mettre l'accent, avant de passer à l'approche, par Google cloud, de la souveraineté numérique.

Département de la société Google, Google cloud n'opère que sur le marché *B to B*, au service, donc, de la compétitivité des entreprises françaises. Nous soutenons l'innovation des petites et moyennes entreprises (PME), des très petites entreprises (TPE) et du tissu associatif. Notre modèle économique, différent de celui de Google, repose sur une souscription payante et implique des engagements spécifiques aux contrats interentreprises.

Google cloud compte plus de 300 collaborateurs à Paris. Le 28 mai 2020 a été annoncée la création de trois centres de données composant une région France pour mieux accompagner le recours croissant des entreprises françaises et européennes au *cloud computing*. Nous avons récemment noué plusieurs partenariats stratégiques contribuant à la transformation numérique d'entreprises comme Renault ou Orange.

La transformation numérique, dont la crise sanitaire a accéléré le besoin, correspond à un enjeu fondamental pour la compétitivité de nos entreprises. Le recours au *cloud* en constitue un pilier : c'est pour optimiser leur compétitivité dans les secteurs, respectivement, de la grande distribution et de l'industrie automobile, que Carrefour ou Renault ont fait appel à Google cloud.

Je soulignerai trois tendances actuelles du *cloud computing* :

–lLe modèle de *cloud* ouvert qui nous tient à cœur distingue Google cloud de ses concurrents. Nous promouvons entre autres des logiciels open source et des *application*

programming interfaces (API) ouvertes pour que nos clients restent libres de leurs choix en se réservant la possibilité de recourir à plusieurs fournisseurs en même temps, d'opter pour un modèle hybride ou de transporter leurs données de notre infrastructure vers une autre ;

– nous facilitons et démocratisons l'accès des entreprises et des organisations à des technologies de pointe (analyse de données ou encore Intelligence artificielle) ;

– nous travaillons à réduire le plus possible notre empreinte environnementale. Nous sommes neutres en carbone depuis 2007. Depuis 2017, nous nous approvisionnons en électricité à l'aide d'énergies renouvelables à 100 %. Nous comptons ne plus recourir qu'aux seules énergies sans carbone à partir de 2030.

Notre philosophie d'entreprise envisage la souveraineté numérique comme la garantie à nos clients qu'ils contrôlent l'accès à leurs données et restent autonomes par rapport aux fournisseurs de *cloud*. Notre positionnement spécifique en faveur des technologies ouvertes facilite l'interopérabilité des systèmes comme des données ainsi que leur récupération à l'issue d'incidents. Le contrôle des données apparaît évidemment comme un enjeu fondamental de la souveraineté numérique. Des réunions avec des décideurs politiques, ces derniers mois, nous ont informés de ce que nos clients attendent d'un fournisseur comme nous en matière de souveraineté numérique. Trois éléments sont ressortis :

– le besoin de décider qui aura accès ou non aux données dans notre *cloud* ;

– la possibilité d'inspecter en toute indépendance ce que font les administrateurs Google des données qui leur sont confiées ;

– la garantie de la survie de celles-ci au cas où nous ne serions plus en mesure d'assurer la continuité de nos services.

En réponse à ces inquiétudes, nous avons défini trois niveaux de souveraineté :

– la souveraineté de la donnée : notre client demeure l'ultime arbitre de l'accès à ses données, grâce au recours à des technologies de chiffrement dont la clé est hébergée hors de notre infrastructure. Nous devons en outre justifier auprès de nos clients nos moindres demandes d'accès à leurs données, qu'ils pourront toujours refuser. Ces technologies s'ajoutent à nos précédentes innovations en matière de sécurité, comme le *confidential computing* permettant de chiffrer les données, non seulement en déplacement et au repos, mais aussi en cours d'utilisation, donc à chaque étape de leur traitement ;

– la souveraineté opérationnelle permet au client de définir des critères de contrôle de la gestion par Google cloud de ses données, imposant par exemple de ne confier celles-ci qu'à des agents de nationalité européenne ;

– la souveraineté logicielle garantit enfin au client la possibilité d'exécuter son environnement *cloud* à court ou moyen terme, même en cas de rupture de service de Google cloud, pour des raisons techniques ou de guerre économique. Cela suppose la mise à disposition de nos clients d'un outil d'orchestration comme Anthos.

Notre approche se concrétisera par le partenariat annoncé en novembre dernier avec OVH cloud, qui pourra dorénavant héberger des produits Google cloud. L'utilisation des technologies de pointe de Google dans l'environnement de confiance d'un acteur français du *cloud* réunira ainsi le meilleur des deux mondes.

M. Philippe Latombe, rapporteur. À quoi le *Cloud Act* vous oblige-t-il, selon vous, en cas de demande du gouvernement américain d'accéder à des données de sociétés ou d'administrations françaises hébergées sur votre *cloud* ? Quelles sont les conséquences juridiques, techniques ou commerciales entraînées, de votre point de vue, par l'invalidation du *Privacy Shield* par l'arrêt *Schrems* II ? Les demandes de vos clients ont-elles changé depuis ?

M. Fenitra Ravelomanantsoa. La localisation d'une donnée ne constitue pas, selon nous, un critère de sa sécurité. Une donnée n'est sécurisée que par les mesures prises en ce sens lors de son hébergement et de son traitement.

Le sujet de la souveraineté numérique n'est pas propre à la France ou à l'Europe. Nous en discutons avec tous nos clients, y compris hors de l'Union européenne.

Quand des autorités adressent à Google cloud une demande d'accès aux données d'un tiers, notre politique est de la soumettre à une équipe de juristes chargés d'en vérifier la validité (sa conformité à la loi, le statut de l'émetteur et l'ampleur raisonnable des données sur lesquelles elle porte). Quand l'un au moins de ces points ne donne pas satisfaction, nous opposons un refus. Nous nous considérons comme des processeurs sous-traitant des données et non comme leur propriétaire. Nous invitons les autorités qui souhaitent y accéder à en formuler la demande directement au client à qui elles appartiennent.

Quand une demande nous semble recevable, nous notifions son exécution à l'entreprise concernée. Dans le cas contraire, nous nous tenons prêts à la contester devant la justice.

Par souci de transparence, nous publions un rapport semestriel des demandes qui nous parviennent. Celles qui visent les entreprises n'en représentent qu'une très petite part et, parmi elles, les demandes suivies d'effet forment une infime minorité. Google cloud n'a communiqué aucune donnée des entreprises de sa clientèle suite à une demande gouvernementale. Nous n'avons en outre identifié aucune demande d'un gouvernement national en vue d'obtenir des informations sur un autre gouvernement national.

Nous sensibilisons la nouvelle administration américaine aux préoccupations de nos clients européens au sujet des lois de surveillance américaines, de manière à trouver une solution constructive au problème posé par les demandes d'accès aux données stockées dans le *cloud*.

M. Philippe Latombe, rapporteur. Je puis admettre que la localisation des données n'entre pas, selon vous, parmi les critères de sécurité. L'invalidation résultant de l'arrêt *Schrems*, les avis rendus par le Conseil d'État et l'affaire Doctolib n'en ont pas moins montré son importance. Pouvez-vous garantir à vos clients le stockage de leurs données dans un pays européen soumis au Réglement général sur la protection des données (RGPD) sans que, pour des raisons de maintenance, de redondance ou de vérification technique, elles soient transférées à l'étranger ?

M. Fenitra Ravelomanantsoa. Nous souhaitons adopter sur ce point la même approche que le RGPD, qui n'a pas interdit mais encadré le transfert de données hors de l'Union européenne. Les travaux résultant de l'arrêt *Schrems* II ont réclamé, au Comité européen de la protection, des recommandations pour que les fournisseurs de *cloud* puissent continuer à transférer des données, dans le respect de normes techniques précises. Leur première version correspond à la manière dont nous sécurisons depuis longtemps le transfert de données et les flux internationaux. Nous attendons leur version définitive pour adapter, si besoin, nos pratiques et nos mesures de sécurité.

M. Philippe Latombe, rapporteur. Êtes-vous en mesure de garantir à une entreprise traitant des données sensibles à caractère personnel que celles-ci seront stockées sur des serveurs européens dont elles ne migreront pas ?

M. Fenitra Ravelomanantsoa. La majorité de nos produits permet à nos clients de choisir le lieu de stockage de leurs données. Sans compter que les mesures techniques que nous mettons à leur disposition leur assurent un niveau de sécurité supplémentaire par rapport à la transmission de leurs données à une autorité étrangère.

Concrètement, nous proposons à nos clients de chiffrer leurs données et justifions auprès d'eux nos moindres demandes d'accès, qu'ils gardent la possibilité de refuser.

Les lois extraterritoriales (notamment américaines) s'appuient sur trois critères pour contraindre un fournisseur de *cloud* à livrer l'accès aux données de ses clients : il faut que le fournisseur de *cloud* contrôle, conserve et possède la donnée. Comme, techniquement, nous n'avons pas connaissance de la clé de chiffrement utilisée par nos clients, ce critère tombe de lui-même.

M. Philippe Latombe, rapporteur. Je ne dis pas cela contre vous, ou pas seulement, mais comprenez-vous que les citoyens, les entreprises et les États s'interrogent sur le traitement des données par les fournisseurs de *cloud* ? Avez-vous d'ailleurs conscience de leurs inquiétudes ?

Un certain nombre de procédures ont été engagées contre vous (par la CNIL, notamment, au sujet des cookies). Votre utilisation des données soulève des questions. Le licenciement par Google de spécialistes de l'Intelligence artificielle a fait grand bruit. Comment l'expliquez-vous ? Par l'incompréhension des citoyens ?

M. Fenitra Ravelomanantsoa. En tant que société américaine opérant en France, nous comprenons évidemment les préoccupations au sujet de la souveraineté numérique et de l'utilisation des données. Nous en discutons régulièrement avec nos clients.

C'est d'ailleurs parce que nous les comprenons que nous mettons sur le marché des technologies innovantes de contrôle garantissant une meilleure protection des données. Notre philosophie d'entreprise nous pousse en outre à travailler en partenariat avec des acteurs locaux pour gagner la confiance de nos clients, libres d'utiliser des produits Google hors d'une infrastructure Google. Nous souhaitons avant tout promouvoir et faciliter la transformation numérique des entreprises françaises en couvrant le plus possible de cas d'usage et en offrant un maximum de fonctionnalités.

M. Olivier Esper. Nous comprenons tout à fait que le succès de nos services implique une surveillance étroite de la part des autorités. Nous nous efforçons de répondre aux préoccupations de manière pragmatique, par des solutions concrètes techniquement innovantes. Nous assurons à nos utilisateurs (le grand public ou les entreprises pour ce qui concerne Google cloud) une parfaite transparence : ce sont eux qui contrôlent leurs données.

M. Philippe Latombe, rapporteur. Le développement de la société Google dans nombre de secteurs, en plus du *cloud*, en amène beaucoup à la juger hégémonique. Il ne s'agit pas là d'une critique. Quel est son objectif de croissance ? Ambitionne-t-elle de multiplier ses secteurs d'intervention dans le champ du numérique ou de se focaliser sur l'un d'eux, comme le *cloud* ou l'Intelligence artificielle ? La question du démantèlement de Google ressurgit régulièrement. Dans quels secteurs continuerez-vous d'investir en France et en Europe ?

M. Olivier Esper. Google a pour objectif de fournir les services les plus utiles et les plus innovants à ses utilisateurs. L'Intelligence artificielle n'est pas une fin en soi mais un outil de développement de fonctionnalités nouvelles. Google s'en tient à une approche responsable de ces innovations.

Google dresse des bilans réguliers de l'application de ses principes éthiques, d'ailleurs rendus publics, et qui tournent autour de la *fairness* (la non-discrimination) de manière à éviter tout biais. L'un de ces principes, valable dans tous les domaines d'intervention de Google, touche à la protection de la vie privée. Des équipes de recherche au sein de la société travaillent à son amélioration par des solutions fondamentales telles que la confidentialité différentielle, l'apprentissage fédéré ou l'apprentissage automatique, sans que les données utilisées quittent à aucun moment le terminal.

M. Philippe Latombe, rapporteur. Vous rendez-vous compte que les citoyens n'en ont pas conscience ? La navigation incognito soulève beaucoup de questions.

Quant à votre éthique, de nombreux entrepreneurs estiment que la même fiscalité devrait s'appliquer à tous. Les Google, Apple, Facebook, Amazon et Microsoft (GAFAM) ne paient pas aujourd'hui leur juste part d'impôts. Vous atteignez un tel degré d'hégémonie que vous tuez l'innovation en l'attirant à vous au lieu de la laisser se développer indépendamment. Je ne vous dresse pas un procès d'intention. Je me contente de vous livrer un ressenti général. Votre discours n'est pas de nature à rassurer.

Comment comptez-vous faire passer votre message auprès des citoyens, des États et des entrepreneurs du numérique ? On vous a reproché vos pratiques commerciales. Le coût pour sortir des données de votre *cloud* s'avère exorbitant rapporté au prix de leur hébergement. Vous distribuez en outre des vouchers aux start-up afin de les capturer parmi votre clientèle. L'intense lobbying des GAFAM, en Europe comme ailleurs, vous a enfin permis de vous introduire dans des projets en principe purement européens comme GAIA-X. Comment répondez-vous à ces critiques ? Quelle preuve avancez-vous que ce que l'on vous reproche ne correspond pas à votre éthique ?

M. Fenitra Ravelomanantsoa. Nous souhaitons mettre en place des partenariats en Europe, conformément aux objectifs de GAIA-X, pour promouvoir l'écosystème du *cloud* et de l'utilisation de la donnée, mais aussi transférer nos connaissances vers des acteurs locaux avec lesquels nous travaillerons. J'ai cité comme exemple notre ambitieux partenariat avec OVH cloud, permettant d'utiliser des produits Google sur un *cloud* français. Nous œuvrons aussi avec Thalès à la mise au point de clés de chiffrement extérieures à notre infrastructure.

Nous avons rejoint l'initiative GAIA-X car nous voulons, nous aussi, que l'Europe dispose d'un service *cloud* de qualité. Nous investissons dans l'Union européenne par la création de quatre nouvelles régions de centres de données, s'ajoutant aux six dont nous disposons déjà. Sur invitation du ministère allemand des affaires économiques et de l'énergie, nous contribuons activement aux groupes de travail techniques de GAIA-X, depuis plus d'un an, leur apportant notre expertise en matière de normes de sécurité et de confidentialité des données.

Notre recours aux technologies ouvertes devrait rassurer quant à notre position hégémonique. Nous nous réjouissons que GAIA-X les promeuve. Nous y voyons un moyen de libérer les clients de leur dépendance par rapport à un fournisseur de *cloud* donné.

M. Philippe Latombe, rapporteur. Sans méchanceté, je vous signale que Google a une très mauvaise réputation en matière de protection des données. Comment pouvez-vous

garantir l'absence de fuite ou de perte des données stockées sur votre *cloud* et votre opposition aux demandes de communication des autorités américaines ?

Vous l'avez dit : le recours au *cloud* pose, par principe, une question de confiance. Comment peut-on vous faire confiance alors que des affaires juridiques médiatisées ont mis en lumière vos défaillances en matière de respect de la confidentialité ? Je songe au procès qui vous a été intenté en Californie à propos du mode de navigation incognito. Le partenariat entre OVH, perçu comme le *cloud* français souverain par excellence, et Google a donné matière à bien des débats dans l'écosystème numérique français. Comment comptez-vous rétablir la confiance ?

M. Fenitra Ravelomanantsoa. Il existe une confusion entre Google et Google cloud, due à la ressemblance entre bon nombre de leurs produits comme Google Drive ou Gmail. Alors que Google s'adresse à des consommateurs, Google cloud se positionne sur un marché *B to B*. Nous veillons à informer nos clients des moyens de contrôle mis à leur disposition, tels qu'une console administrateur, de manière à les rassurer.

Les sanctions prises par la CNIL ne portaient pas sur des produits de Google cloud mais sur d'autres, à destination des consommateurs.

Nous travaillons en toute transparence, par des audits réguliers notamment, à gagner la confiance de nos clients. Nous disposons des certifications les plus strictes en matière de confidentialité, de sécurité et de protection de données.

M. Philippe Latombe, rapporteur. On vous reproche beaucoup une forme d'évasion fiscale vous assurant un avantage sur vos concurrents. Le recours des GAFAM à des montages fiscaux ressurgit systématiquement dans les discussions autour de la confiance. L'écosystème numérique européen estime ne pas lutter sur le marché à armes égales. Certains réclament dès lors, soit d'abaisser la fiscalité européenne, soit de vous y soumettre.

M. Olivier Esper. Rappelons les faits et les chiffres : Google paie la majorité de ses impôts aux États-Unis puisque c'est là qu'elle est domiciliée. Ces dix dernières années, son taux d'imposition global tournait autour de 20 %, ce qui correspond à la moyenne constatée dans les pays de l'OCDE en matière d'impôt des sociétés. Nous entendons parfaitement les critiques visant les règles de fiscalité appliquées aux multinationales. À peu près depuis que l'OCDE a commencé à se pencher sur le sujet, nous soutenons l'idée de réformer le système de fiscalité actuel.

Pour revenir sur les formations que nous organisons, gratuites et agnostiques (c'est-à-dire ne mettant pas en avant de services ni de produits Google), compte tenu de la situation présente, nous y mettons surtout l'accent sur les commerces et la cybersécurité.

M. Philippe Latombe, rapporteur. Vous vous différenciez en cela de vos collègues d'AWS qui, eux, estampillent les leurs.

Audition ouverte à la presse, de M. Bruno Sportisse, président-directeur général de l'institut national de recherche en sciences et technologie du numérique (Inria)
(18 mars 2021)

Présidence de M. Philippe Latombe, rapporteur.

M. Philippe Latombe, président et rapporteur. Nous recevons M. Bruno Sportisse, président-directeur général de l'Institut national de recherche en sciences et technologies du numérique (Inria).

Établissement public à caractère scientifique et technologique (EPST), l'Inria soutient la recherche et l'innovation numérique en France et en Europe depuis cinquante ans. Il rassemble une large communauté scientifique (près de 200 équipes-projets réunissant 3 500 scientifiques). Sans entrer dans le détail de ses différentes actions, je signalerai son rôle central dans la stratégie française en matière d'Intelligence artificielle, son soutien au développement de l'écosystème technologique et enfin son engagement en vue du partage des connaissances et des compétences numériques, *via* le Class'Code notamment.

Je vous poserai d'abord la question rituelle qui ouvre chacune de nos auditions : que recouvre selon vous la notion, assez vaste, de souveraineté numérique ? Les pouvoirs publics y portent une attention croissante depuis la crise sanitaire. Nous en avons entendu de multiples définitions. Certains la rapprochent d'une forme d'autonomie stratégique ou décisionnelle. Comment l'appréhendez-vous personnellement ? Comment l'action de l'Inria contribue-t-elle à la promotion de notre souveraineté numérique nationale ou européenne ?

Je vous interrogerai en second lieu sur les forces et les faiblesses de la France et de l'Europe dans votre domaine de compétence, c'est-à-dire les technologies numériques (*cloud*, Intelligence artificielle, etc.). Votre positionnement d'acteur de la recherche soutenant par ailleurs le développement de start-up technologiques me semble conférer une pertinence particulière à votre point de vue. L'écosystème numérique français rencontre-t-il selon vous des difficultés que nous pourrions contribuer à lever, le cas échéant ?

Nous souhaiterions aussi un point d'étape sur la stratégie nationale en matière d'Intelligence artificielle, où l'Inria joue un rôle clé. Nous n'ignorons pas que les instituts 3IA ont dû faire face à la crise sanitaire dès le lendemain de leur implantation.

Enfin, j'aimerais que nous échangions sur l'une de vos thématiques de recherche : la cybersécurité. L'actualité est régulièrement marquée par la révélation de cyberattaques de plus en plus sophistiquées. La crise sanitaire a donné une visibilité nouvelle aux menaces qu'elles font peser sur la France. Quelles réflexions vous inspirent-elles, tant du point de vue de la formation, de l'acculturation des acteurs privés et publics, qu'en termes de doctrine stratégique, de capacité d'action et de réaction ? Nous aborderons, à partir de là, plus généralement, la transmission des savoirs et des compétences numériques, qui doit constituer une priorité pour notre pays.

M. Bruno Sportisse, président-directeur général de l'Inria. L'Institut national de recherche en sciences et technologies du numérique occupe, du fait de certaines de ses spécificités, une place unique dans le paysage français et européen de la recherche, où il n'existe pas d'autre organisme national de recherche entièrement dédié au numérique. Placé sous la double tutelle des ministères de la recherche et de l'industrie, il porte, de longue date,

une attention soutenue à sa mission en matière de souveraineté. Il repose sur un modèle organisationnel unique d'une extrême fécondité dans le champ du numérique.

L'unité de base n'en est autre que l'équipe-projet. Cette structure de petite taille, groupant quinze à vingt personnes, se concentre sur un projet de recherche et d'innovation, explicité par une feuille de route, pendant une période de quatre ans, à l'issue de laquelle ses travaux sont évalués. Son agilité permet à l'équipe-projet d'avancer sur un sujet précis en produisant des résultats. Elle se prête en outre aux partenariats aussi bien académiques qu'industriels. L'Inria compte 220 de ces équipes-projets, dont 90 % communes aux grandes universités de recherche françaises. Elles emploient près de 3 500 chercheurs, enseignants-chercheurs, ingénieurs, doctorants et post-doctorants, répartis sur neuf centres de recherche dans tout le territoire.

En plus de ces équipes-projets, l'INRIA porte des dispositifs destinés :

– à exercer un impact, notamment économique, sur l'ensemble de la recherche publique, dont nos partenaires ;

– à la production de contenu en ligne massif de type *massive online open course* (MOOC) au travers de l'Inria Learning Lab ;

– au développement de plateformes technologiques (InriaSoft) ;

– à la formation continue au logiciel à destination du tissu industriel avec Inria Academy ;

– et, enfin, à l'accompagnement à la création de start-up technologiques par le biais d'Inria Startup Studio.

L'actualité de l'Inria est marquée par deux dynamiques cohérentes.

La première n'est autre que la signature, le 18 février 2020, par Mme Frédérique Vidal, ministre de l'enseignement supérieur, de la recherche et de l'innovation, et M. Cédric O, secrétaire d'État en charge du numérique, d'un nouveau plan stratégique de l'Inria, sous la forme d'un contrat d'objectifs et de performance couvrant la période de 2019 à 2023.

L'Inria y est présenté comme le bras armé de l'État pour construire, par la recherche, la souveraineté numérique de la nation, comme l'indique le préambule : « l'ambition stratégique de l'Inria est d'accélérer la construction d'un leadership scientifique, technologique et industriel, dans et par le numérique, de la France engagée dans la dynamique européenne. L'Inria doit ainsi assumer qu'il est un outil de la souveraineté et de l'autonomie stratégique numérique de la nation. ». Ce positionnement n'est pas anodin dans le contexte académique aussi bien national qu'international. Quatre axes structurent ce plan stratégique :

– La cristallisation de moyens, en fonction de choix scientifiques, sur des thèmes stratégiques à la composante technologique pleinement assumée : la cybersécurité, une Intelligence artificielle de confiance au bénéfice de notre industrie et l'informatique quantique. À ces thèmes d'actualité dans le plan de relance, s'en ajoutent d'autres, d'application du numérique à la santé et aux objectifs de développement durable. Ceci pose d'ailleurs le problème de la frugalité du numérique et de son empreinte énergétique sur l'environnement ;

– L'Inria doit accorder la priorité à son impact économique sur le tissu industriel français au travers de ses partenariats bilatéraux, de ses équipes-projets communes avec des

industriels français, de la formation continue par le transfert de compétences et, enfin, de son ambition entrepreneuriale renouvelée. L'Inria compte en effet accompagner 100 projets de start-up de logiciels par an à partir de 2023 ;

– L'appui aux politiques publiques passe par le développement d'infrastructures logicielles critiques grâce à des unités conjointes avec des départements ministériels en pleine transformation numérique. Un bon exemple en est le projet pilote Regalia, en appui de la direction générale des entreprises, en vue de la régulation des plateformes numériques. L'Inria assume en outre un rôle d'assistance à maîtrise d'ouvrage auprès de l'administration et notamment auprès de la direction générale de la santé dans sa gestion numérique de la crise à travers le projet TousAntiCovid, piloté par un consortium public/privé inédit. Les opérations menées par le LabIA conjointement avec la direction interministérielle du numérique ont apporté une expertise scientifique et technologique à des projets portés par des départements ministériels et tournant autour de l'Intelligence artificielle. La mission Inria Défense incarne notre volonté de nouer un partenariat ambitieux répondant aux besoins numériques, et plus largement scientifiques et technologiques liés au numérique, du ministère des armées, en accord avec l'Agence de l'innovation de défense et la toute nouvelle Agence du numérique de défense. Ces exemples montrent qu'il n'existe pas de recette unique en matière de numérique pour soutenir les politiques publiques et qu'on ne saurait se passer d'une pluralité d'approches largement expérimentales ;

– L'axe territorial, d'une importance considérable, place l'Inria au service du développement des grandes universités de recherche sur chacun des sites d'implantation de l'institut. Avant l'été, nos centres de recherche deviendront des centres Inria des universités qui les hébergent, ce qui souligne l'intense participation de notre organisme national de recherche à la dynamique universitaire, en matière, notamment, de formation. Celle-ci constitue l'une des clés de construction de la souveraineté technologique.

La seconde dynamique à se manifester dans l'actualité de l'Inria est bien sûr liée à la forte implication de notre institut dans le plan de relance. L'Inria pilote la partie recherche de la stratégie nationale sur l'Intelligence artificielle, tout en s'engageant pleinement dans les stratégies nationales d'accélération où le numérique joue un rôle clé. À ce titre, l'Inria copilote avec d'autres acteurs, comme le Commissariat à l'énergie atomique et aux énergies alternatives (CEA) ou le Centre national de la recherche scientifique (CNRS), les programmes prioritaires de recherche associés aux stratégies nationales d'accélération en matière de cybersécurité ou encore d'informatique quantique. L'Inria copilote également avec le CNRS et l'université d'Aix-Marseille un programme prioritaire de recherche dédié à la transformation numérique de l'enseignement. L'implication structurante de l'Inria dans les réflexions au long cours sur les stratégies d'accélération (et les programmes de recherche associés en cours d'élaboration) en matière de santé numérique, de *cloud* et de mobilité intelligente est parfaitement cohérente avec les perspectives stratégiques ouvertes par notre nouveau contrat d'objectifs et de performance.

En somme, notre actualité entre tout à fait en résonance avec les questions qui agitent la mission parlementaire sur la souveraineté technologique et numérique.

M. Philippe Latombe, rapporteur. Revenons justement sur ce terme de souveraineté numérique (française ou européenne). Quelle définition en proposez-vous ?

M. Bruno Sportisse. Vous avez évoqué la notion d'autonomie stratégique, d'ailleurs inscrite en tête de notre contrat d'objectifs et de performance. J'assimile pour ma part la souveraineté numérique à la capacité de maîtriser le cadre de développement de la société

numérique, les valeurs qui la fondent et les normes technologiques qui la régissent. Je l'illustrerai par quelques exemples, sachant qu'une telle capacité s'étend à tous les domaines.

Dans la sphère privée, où le numérique apparaît fortement lié à la question des données personnelles, la souveraineté numérique implique de savoir qui maîtrise ces données. Elle revient à les encadrer au niveau juridique et législatif. Je songe au Règlement général sur la protection des données (RGPD). L'existence d'un tel cadre, en tant que telle, ne suffit pas. Encore faut-il s'assurer de son application, ce qui ne va pas sans implications technologiques. C'est le sens de notre partenariat avec la Commission nationale de l'informatique et des libertés (CNIL).

Il en est de même dans la sphère de l'éducation, où l'enjeu consiste à déterminer qui accédera aux contenus et aux plateformes. En matière de santé où le numérique joue un rôle croissant dans l'aide à la décision et au diagnostic, la souveraineté implique de décider qui définit les algorithmes utilisés et à partir de quand ces algorithmes d'aide au médecin se substituent à lui dans une partie de son métier. Il s'agit là d'une question éminemment politique, qu'il conviendra de trancher à l'issue d'un débat. Il est en tout cas impératif de maîtriser les technologies en jeu pour apporter une réponse adéquate. Il faut en outre impliquer des acteurs industriels français et européens si l'on ne veut pas se contenter de postures incantatoires. La remarque s'applique à l'ensemble des politiques publiques où le numérique joue un rôle clé en lien avec des données ou l'aide à la décision. Quels sont les outils mobilisés ? Selon quels algorithmes les politiques publiques s'orientent-elles dans telle direction plutôt que telle autre ?

La souveraineté numérique nécessite, selon moi, d'agir dans deux directions.

La première, de laquelle dépend tout le reste, vise à s'assurer un vivier de talents et de compétences. La transformation numérique ne se réussira pas autrement. Du fait que le numérique évolue en permanence, il est nécessaire de se former à ces changements tout au long de la vie. Si j'aborde en premier lieu l'enjeu de la formation initiale et continue, c'est parce qu'il constitue d'après moi la clé de voûte de toute politique à mener dans ce domaine.

Il faut s'attaquer au problème par la base en attirant plus de jeunes vers les filières scientifiques et technologiques, puis en poussant une part significative d'entre eux vers le numérique. Il faut ensuite mettre à profit leur expertise de haut niveau, sanctionnée par des diplômes de master et au-delà, pour construire les prochaines révolutions numériques en évitant la captation des compétences par les Google, Apple, Facebook, Amazon et Microsoft (GAFAM) et les Baidu, Alibaba, Tencent et Xiaomi (BATX). Sans combattants, nous ne mènerons pas la bataille pour la souveraineté numérique.

Nous devons en second lieu diriger notre action sur les infrastructures critiques, dont un certain nombre sont bien connues. On met généralement en avant les moyens de calculs en tant qu'exemple d'infrastructure numérique clé, ce à quoi je souscris entièrement. S'y ajoutent, de mon point de vue, les infrastructures logicielles, moins palpables et moins aisément visualisables que celles que nous avons l'habitude de considérer comme critiques (routes, télescopes, etc.). Concrètement, il s'agit de systèmes d'exploitation, c'est-à-dire de ce qui rend intelligents les terminaux et les smartphones. Nous avons largement abandonné ce terrain au fil du temps, si bien que quelques acteurs dominants du numérique, tels que Google ou Apple, contrôlent aujourd'hui en grande partie les terminaux et leurs fonctionnalités, à travers Android et iOS. Il faudra absolument réinvestir dans ce domaine.

Les boîtes à outils permettant d'œuvrer dans le domaine de l'Intelligence artificielle fournissent un autre exemple d'infrastructure critique. Pour manipuler des données ou utiliser

des algorithmes qui leur apportent de la valeur, il faut des plateformes logicielles. Quelques-unes sont disponibles en open source au niveau mondial. Autour d'elles se constituent des écosystèmes de développeurs de logiciels, de formations et d'entreprises créatrices de valeur.

Bien que ces boîtes à outils soient en open source, celui qui les maîtrise maîtrisera du même coup l'écosystème entier, qu'il pourra orienter dans telle direction plutôt que telle autre, en ayant accès au vivier de compétences. PyTorch fait partie de tels écosystèmes. Facebook y assume un rôle clé. TensorFlow en est un autre et, là, c'est Google qui y joue un rôle majeur. La France a la chance de disposer d'une telle boîte à outils avec Scikit-learn, développée par l'Inria. Il apparaît capital de continuer à soutenir son développement pour rester dans la course. Sinon, demain, ces écosystèmes de compétences en entreprise et de nouvelles perspectives technologiques offertes par l'Intelligence artificielle, passeront entièrement sous le contrôle d'autres acteurs.

Je donnerai un autre exemple d'infrastructure logicielle critique : le futur du web, qui repose sur des technologies logicielles que l'on désigne en général par le vocable de standards ouverts du web. Ces technologies, déterminantes du point de vue de l'interopérabilité, assurent la capacité de naviguer sur la toile. Un certain nombre de standards fixe ainsi un niveau minimal de sécurité des transactions en ligne.

C'est l'organisme de standardisation W3C Europe (World Wide Web Consortium) créé voici une trentaine d'années, et dont je suis moi-même le président, qui les définit en s'appuyant sur trois piliers technologiques : un au Japon, un aux États-Unis bâti autour du Massachusetts Institute of Technology (MIT), et un en Europe qui regroupe des acteurs de la recherche autour de l'Inria.

L'un des enjeux qui se posent actuellement consiste à garantir dans la durée qu'un consortium chargé d'imprimer une direction à l'avenir du web, et donc de décider des valeurs qui le sous-tendront, demeurera dans un cadre multilatéral ouvert, sans passer sous le contrôle d'une poignée d'entreprises. W3C est appelé à déterminer le niveau d'interopérabilité du web et à y imposer des normes en matière de sécurité ou de respect de la vie privée.

De la capacité à mener une politique d'infrastructures logicielles critiques dépend tout le reste. C'est elle qui drainera en effet les talents et les entreprises. Le numérique et sa valeur se construisent autour du logiciel. Pour citer l'un des grands investisseurs de la Silicon Valley, Marc Andreessen : « le logiciel dévore le monde ».

En résumé, celui qui maîtrise les infrastructures logicielles critiques maîtrise l'ensemble de la chaîne de valeur. Le problème vient ici en partie de ce qu'en Europe, l'importance du logiciel n'a, historiquement, pas toujours été clairement perçue.

M. Philippe Latombe, rapporteur. Plusieurs de nos auditions ont porté sur les données de santé. Vous avez vous-même évoqué les algorithmes utilisés dans le domaine de la santé. Faudrait-il nous doter d'un système de validation de tels algorithmes, sur le modèle de ce qui existe déjà pour les médicaments ? Est-il nécessaire de s'en préoccuper dès aujourd'hui ? A-t-on besoin d'une loi pour encadrer ces algorithmes de santé ?

Ces questions valent pour la santé, mais elles pourraient très bien s'appliquer, à terme, à l'Intelligence artificielle. J'ai conscience que ma question porte sur un point très précis mais je profite de nos récentes auditions sur ce thème pour vous la soumettre, puisque vous l'avez mentionné.

M. Bruno Sportisse. Votre question dépasse à mon sens le cadre strict de la santé. Elle revient à s'interroger sur ce que recouvre la notion d'IA de confiance : des algorithmes certifiés, prouvés, validés, s'insérant dans des chaînes de traitement de la donnée. Il faut garder en tête le continuum entre les données disponibles et les algorithmes qui évoluent, justement, en fonction de ces données disponibles et apprennent grâce à elles. C'est l'ensemble de cette chaîne de traitement continue, où l'on assiste à des allers-retours, des échanges et des adaptations entre algorithmes et données, qu'il convient de certifier.

La notion d'IA de confiance s'étend à tout un outillage et à la possibilité de s'appuyer sur des tiers de confiance pour garantir les résultats. Elle englobe aussi des normes et un cadre mis en place par le législateur. Ceci dit, il faut prendre garde, vu la plasticité du numérique et sa rapide évolution, à ne pas lui imposer de règles trop rigides au risque d'empêcher la naissance de l'innovation. C'est là toute la difficulté que pose le numérique : il faut à la fois l'encadrer par souci de transparence, sans pour autant étouffer l'innovation, puisque c'est sur elle qu'il repose, autant que sur la confiance.

Ma réponse s'est éloignée du cadre strict de la santé, dans la mesure où votre question allait elle-même bien au-delà.

M. Philippe Latombe, rapporteur. Pour en revenir aux talents et aux compétences, où doit commencer notre effort ? Les initiatives prises à l'école, au collège, au lycée vous paraissent-elles suffisantes ? Où s'enracine le problème ? Comment amorcer un cercle vertueux qui nous permettrait de disposer des talents et des compétences nécessaires ? Vous paraît-il urgent d'intervenir dès maintenant dans certains domaines ? Quelles actions faudrait-il selon vous mettre en place à moyen et à long terme ?

M. Bruno Sportisse. La question porte sur le flux de compétences qui alimentera l'enseignement supérieur, organisé sous la forme d'une pyramide, dont le sommet correspond aux diplômes les plus élevés.

Elle se pose dans un premier temps pour la base de cette pyramide, qui correspond à ce que les Anglo-saxons appellent *Science, technology, engineering, and mathematics (STEM)* et que nous désignons par le vocable de « sciences dures ». Tout part du nombre de jeunes de l'enseignement secondaire intéressés par les sciences et technologies, où le numérique fait figure de thématique interdisciplinaire liée à nombre d'autres domaines. C'est la désaffection durable des jeunes pour les sciences et technologies qui doit nous interpeller.

L'Inria s'est engagé voici un an et demi auprès du ministère de l'éducation nationale, de la jeunesse et des sports, par un protocole d'accord que j'ai moi-même signé, dans un programme intitulé « Un scientifique - une classe : chiche ! ». L'Inria le pilote avec d'autres partenaires (universités et acteurs de la recherche). Son objectif est que, d'ici trois ou quatre ans, l'ensemble d'une classe d'âge parvenue en seconde ait eu l'occasion d'échanger avec un ou une scientifique (éventuellement ingénieur) du numérique afin de donner le goût des sciences et technologies par le biais, et dans l'intérêt du numérique.

Le programme vise notamment les jeunes filles. Des statistiques montrent qu'elles pratiquent une forme d'autocensure ou, du moins, témoignent d'une désaffection plus marquée pour ces disciplines scientifiques.

On pourrait penser a priori que l'Inria s'éloigne avec ce programme de sa zone de légitimité. Je ne le crois pas, puisque la priorité doit aller à l'élargissement de la base de cette pyramide de compétences. Ce programme est le premier du genre mis en place depuis ma prise

de fonction. Nous avons identifié son objectif de sensibilisation en milieu scolaire comme une préoccupation fondamentale, dont découlera le reste.

Il reste des actions à mener à d'autres niveaux de la pyramide, par exemple, celui des masters dans les domaines touchant aux mathématiques appliquées et à l'informatique. Les entreprises engagées dans la transformation numérique ont, bien entendu, un énorme besoin de talents. Prenons pour hypothèse que, la base de la pyramide une fois élargie, les jeunes poursuivront, en plus grand nombre, un master. Si on ne peut pas garantir qu'une partie de ces diplômés s'engageront dans des travaux de recherche parce que les entreprises, ne pouvant se passer d'eux pour mener à bien leur transformation numérique, les attireront tous à elles, alors nous ne parviendrons jamais à préparer les prochaines révolutions du numérique.

Ce segment du marché du travail connaît une très forte tension. Je ne dis surtout pas qu'il faudrait dissuader des jeunes de rejoindre le monde de l'entreprise. J'ai moi-même été directeur général délégué d'une entreprise de taille intermédiaire du secteur médical en pleine transformation numérique. L'arrivée de talents dans le tissu industriel français relève d'une nécessité vitale. Voilà d'ailleurs pourquoi il faut que tant d'étudiants intègrent des masters. Seulement, si certains d'entre eux ne poursuivent pas une carrière dans la recherche, nous ne serons jamais prêts pour les prochaines évolutions du numérique, qui se renouvelle en permanence.

Si, à un niveau supérieur encore de la pyramide, tous les chercheurs sont happés par les grands acteurs internationaux des nouvelles technologies disposant d'une force de frappe académique comparable, si ce n'est supérieure, à celle de nombreux pays et du secteur public de la recherche, nous ne pourrons pas, là non plus, rester dans la course. Il faut prendre d'autres mesures encore pour que le monde de la recherche continue d'attirer durablement à lui des talents.

Voilà pourquoi je recours à l'image de la pyramide : si la base n'en est pas assez large, des difficultés s'ensuivront à tous les niveaux. Voilà pourquoi aussi il faut mener des politiques dans la durée. Gravir tous les échelons de cette pyramide prend une dizaine d'années. Il s'agit en somme de mener un combat sur le long terme impliquant quantité de parties prenantes : l'enseignement secondaire et supérieur mais aussi les entreprises nationales convaincues de l'importance de disposer d'un vivier de talents et d'être accompagnées par des forces académiques. Des alignements collectifs seront nécessaires.

Venons-en maintenant à la formation continue. Beaucoup d'entreprises du secteur des nouvelles technologies sont déjà parfaitement capables de sélectionner des personnes dotées d'un bagage scientifique (pas nécessairement numérique) pour les former à l'ingénierie du numérique. Nous devons de notre côté mettre en place des programmes similaires, sans parler de la formation continue de ceux qui travaillent déjà dans le numérique, un domaine en constante et rapide évolution, où il faut donc s'adapter en permanence. On le voit : la formation continue apparaît comme un domaine clé.

Ces enjeux de formation sont inscrits dans notre contrat d'objectifs et de performance. L'Inria s'intègre complètement aux dynamiques des universités qui, outre leur rôle de premier plan en matière de recherche, ont une totale légitimité à intervenir dans ces domaines. Les standards internationaux constituent en effet un lien entre recherche et formation de ce point de vue.

M. Philippe Latombe, rapporteur. J'entends bien qu'alimenter la base de la pyramide prendra du temps. Pour autant, voyez-vous, dans l'immédiat, des lacunes à combler parmi les compétences et les talents sur lesquels nous devons nous appuyer ? La mise en place

de la politique que vous appelez de vos vœux prendra entre une dizaine et une quinzaine d'années. Repérez-vous dès aujourd'hui des compétences qui nous manqueraient et justifieraient que l'on organise des formations accélérées au cours des deux ou trois années à venir, voire que l'on fasse venir en France des talents à même de nous aider à franchir un cap difficile ?

M. Bruno Sportisse. Je ne pense pas qu'il nous manque des compétences spécifiques dans tel ou tel domaine. Nous devons mener une politique d'attractivité du territoire. Nous y œuvrons notamment dans la première version du plan Intelligence artificielle, au travers d'une action portée par l'Inria et qui s'intitule « Choose France ». Elle consiste en pratique, et nous l'assumons, à cibler les talents que nous attirons en France.

Il ne me semble pas pertinent de chiffrer précisément des besoins en cybersécurité, en Intelligence artificielle, en *cloud* ou encore en robotique, car le numérique touche à de multiples domaines. On note parfois une tendance à le segmenter alors qu'il s'intègre à d'autres champs de compétences. Les grands acteurs des nouvelles technologies américaines ont, eux, bien en tête les implications, en termes de commerce et d'affaires, des dynamiques scientifiques et technologiques du numérique. Je n'ai donc pas envie de cibler telle ou telle sous-partie du numérique, de telles découpes m'apparaissant le plus souvent artificielles.

En résumé, il convient de mener dès aujourd'hui, ce que nous faisons d'ailleurs, des actions inscrites dans une dynamique internationale en vue de l'implantation en France de talents et de compétences. Des actions de formation continue, souvent perçue comme le parent pauvre de l'enseignement en France, sont également en cours. J'ai déjà évoqué l'initiative de l'Inria en la matière. Il faut savoir inventer, avec des entreprises, des actions pour que des compétences scientifiques puissent évoluer vers des compétences numériques. Je suis extrêmement impressionné par les programmes mis en place dans cet esprit par certains grands éditeurs de logiciels, qui transforment des physiciens, des chimistes ou encore des mécaniciens désireux de changer de branche en développeurs et en ingénieurs du numérique.

Il me paraît par ailleurs important de ne pas s'en tenir à l'idée d'un mur à construire. C'est à mes yeux le flux qui compte. J'ai conscience que tout le monde ne partage pas ma position, mais je ne m'inquiète pas particulièrement d'une fuite des cerveaux, de la recherche publique, vers d'autres acteurs. Il me semble surtout crucial de veiller au maintien constant d'un flux entrant. Il est normal qu'il existe en contrepartie un flux sortant et aussi un flux de mobilité au bénéfice d'un tissu industriel, que j'espère en premier lieu français puis européen. Ce n'est pas en élevant des cloisons que nous résoudrons le problème mais en augmentant les flux, qui devront atteindre un équilibre entre les entreprises et la recherche publique. Les positions que celles-ci partagent apparaissent, dans ce contexte, déterminantes. Plusieurs dispositions récentes, telles que la loi relative à la croissance et à la transformation des entreprises (loi PACTE), facilitent heureusement leur entente.

M. Philippe Latombe, rapporteur. Au sujet de la formation continue, vous avez rappelé que des éditeurs de logiciels sélectionnent des scientifiques aux profils divers pour en faire des développeurs. Vaut-il mieux les laisser agir indépendamment les uns des autres ou vous paraît-il préférable de structurer leurs initiatives ?

M. Bruno Sportisse. Il faut selon moi structurer la filière. Des programmes comme ceux que vous évoquez me semblent une bonne chose. Il ne m'en paraît pas moins bon de les organiser plus systématiquement.

Le sens de ma remarque était que, puisque de grands éditeurs de logiciels parviennent à mener à bien des actions de formation continue, alors il doit être possible de généraliser leurs efforts.

M. Philippe Latombe, rapporteur. La population dispose-t-elle aujourd'hui, selon vous, d'un niveau de connaissances suffisant sur le numérique ? Le terme de fracture numérique a d'abord une acception territoriale, mais n'observe-t-on pas aussi une fracture au niveau des usages et de la compréhension du numérique ?

M. Bruno Sportisse. Je suis entièrement d'accord avec vous. Une politique de souveraineté repose à mon avis sur une dynamique d'innovation, qui repose elle-même sur des viviers de compétences et sur la capacité à comprendre ce que sont les infrastructures technologiques critiques. Il faut aussi s'appuyer sur un consensus politique et citoyen à ce sujet.

C'est en tout cas ce qu'a montré l'année qui vient de s'écouler dans le contexte très particulier de la crise sanitaire. J'ai déjà eu l'occasion de m'exprimer, lors d'auditions devant le Parlement, sur les outils numériques mis en place à cette occasion. Je songe au projet TousAntiCovid que l'Inria a eu l'honneur de piloter auprès de la direction générale de la santé. Il a été mis en œuvre dans un contexte de souveraineté de la politique sanitaire. Il faut être capable de déterminer dans quelles conditions on déploie un tel outil et selon quels paramètres, en s'appuyant sur l'expérience tirée de la gestion de la crise par la France. L'adoption de ces outils par la population s'avère évidemment décisive. On ne peut construire de la souveraineté technologique que sur la base d'un consensus politique et citoyen, c'est-à-dire, qu'à condition que les enjeux du numérique soient bien perçus.

Il faut comprendre ce qu'est le web et ce qui se joue derrière, qui le contrôle et ce qui se passe dans un smartphone. Il faut aussi mesurer l'enjeu du respect de la vie privée et ce qui se cache derrière les mots pompeux de gouvernance algorithmique. Le numérique est présent dans de multiples domaines de la vie quotidienne. Nous avons parlé du rôle des algorithmes dans la santé. Il est capital de savoir qui les détermine. En somme, il faut communiquer sur les enjeux du numérique et les arracher à la sphère de ceux qui détiennent le savoir, à la sphère technologique. Le numérique s'immisce aujourd'hui dans les moindres aspects de notre vie. Qu'est-ce qui se joue à travers le choix d'un outil de visioconférence ? Qu'est-ce qu'implique le recours à Zoom ? Le partage des enjeux du numérique, qui fait désormais partie du quotidien des entreprises et intervient jusque dans les politiques publiques, doit déboucher sur leur compréhension pour que la notion de souveraineté numérique ne s'apparente pas à un bombage de torse ou un concept creux. Elle recouvre en réalité des éléments très concrets.

C'est d'ailleurs la raison pour laquelle, au titre de mes fonctions à l'Inria, suite à un retour d'expérience sur le projet TousAntiCovid, j'ai pris la décision de faire de l'année 2021 celle du dialogue entre les sciences et technologies, et la société, autour du numérique. Je n'aime pas ce terme de dialogue, car les sciences et technologies ne se situent pas hors de, mais bien dans la société. Ceci dit, je n'en dispose pas de meilleur. Voilà en tout cas l'autre pilier de la construction d'une souveraineté technologique, en plus d'une politique d'innovation menée en cohérence avec des acteurs industriels et l'État.

Il reviendra ensuite à la société d'opérer des arbitrages, selon l'importance qu'elle attachera à l'autonomie stratégique et aux enjeux associés. Quoi qu'il en soit, le partage des enjeux du numérique et la compréhension de ce qu'il signifie ne me semblent pas complètement étrangers à la question de la sensibilisation en milieu scolaire évoquée tout à l'heure. Il faut sortir ces problématiques d'un cercle de spécialistes et des milieux d'affaires et dissiper les écrans de fumée dont les entourent certains acteurs du numérique.

La société m'y paraît aujourd'hui préparée. Voici dix ans, dans d'autres fonctions, j'ai été frappé par l'idée fort répandue, jusque dans les états-majors, que le numérique se résumait à une affaire de tuyaux. Le milieu entrepreneurial n'était pas forcément conscient alors qu'avec le numérique se jouaient la maîtrise de la chaîne de valeur, les modèles économiques des entreprises, la relation au client, les cycles d'innovation et de conception des produits et des services, et jusqu'aux politiques en matière de ressources humaines. Voici dix ans, soulever la question du numérique renvoyait encore à une simple consultation avec la direction des services informatiques.

Nous sommes évidemment sortis de cette situation. Il faut étendre une telle évolution au reste de la société, faute de quoi nous ne parviendrons jamais à un consensus sur le sens à donner à la notion de souveraineté numérique. Ce terme pour l'heure encore assez vague n'est pas exempt de connotations péjoratives, à en juger par les dernières tentatives de l'affirmer, pas vraiment couronnées de succès.

Il me paraît fondamental de lui donner une signification, dans la vie quotidienne, qui permette d'en mesurer les enjeux.

M. Philippe Latombe, rapporteur. La France a fait avec TousAntiCovid (à l'origine StopCovid) un choix singulier, la distinguant de certains de ses voisins européens. Existe-t-il des divergences en Europe, aussi bien dans la définition de la souveraineté que dans une forme de soumission (ou de refus de soumission) ou encore dans le développement de solutions ? La France a choisi de se passer des briques iOS et Android, contrairement à d'autres pays. Un tel choix vous semble-t-il révélateur et, si oui, de quoi ? Faut-il en déduire que nous peinerons en Europe à nous accorder sur une vision commune de ce type de sujets ?

M. Bruno Sportisse. La problématique de la souveraineté touche à la volonté politique et la capacité aussi bien de parvenir à un consensus citoyen et politique sur l'ensemble des enjeux que de se donner les moyens de ses ambitions. TousAntiCovid l'illustre parfaitement. Des acteurs industriels et des instituts de recherche s'y sont impliqués ensemble. Ils disposaient des moyens de réaliser leurs ambitions. Celles-ci étaient certes limitées car, dans le cas contraire, nous ne débattrions pas de souveraineté numérique. Cela étant, sans recherche, notamment sur les protocoles ayant permis la création de StopCovid, aucune application mobile n'aurait vu le jour.

La souveraineté numérique suppose donc d'avoir investi dans une politique de recherche et d'innovation. Je répondrai donc à votre question en vous confiant mon sentiment qu'une telle ambition existe bel et bien au niveau européen.

En vertu d'un hasard du calendrier, ce matin a été officiellement lancé le Conseil européen de l'innovation *(European Innovation Council, EIC)*, qui existait en réalité depuis déjà deux ans à l'état de prototype. J'ai l'honneur de siéger à son conseil consultatif et il se trouve que j'ai pris part à sa conception, voici deux ans et demi, dans une mission que m'avaient confiée les ministres Frédérique Vidal, Bruno Le Maire, Mounir Mahjoubi et Florence Parly, à la suite du discours du Président de la République, dit de la Sorbonne, où il appelait de ses vœux la création d'une agence européenne de l'innovation.

Ce Conseil européen de l'innovation assume parfaitement son positionnement d'outil de la souveraineté technologique européenne, selon une ambition d'ailleurs rappelée par les commissaires ou la présidente de la Commission européenne. Le Président de la République, dans son allocution, ce matin, a lui aussi parlé de souveraineté technologique au travers de la planification technologique.

La volonté d'une souveraineté numérique existe selon moi. Seulement, elle doit s'incarner dans des projets concrets. Une période de crise sanitaire ne fournit pas le contexte le plus favorable pour la traduire sereinement dans la réalité et dans la durée. Ceci passera par des actions très concrètes. Nous avons évoqué le plan de relance et l'informatique quantique. Qu'adviendrait-il, en termes de cybersécurité, au cas où un ordinateur quantique verrait le jour ? Il n'est pas envisageable que la France ou l'Europe quittent la course engagée pour garder la maîtrise d'outils de cybersécurité. Il faut s'attaquer à un tel enjeu au niveau français, en coordination avec des partenaires européens.

J'ai évoqué un peu plus tôt les infrastructures logicielles de l'IA. Elles aussi doivent figurer sur des feuilles de route technologiques conçues avec des partenaires européens. Le lancement d'un Conseil européen de l'innovation apporte déjà, en soi, un élément de réponse. En assumant sans ambiguïté l'importance des technologies et des feuilles de route technologiques, il prouve notre capacité à avancer sur de vrais projets.

M. Philippe Latombe, rapporteur. Vous ne souhaitez peut-être pas répondre à ma question, mais, selon vous, pourquoi la France n'a-t-elle pas réussi à entraîner avec elle dans les projets StopCovid ou TousAntiCovid au moins quelques-uns des pays qui l'entourent ? Cet échec s'explique-t-il par l'urgence générée par la crise sanitaire ? Le temps nous aurait-il manqué de soulever toutes les questions voulues et de bâtir ensemble un projet convaincant ? Ou, au contraire, une volonté existait-elle, chez les Allemands notamment, d'opter pour des solutions différentes ?

M. Bruno Sportisse. Je rappellerai d'abord que StopCovid et TousAntiCovid reposent sur des technologies franco-allemandes issues d'un important projet mené au titre d'un programme européen, monté en quelques jours, avec l'ensemble des acteurs européens, autour d'une collaboration de l'Inria avec l'institut Fraunhofer-Gesellschaft. Les protocoles qui en ont résulté sont donc issus de travaux de scientifiques français et allemands.

Par la suite, plusieurs gouvernements souverains ont résolu de privilégier d'autres solutions. Une multiplicité de facteurs sont entrés en jeu. Le contexte d'une crise sanitaire, contraignant à prendre, en l'espace de quelques jours ou semaines, des décisions de poids, ne prédisposait pas à un tel exercice. Par ailleurs, il ne m'appartient pas de commenter les décisions prises par chaque pays. Il me paraît plus intéressant de poser la question à froid, ce pourquoi j'ai rebondi sur le terme de planification technologique employé par le Président de la République dans son discours en honneur du lancement de l'*EIC*.

Il faut que de grandes feuilles de route technologiques prennent en compte les enjeux que nous devrons affronter au cours des années qui viennent. Celui de l'informatique quantique prendra sa pleine mesure d'ici cinq à dix ans. Quand on parle d'IA de confiance sans se contenter d'effets d'annonce un peu creux, il faut bien songer que se tiennent derrière des socles technologiques et des chaînes de traitement des données couplées à des algorithmes maîtrisés de bout en bout. Des normes et des standards devront encadrer ces technologies. N'oublions pas non plus que les systèmes de détection en cybersécurité, dont nous devrons nous équiper avec nos partenaires, reposent sur des infrastructures logicielles.

La nécessité d'établir des feuilles de route communes sur ces sujets a, selon moi, bien été perçue. Des partenariats se mettront en place, car la volonté d'y parvenir est présente. Les acteurs à mobiliser sont déjà là. Il est enfin admis que parler de souveraineté technologique et de technologie, et des modes d'intervention requis pour la garantir ne revient pas qu'à se gorger de grands mots.

Envoyer une fusée sur la lune ou construire une bombe nucléaire résulte de démarches que nos pays ont été capables de mener à bien lors des cinquante dernières années, et qui se prêtent parfaitement à la planification telle qu'on se la représente d'ordinaire. Le numérique n'obéit pas aux mêmes dynamiques. La planification technologique du numérique s'inscrit dans des logiques d'écosystème où les démarches spontanées, entrepreneuriales et les écosystèmes ouverts jouent un rôle clé.

Il n'en convient pas moins de l'organiser, même si on ne recourra pas pour cela aux mêmes outils que pour envoyer une navette dans l'espace ou mettre au point un dispositif d'armement. Il est d'autant plus impératif d'ordonner la planification technologique qu'elle mobilise une pléthore d'acteurs (de la recherche, de la formation, des start-up, des entreprises, sans compter les usagers) mal coordonnés.

Les feuilles de route bilatérales et multilatérales relatives à des objets technologiques clairement identifiés prennent dès lors une extrême importance. Vous avez évoqué tout à l'heure la stratégie européenne en matière d'Intelligence artificielle. Nous avons fait le choix à l'Inria d'un partenariat stratégique avec un acteur allemand, le *DFKI* (*Deutsches Forschungszentrum für Künstliche Intelligenz GmbH* - Centre de recherche allemand sur l'Intelligence artificielle). Nous recourons dans ce cadre à tous les types d'action à notre portée en vue du développement de ces feuilles de route conjointes. Il faut à mon avis aller jusqu'à s'accorder sur une feuille de route technologique autour des infrastructures logicielles critiques que j'ai évoquées plus tôt.

M. Philippe Latombe, rapporteur. On nous informe, ces derniers temps, d'un nombre accru de cyberattaques et surtout de leur niveau technologique de plus en plus avancé. A-t-on suffisamment pris en compte, dans l'espace économique français et européen, la menace qu'elles représentent ? Vous semble-t-il que les entreprises ont intégré ces possibilités de cyberattaques à leur plan de risque, de manière à investir en conséquence ? Ou estimez-vous qu'il reste encore des progrès à accomplir dans ce domaine ?

M. Bruno Sportisse. Je sortirais de ma zone de légitimité en émettant un avis définitif sur ce sujet. L'Inria est engagé dans un partenariat étroit avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI). La cybersécurité a été le premier des axes stratégiques de développement de l'institut identifié. Nous avons annoncé, M. Guillaume Poupard, le directeur général de l'ANSSI et moi-même, à l'occasion du dixième anniversaire de l'agence, le lancement d'équipes-projets conjointes, ce qui prouve l'intensité de notre collaboration.

Un plan cybersécurité, incarnant une stratégie d'accélération de la cybersécurité, a été annoncé voici quelques semaines. Il repose sur diverses actions portées par l'ANSSI, dont la constitution d'un campus cybersécurité, à l'issue de la mission de M. Michel Van Den Berghe, le dirigeant d'Orange Cyberdefense. Une perspective d'écosystème le sous-tend. Un plan de recherche est en cours d'élaboration. Son pilotage a été confié à l'Inria, au CEA et au CNRS. Il mobilise en tout cas beaucoup d'acteurs, ce qui prouve l'existence d'un mouvement en ce sens.

Quant à savoir si, au cours des cinq ou dix dernières années, la menace des cyberattaques a suffisamment été prise en compte, je ne suis pas habilité à en juger. Je constate en revanche une dynamique extrêmement forte, incluant aussi bien les acteurs de la recherche que les entreprises de toutes tailles, ce qui nous ramène à la question du vivier de compétences.

Il faut pouvoir compter sur des personnes formées à la cybersécurité pour diffuser les technologies et les savoir-faire associés dans toutes les organisations concernées.

M. Philippe Latombe, rapporteur. Comment voyez-vous le rôle d'innovation des GAFAM et leur volonté de promouvoir le développement des nouvelles technologies du numérique, aussi bien en interne que par le biais d'acquisitions ? Faut-il y voir une réelle menace ? Par quel moyen, si ce n'est contrôler ces GAFAM, en tout cas parvenir à un équilibre ?

M. Bruno Sportisse. Vous soulevez la question des écosystèmes. L'emporte dans le numérique, celui qui parvient à construire un écosystème alimenté par des flux : de compétences, comme je l'évoquais tout à l'heure, et de start-up, dans la mesure où une start-up constitue un excellent vecteur technique d'innovation.

Très souvent, un tel écosystème se structure autour d'infrastructures logicielles. Les GAFAM, qui maîtrisent parfaitement ces dynamiques, disposent de leurs propres écosystèmes et y piochent les outils, les talents et les start-up nécessaires au développement de nouveaux produits ou services à commercialiser.

Voilà ce que nous devons à notre tour maîtriser : les ingrédients, les mécanismes de l'innovation dans le numérique – d'où l'importance du renouvellement de nos pratiques dans la durée – et des politiques publiques en faveur de l'innovation. C'est d'ailleurs en vue de la construction d'un écosystème qu'a été lancée la French Tech ou encore qu'a été créé l'*EIC*, afin de partager le risque au niveau européen. Les stratégies d'accélération du plan de relance vont dans le même sens. Nous devons éviter toute solution de continuité et tout cloisonnement, si nous voulons disposer de véritables écosystèmes technologiques. Par ailleurs, il ne faudrait pas qu'ils soient rythmés par des appels à projets au financement public. Un écosystème doit suivre sa propre dynamique, sur laquelle s'accordent l'ensemble de ses acteurs.

On ne construit pas la souveraineté numérique à coups d'appels à projets, mais grâce à des écosystèmes opérationnels non cloisonnés. Les outils d'intervention de l'État revêtent une importance capitale. Bpifrance a de ce point de vue assumé un rôle majeur ces dernières années par le financement d'écosystèmes où les start-up jouent un rôle clé et dont les acteurs doivent comprendre la nécessité d'une proximité avec les acteurs de la recherche et les universités, de même que celle d'identifier les nouveaux concepts et les équipes dotées de fortes compétences autour de start-up.

Ceux qui ne comprendront pas cette mécanique éprouveront des difficultés à avancer dans le numérique.

Je trouve personnellement que les outils d'intervention français et européens ont très bien évolué dans la durée. Mon propos ne se veut pas lénifiant. Je souhaite seulement faire observer que la dynamique a bel et bien été enclenchée. Reste à voir comment les politiques initiées évolueront au fil du temps. C'est une question de constance. Nous n'en disposons pas moins de tous les ingrédients nécessaires.

M. Jean-Michel Mis. Ma question s'apparente à un constat. Depuis le discours de la Sorbonne, nous voyons qu'une dynamique s'est bel et bien amorcée, comme l'illustrent les annonces de ce matin à propos de l'Agence européenne de l'innovation.

J'aimerais que l'on revienne sur vos propos concernant les acteurs systémiques (GAFAM et BATX) et la possibilité, grâce à l'important fonds de l'agence européenne, de toucher plutôt les start-up ou *scale-up* à l'origine d'une technologie de rupture susceptible, par un effet d'entraînement, de changer la situation actuelle.

Quel regard portez-vous de ce point de vue sur la feuille de route française ? Nous assumerons la présidence de l'Union européenne au 1er janvier prochain. Est-il encore possible de franchir un palier, au-delà de l'agence, en vue d'une synergie entre souverainetés française et européenne ? Nous comptons en revendiquer notre part en proportion de ce que représentent nos écosystèmes. Comment voyez-vous cette volonté de financer en priorité les *deep tech* porteuses d'innovations de rupture, dans l'espoir, si ce n'est de combler notre retard, de trouver de nouveaux relais de croissance basés sur des modèles économiques nouveaux ? Estimez-vous la France capable d'incarner une doctrine relative aux enjeux de la souveraineté ?

M. Bruno Sportisse. Il existe une profonde cohérence entre tous ces éléments, d'où mon emploi du terme de planification technologique, utilisé ce matin par le président Emmanuel Macron. Les start-up sont des vecteurs. Ce qui compte, c'est la feuille de route globale qui porte sur quelques grandes technologies. Un travail colossal a été réalisé autour de DigitalEurope au niveau européen. Au niveau français, d'importants efforts ont été consentis au travers du plan de relance. Il en va de même dans d'autres pays. Il faudra bien sûr articuler un effort tel que notre plan de relance avec la feuille de route DigitalEurope et ses instruments comme l'*EIC*. Tout ceci se joue dès aujourd'hui.

Pour prendre l'exemple de l'Intellligence artificielle, nous avons avancé sur la version 1 de la stratégie nationale en la matière. Une version 2 est en cours d'élaboration. L'un des enjeux n'en est autre que la création de liens avec des partenaires européens. Il faut s'engager à suivre des feuilles de route technologiques conjointes, c'est-à-dire à livrer des résultats concrets dans un horizon de quelques années.

Il ne faut pas se contenter, je m'excuse de revenir encore là-dessus, de réagir à des appels à projets communautaires, mais pouvoir s'appuyer sur tout un écosystème.

Soucieux d'inscrire son action dans le long terme, l'Inria multiplie actuellement les partenariats avec d'autres organismes européens. Se contenter des interventions publiques comporte le risque de l'opportunisme. Les sommes débloquées pour le numérique sont colossales. Un décideur politique doit être en mesure de distinguer ce qui relève de stratégies opportunistes d'accès au financement (dont tous les chercheurs ont besoin), de l'engagement, selon des feuilles de route, d'acteurs coordonnés en faveur de la souveraineté.

Vous avez raison, M. le député, de soulever ce point : nous vivons une année difficile néanmoins intéressante à plus d'un titre. Elle apparaît comme une année charnière, à l'issue de laquelle la présidence de l'Union européenne reviendra à la France au premier semestre 2022, ce qui nous ouvre bien des perspectives. Il faudra d'autant mieux s'y préparer que le rôle moteur de la France dans le domaine numérique est bien connu.

M. Jean-Michel Mis. Vous parliez également de coopération et des implantations régionales de l'Inria. Pourrait-on, selon vous, imaginer, dans les thématiques que nous évoquons, des coopérations interrégionales, ou estimez-vous absurde de réfléchir à l'échelle de bassins géographiques, sachant que nous devons veiller à l'intégrité de nos territoires et ne pas nous contenter, pour cette raison, de quelques « silos » implantés en région parisienne ?

Comment envisager des coopérations de haut niveau qui ne soient pas uniquement politiques, c'est-à-dire qui ne suscitent pas seulement de l'intérêt pour l'innovation ou les ambitions que nous nous fixons en termes de souveraineté ? Peut-on envisager des collaborations réellement pertinentes en Europe en matière de recherche et d'innovation, permettant le maintien, sur l'ensemble des territoires, de ces enjeux technologiques ?

M. Bruno Sportisse. Les cadres de coopération possibles sont multiples. Des enjeux se mélangent, liés à la formation, à la mobilité des talents, aux programmes de recherche, sans

parler des enjeux industriels relatifs aux plateformes technologiques. Même si tous sont liés, ils obéissent à des dynamiques subtilement différentes.

La dynamique qui porte l'informatique quantique peut-elle s'épanouir autrement que dans un cadre planifié ? Je ne crois pas trop à la pertinence de la notion de territoire par rapport à cette dynamique précise.

Cela étant, la notion de souveraineté numérique recouvre un tel nombre d'enjeux que les outils de coopération incluent de fait ceux que vous évoquez, dont certains sont d'ailleurs déjà en place. Ainsi, en matière de coopération transfrontalière, le centre Inria de Nancy a noué des partenariats avec d'autres acteurs de la recherche en Sarre, autour de la cybersécurité notamment.

Quoi qu'il en soit, il n'existe pas de recette unique concernant le numérique, où prévaut simplement un plan général supposant le recours à différents vecteurs d'action.

M. Philippe Latombe, rapporteur. Vous viendrait-il à l'esprit d'autres sujets que nous devrions aborder dans notre mission d'information ?

M. Bruno Sportisse. Il me semble que nous avons fait le tour des thématiques auxquelles touchaient vos questions. Je vous enverrai par écrit mes réponses à la partie de votre questionnaire que nous n'avons pas abordée, à propos du rôle de l'Inria et du numérique dans la réponse à la crise sanitaire, au-delà du projet TousAntiCovid. Nous avions mis en place des modes de fonctionnement intéressants en matière de souveraineté.

Audition, ouverte à la presse, de MM. Jean-Claude Laroche, vice-président, et Henri d'Agrain, délégué général, du Club informatique des grandes entreprises françaises (Cigref)
(18 mars 2021)

Présidence de M. Philippe Latombe, rapporteur.

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

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

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

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

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

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

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

M. Jean-Claude Laroche, vice-président du Club informatique des grandes entreprises (Cigref). La souveraineté numérique est, depuis plusieurs années, un sujet d'intérêt pour le Cigref. C'est une question qui fait débat au sein même du Cigref, entre ses différents membres, puisque les grandes entreprises adhérentes ont souvent une activité à l'échelle de la planète, partout dans le monde. La question de la souveraineté ne se pose donc

pas de la même manière selon que nous regardons uniquement le périmètre du territoire national ou plus largement l'ensemble de la planète où nous pouvons exercer nos activités.

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

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

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

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

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

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

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

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

Le second volet concerne la *supply chain*. Au moment de la pandémie, par exemple, un certain nombre de nos adhérents se sont demandé s'ils réussiraient à s'approvisionner en masse en ordinateurs portables pour assurer le passage en télétravail massif des salariés de leurs organisations.

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

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

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

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

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

Sur le plan des technologies, cette évolution a mis en évidence la centralité du *cloud*, de l'informatique en nuage, pour pouvoir exercer son activité depuis n'importe quel terminal, depuis n'importe quel lieu, à n'importe quel moment. C'est le *cloud* qui le permet en termes d'infrastructures. Il s'ensuit le besoin urgent d'un *cloud* de confiance pour les grandes entreprises et les administrations françaises, de sorte que nous puissions travailler à distance, sur la base d'infrastructures partagées dans le *cloud* et en toute sécurité.

Que signifie un *cloud* de confiance ? Volontairement, nous ne parlons pas de *cloud* souverain, puisque toutes sortes de technologies peuvent se trouver dans un *cloud*, y compris des technologies américaines, israéliennes… Nous avons essayé de définir un *cloud* de confiance, d'abord comme un *cloud* immune au droit extra-européen. Typiquement, il ne faut pas qu'un juge d'un pays extra-européen puisse s'appuyer sur la législation de son État pour

aller regarder les données hébergées dans le *cloud* d'une entreprise qui serait considérée comme extra-européenne et appartenant à cet État.

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

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

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

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

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

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

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

Je prends deux exemples récents. J'ai été personnellement frappé de voir le rachat de l'entreprise Sentryo par Cisco. Sentryo était spécialisée dans la cybersécurisation des systèmes d'information industriels. Cisco a proposé à Sentryo en la rachetant un financement lui permettant de développer ses activités, mais celles-ci ne sont plus françaises ou européennes. Plus récemment, Alsid qui est également une vraie pépite spécialisée dans la sécurisation des annuaires, des composants sensibles de nos systèmes d'information, a été rachetée par

Tenable, une société américaine. La question de la protection et du financement de nos *start-up* offrant des solutions innovantes touche donc pour nous à la souveraineté.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

M. Henri d'Agrain. Absolument.

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

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

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

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

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

Cela n'a rien à voir avec le *Cloud Act* Lorsque des entreprises comme IBM vous disent être immunes face au *Cloud Act*, ce n'est pas vraiment le problème, notamment pour des entreprises globales. Les entreprises globales qui ont des activités aux États-Unis sont de toute façon américaines aux États-Unis et donc soumises directement à la réglementation américaine. Le principal problème pour les entreprises provient de réglementations très intrusives comme l'article 702 du *FISA*, ainsi que l'a très justement reconnu la Cour de justice de l'Union européenne.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

M. Jean-Claude Laroche. Avons-nous des personnes de talent ? La réponse est oui. En avons-nous assez ? La réponse est non. Le marché des personnes ayant un haut niveau de qualification dans le domaine de la cybersécurité est extrêmement tendu et, pour certains types de compétences, les éléments de rémunération ont tendance à augmenter fortement, ce qui n'est qu'une traduction de la rareté de ces compétences.

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

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

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

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

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

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

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

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

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

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

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

être présente sur l'ensemble du spectre des technologies nécessaires pour assurer cette souveraineté.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

M. Henri d'Agrain. Vous aviez abordé la question du *DMA* sur lequel le Cigref est particulièrement engagé. Du point de vue de nos adhérents, c'est une opportunité absolument indispensable pour l'économie européenne. Nous ne travaillons pas seulement pour nos adhérents mais nous pensons que faire en sorte que le *DMA* permette de maîtriser la

dépendance de l'économie européenne par rapport à des offres extra-européennes, aujourd'hui et encore plus demain, est vraiment d'une mission d'intérêt général. Il ne s'agit pas d'évincer les offres extra-européennes mais de maîtriser les taux de dépendance, la façon dont l'économie européenne sera complètement enfermée par ce type de solution. Si ces solutions ne sont pas européennes, je pense que nous aurons demain de grosses difficultés économiques.

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

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

Audition, ouverte à la presse, de M. Gwendal Le Grand, secrétaire général adjoint de la Commission nationale de l'informatique et des libertés (CNIL)

(25 mars 2021)

Présidence de M. Philippe Latombe, rapporteur.

M. Philippe Latombe, président et rapporteur. Nous accueillons aujourd'hui M. Gwendal Le Grand, secrétaire général adjoint de la Commission nationale de l'informatique et des libertés (CNIL), accompagné de Mme Manon de Fallois, juriste au service de la santé et de M. Etienne Maury, juriste au service des affaires européennes et internationales.

La CNIL est une autorité administrative indépendante, créée par la loi Informatique et Libertés du 6 janvier 1978. Elle compte deux cent quinze agents et son collège est composé de dix-huit membres parmi lesquels quatre parlementaires.

La CNIL a pour mission de veiller à la protection des données personnelles contenues dans les fichiers informatiques ou papier, aussi bien publics que privés. Elle rend, en conséquence, un certain nombre d'avis et peut prendre des décisions de sanction en cas de non-respect du cadre juridique. Elle se situe donc au cœur des enjeux de notre mission d'information.

Nous souhaitons avant tout vous entendre sur trois sujets.

En prmier lieu, comment la CNIL se positionne-t-elle vis-à-vis de la souveraineté numérique ? Ce concept comprend de nombreuses définitions et déclinaisons, qui renvoient essentiellement, d'un point de vue juridique, à la capacité des pouvoirs publics à imposer le respect du cadre de régulation existant dans la sphère numérique, afin de protéger les droits et les libertés des citoyens.

Comment envisagez-vous votre action, dans un contexte marqué par le caractère évolutif des technologies numériques et un cadre juridique en mouvement, comme le montrent les différentes initiatives de régulation engagées au niveau européen ?

Nous souhaitons également échanger sur la façon dont les CNIL européennes coopèrent face aux pratiques de certains acteurs comme les GAFAM, qui déjouent largement les frontières nationales.

Notre deuxième questionnement porte sur les conséquences des récentes décisions de la Cour de justice de l'Union européenne (CJUE) sur la protection des données.

Notre mission d'information s'intéresse aux données de santé, dont l'exploitation est à la fois pleine de promesses, en termes d'innovation, et pleine de risques, raison pour laquelle elle est strictement encadrée en droit.

Nous aimerions savoir comment la CNIL se positionne sur ce sujet, notamment vis-à-vis des plateformes de données de santé et de la situation plus spécifique du Health Data Hub.

Nous nous interrogeons également sur les conséquences de la décision *Schrems* II, qui a invalidé le *Privacy Shield*, car il crérait une situation juridique insécure pour les entreprises, qui pouvaient transférer leurs données vers des pays tiers, en particulier les États-Unis.

Nous souhaiterions savoir quel regard vous portez à ce sujet et vous entendre sur les enjeux d'extra-territorialité du droit américain, le *Cloud Act* ou le *Foreign Intelligence Surveillance Act (FISA)*.

Enfin, nous aimerions échanger sur les évolutions souhaitables ou nécessaires pour la CNIL dans ce contexte mouvant. Nous savons qu'elle souhaite intégrer davantage les problématiques de cybersécurité, qui est l'une de ses priorités en matière de contrôle en 2021. Le projet de loi 4D pourrait aussi renforcer l'effectivité du pouvoir de sanction de l'autorité en proposant une procédure simplifiée dans ce domaine.

Identifiez-vous d'autres évolutions souhaitables pour renforcer votre capacité d'agir en faveur de la protection des données, des droits et des libertés des citoyens dans le domaine du numérique ?

M. Gwendal Le Grand, secrétaire général adjoint de la Commission nationale de l'informatique et des libertés (CNIL). Mmes et MM. les députés, Mmes et MM, je suis très honoré d'avoir l'occasion de m'exprimer devant votre mission d'information et je vous remercie, au nom de la CNIL, pour votre invitation.

Je suis accompagné de M. Etienne Maury, qui travaille au service des affaires internationales et européennes, et de Mme Manon de Fallois, qui travaille au service de la santé.

La souveraineté numérique est devenue, en quelques années, un sujet politique majeur et décisif. Depuis sa création, il y a plus de quarante ans, la CNIL a observé comment les innovations technologiques ont progressivement envahi les espaces de la vie privée et de la vie en collectivité, au travail comme dans les entreprises ou les services publics. Le numérique a même modifié la perception de nos frontières, des valeurs de nos sociétés et de notre équilibre économique.

Cette difficulté nécessite de repenser le concept de souveraineté nationale et européenne pour faire face à deux principaux enjeux.

Le premier enjeu est lié à la capacité des États à appliquer leurs normes. En effet, rien de ce qui définit la puissance publique (un territoire, des frontières, des règles) ne fonctionnent en ligne, car Internet n'est pas un lieu, mais un lien dans lequel s'effectue d'innombrables traitements et transferts internationaux de données. La singularité de la révolution numérique tient d'ailleurs au fait que les gisements de données ne se tarissent pas avec le temps. L'usage de données génère de la valeur par leur recoupement, leur agrégation et leur mise en relation.

Le deuxième enjeu est celui de l'éthique. Le *« solutionisme technologique »* proposé par de multiples acteurs, qui se confrontent sur des marchés, est une tendance forte, qui pourrait nous conduire à subir des choix d'organisation de la vie en société. Le risque réside dans le fait que ces choix soient *in fine* opérés à notre insu, en dehors des circuits démocratiques traditionnels, et que les nations n'aient plus la capacité d'opérer des choix collectifs.

L'État est mis au défi dans toutes ses facettes d'expert, de stratège, de législateur, de régulateur et de pouvoir exécutif. Face à ce défi, l'intervention de la puissance doit se recomposer autour de leviers robustes, que je vous propose d'explorer au travers du prisme de la CNIL.

Je reviendrai rapidement sur la genèse du Règlement général sur la protection des données (RGPD) et la structuration de la souveraineté numérique, avant de présenter un bilan européen de la protection des données. Je terminerai sur les axes prioritaires à renforcer pour que la CNIL soit à la hauteur des enjeux dans un monde post-Covid. Mon propos répondra ainsi à la plupart de vos questions.

S'il existait un ADN du numérique à l'échelle française ou européenne, il s'agirait de placer la personne humaine au centre de la régulation. Celle-ci a évolué afin de répondre à des défis politiques, économiques et géopolitiques.

S'agissant des défis politiques, l'article premier de la loi Informatique et Libertés de 1978, qui a donné naissance à la CNIL, pose le principe selon lequel l'informatique doit être au service de chaque citoyen et ne porter atteinte ni à une entité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles et publiques. Quarante ans plus tard, cet article premier constitue toujours une boussole.

La loi Informatique et Libertés a également imposé quatre types de nouveaux droits citoyens : les droits d'information, d'opposition, d'accès et de rectification.

À partir des années 1990, des défis économiques surviennent. Avec l'explosion d'Internet, l'Europe se dote d'une directive en 1995, qui reprend les principes de la loi Informatique et Libertés. En 2002, une directive dite *« on Privacy »* (Vie privée et communication électronique) reconnaît la spécificité du secteur des communications électroniques. Depuis, le contexte économique a beaucoup évolué, avec les GAFAM qui sont devenues hégémoniques et de nombreuses avancées technologiques, comme les objets connectés, les techniques de profilage, de surveillance, les outils de contrôle, les algorithmes et le développement des cyberattaques, qui nourrissent la conscience collective de devoir revoir à la hausse le niveau de protection des données personnelles. Les révélations d'Edward Snowden aux débuts des années 2010 en sont le symbole.

Dans ce contexte, la directive a évolué le 25 mai 2018 en Règlement général sur la protection des données (RGPD), qui s'articule autour de cinq axes majeurs.

Le premier axe est le renforcement quantitatif et qualitatif du droit des personnes, une meilleure explication de la loi Informatique et Libertés, l'apparition de nouveaux droits, comme le droit à l'oubli, le droit à la portabilité et la possibilité de mener des actions de groupe.

Le deuxième axe est la responsabilisation de l'ensemble des acteurs de traitement de données, publiques et privées, sur la base de principes de minimisation de la collecte, de limitation de la durée de conservation et d'obligation de sécurité pour garantir à tout moment le respect du Règlement.

Le RGPD est d'ailleurs fondé sur la notion de risques présentés par les traitements, tant en volume qu'en sensibilité des données. En clair, plus l'acteur est important dans l'écosystème numérique, plus ses obligations et ses responsabilités sont nombreuses

Le troisième axe s'inscrit en contrepartie du précédent, par le renforcement du pouvoir de sanction administrative des différentes CNIL au niveau européen. Les sanctions peuvent aller jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires mondial d'une entreprise, l'option majeure étant appliquée. La gamme des sanctions est également élargie.

Le quatrième axe est la mise en place d'un nouveau modèle de gouvernance de la régulation, inédit au niveau européen, au travers d'un guichet unique pour les entreprises et

d'un guichet unique pour les citoyens. Si l'entreprise n'a qu'un seul interlocuteur, les décisions qui la concernent sont prises selon des principes de consensus et de coopération entre les différentes autorités nationales, afin de prononcer une décision applicable harmonisée à l'échelle européenne. En cas de désaccord entre les autorités, le nouveau Comité européen de la protection des données (CEPD), c'est-à-dire le groupe des CNIL européennes, arbitrera et prendra une décision contraignante vis-à-vis de l'autorité de l'établissement principal.

Le cinquième axe est le RGPD, qui a constitué une première étape décisive dans la souveraineté numérique, grâce à son principe de libre circulation des données sur l'ensemble du territoire de l'Union et son principe inédit d'extra-territorialité, selon lequel il s'applique à tous les acteurs dès lors qu'un organisme cible des citoyens européens. Il ne s'agit pas, pour l'Europe, de se livrer à du protectionnisme, mais d'affirmer un modèle de régulation fondé sur la défense du droit des personnes, héritée de la philosophie humaniste des droits de l'Homme, en vue de générer la confiance indispensable à la réussite de cette politique publique.

En outre, toutes les études récentes montrent une profonde aspiration de maîtrise des personnes sur leurs données. Ainsi, 87 % des Français se déclarent sensibles à la protection des données.

S'agissant des défis d'ordre stratégique, plusieurs modèles de régulation fondamentalement différents s'affrontent à l'échelle mondiale. Le RGPD est devenu un instrument de *soft power* de diplomatie. Nous constatons un avant et un après 25 mai 2018 au niveau mondial. Des pays ont procédé à la mise à jour de leur cadre national en matière de protection des données, afin de continuer à commercer avec l'Europe. Tel est le cas de la Suisse, du Japon, de la Corée du Sud, du Bénin ou de l'Australie. Des processus législatifs sont en cours dans d'autres pays comme la Tunisie ou le Burkina Faso. Des États ont, pour la première fois, adopté un cadre juridique général de protection des données personnelles comparable au RGPD dans ses principales dispositions. Tel est le cas de la Californie avec le *California Consumer Privacy Act (CCPA)* adopté en octobre 2018 et entré en application le 1er janvier 2020. Le Brésil a adopté son règlement en 2019. En Inde, la Cour suprême a consacré, en 2017, le droit à la protection de la vie privée comme un droit fondamental. Un projet de loi est en discussion au parlement.

En tout état de cause, le RGPD est un des rares textes dont nous parlons encore trois ans après son adoption, ce qui démontre que les échanges de données personnelles sont au cœur de toutes les discussions politiques au niveau international, au même titre que les règles en matière de concurrence ou de commerce.

Trois ans après la mise en œuvre du RGPD, quel bilan l'Europe peut-elle tirer ?

À l'échelle de la France, la CNIL en a véritablement constaté l'effet. Les citoyens se saisissent de leurs droits lorsque ceux-ci leur sont mieux expliqués. En 2019 et en 2020, nous avons reçu environ 14 000 plaintes, ce qui représente une augmentation de 27 % par rapport à 2018, qui était déjà une année record.

En 2020, la crise sanitaire a fait émerger de nombreux enjeux. Les visites sur le site de la CNIL ont augmenté de 18 % en un an, ce qui témoigne de l'intérêt des citoyens pour ces questions au regard de l'actualité récente. Nous comptons aujourd'hui plus de 24 000 délégués à la protection des données, qui représentent plus de 72 000 organismes. Nous avons reçu près de 6 500 notifications de violation de données personnelles depuis 2018 et près de 1 200 dossiers en 2018, 2 300 en 2019 et plus de 3 000 dossiers en 2020. Ces dossiers permettent à la CNIL d'orienter son action de conseil et de répression et de mieux jouer son rôle dans l'écosystème de la cybersécurité.

En ce qui concerne la répression, la CNIL conduit environ 300 contrôles formels chaque année. Le nombre de mesures correctrices est en constante hausse. Après une période d'actions pédagogiques en 2018, la CNIL a prononcé une quinzaine de sanctions en 2020 (contre huit sanctions en 2019) pour un montant cumulé d'environ 139 millions d'euros.

À l'échelle européenne, la mise en œuvre de nouveaux modèles est clairement enclenchée, avec plus de 1 500 cas transfrontaliers identifiés, 550 procédures de guichet unique lancées avec nos homologues et plus de 190 décisions finales adoptées en application du mécanisme de coopération et de cohérence.

Fin 2020, une première décision contraignante a arbitré un différend entre l'autorité irlandaise et les autorités européennes concernant Twitter. Le CEPD a également ajouté une vingtaine de lignes directrices précisant le RGPD sur des notions essentielles, comme son champ d'application territorial, le ciblage des utilisations sur les réseaux sociaux ou le *privacy by* design – la protection des données dès la conception – contribuant ainsi à une véritable doctrine européenne en la matière.

À ce jour, la CNIL a prononcé plus de 550 sanctions représentant plus de 300 millions d'euros d'amendes.

Le RGPD a passé le test de la crise sanitaire, en évitant le détournement d'usage des données sensibles tout en se montrant suffisamment souple pour permettre aux États membres de traiter et de partager ce type d'informations dans un contexte exceptionnel.

Ces fondements posés, quels sont les axes prioritaires des années à venir pour renforcer la souveraineté numérique ? Ces axes relèvent de trois domaines : la cybersécurité, la politique industrielle et le cadre législatif européen.

Concernant la cybersécurité, il ne se passe pas un jour sans que ne nous soit signalée une attaque ciblant les réseaux de grands organismes publics ou privés, y compris ceux ayant des moyens financiers importants ou menant des activités particulièrement critiques.

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a traité plus de 200 attaques en 2020 contre 50 en 2019. La plupart du temps, ces attaques prennent la forme de rançongiciels, qui paralysent le système d'information et demandent le paiement d'une rançon pour récupérer l'accès aux données. Ces attaques sont la première cause de recherche et d'assistance auprès du site cybermalveillance.gouv.fr.

La CNIL reçoit des notifications de violation de données. Elle vérifie la sécurité et accompagne les personnes et les PME, tandis que l'ANSSI traite plutôt de grandes failles ou d'actions particulièrement malveillantes.

Le deuxième levier d'action consiste à déployer une politique volontariste pour faire émerger les champions européens du numérique. Le respect de la vie privée et l'intégration du principe de *privacy by design* sont de véritables avantages concurrentiels pour les acteurs européens qui sauront s'en saisir, car ils répondent aux aspirations actuelles des consommateurs. La sécurité du *cloud* en est un bon exemple. En dépit de l'échec des premiers *clouds* souverains, la France défend une solution nationale ou européenne pour abriter les données sensibles et favoriser l'émergence d'un marché de confiance, en ajustant des offres déjà matures pour les mettre en conformité avec les standards de protection des données et de transparence des contrats. La CNIL entend suivre et accompagner ces initiatives, qui offrent une alternative viable aux géants du c*loud*, tant pour le fournisseur que pour le client.

Un exemple stratégique est l'hébergement des données de santé, qui doit être transféré sous deux ans vers une solution française ou européenne relevant exclusivement de la juridiction de l'Union européenne. Pour la CNIL, ce délai garantit un juste équilibre entre la préservation du droit à la protection des données personnelles et l'objectif de favoriser la recherche et l'innovation dans le domaine de la santé.

Le troisième levier d'action est la préservation de notre ordre juridique européen. La question du transfert des données est devenue prégnante en 2020 et plusieurs décisions législatives d'envergure ont été prises.

L'arrêt *Schrems* II, rendu le 16 juillet 2020 par la Cour de justice de l'Union européenne, a tout d'abord invalidé le bouclier de protection de données, le *Privacy Shield,* qui permettrait le transfert de données vers les États-Unis sans formalité supplémentaire. Le CEPD, le groupe des CNIL européennes, et la CNIL se sont emparés de cette décision, afin d'en tirer toutes les conséquences.

La Commission européenne a annoncé, fin 2020, sa stratégie de régulation de l'écosystème numérique européen. Le *Digital Market Act (DMA)* pose le principe de régulation économique en présentant un certain nombre d'adhérences avec le RGPD en matière d'obligations, d'interopérabilité des données, de transparence des traitements et de consentement explicite des consommateurs pour la mutualisation des données.

Le *Digital Services Act (DSA)* concerne la responsabilité des plateformes face à la souveraineté de l'État.

Le *Data Governance Act* (*DGA)* vise, quant à lui, à définir un cadre européen pour la réutilisation et le partage des données, qu'elles soient personnelles ou non. Ce texte ambitieux constitue le socle d'une future économie européenne de la donnée.

Pour conclure, le contexte actuel offre un alignement assez inédit des intérêts entre notre modèle de gouvernance de la donnée et notre politique industrielle. Il est essentiel que nous parvenions collectivement à nous en saisir pour mener une politique ambitieuse de souveraineté numérique européenne. Le RGPD est un facteur clé de cette ambition.

Je me tiens maintenant à votre disposition pour répondre à vos questions.

M. Philippe Latombe, rapporteur. Nos questions sont nombreuses.

Dans les récents arrêts *Schrems* de la Cour de justice européenne et la jurisprudence *Tele2 Sverige* et *Prokuratuu*r, il y a quelques semaines, qu'est-il autorisé et interdit aujourd'hui ? Les addendas ou les spécificités techniques sont-ils suffisants pour assurer la protection des données lorsque nous utilisons les *clouds* étrangers des GAFAM ? Quelle est la portée de l'extra-territorialité américaine réelle sur les filiales de ces grands groupes en Europe ?

Nous avons interrogé IBM, qui nous a répondu que les jurisprudences *Schrems* ne lui sont pas applicables en raison de ses filiales en France relevant du droit français. À la même question, Google et Amazon nous ont répondu, la semaine passée, que ces jurisprudences leur étaient évidemment applicables, malgré leurs filiales irlandaises.

Quelle est la position de la CNIL sur les données personnelles classiques et les données personnelles sensibles ? Cette demande émane aussi des entreprises, qui ne savent plus où elles en sont.

M. Gwendal Le Grand. Un avis sur la mise en œuvre de l'arrêt *Schrems* a été publié assez rapidement par le Comité des CNIL européennes pour consultation publique. Nous travaillons aujourd'hui sur sa version définitive. La CNIL et le CEPD ont également rédigé des questions fréquentes pour répondre aux entreprises.

Cette décision *Schrems* est cruciale sur trois plans. La Cour a reconnu la validité des clauses contractuelles-types de la Commission européenne comme outil de transfert. Elle a toutefois précisé que pour recourir à cet outil, il appartient à l'exportateur des données de vérifier que la législation applicable à ce transfert dans le pays tiers de destination n'aboutit pas à affaiblir le niveau de protection des données. À défaut, des mesures supplémentaires doivent être prises pour protéger les données. Enfin, la Cour a invalidé la décision concernant le bouclier de protection des données.

Le CEPD a publié des recommandations. Une consultation publique a été ouverte jusqu'en début d'année. Leur mise à jour est en cours pour tenir compte des nombreux commentaires reçus.

Concernant la question de l'accès aux données par les autorités américaines, l'une des premières questions à se poser pour déterminer si l'entité est sujette à l'extra-territorialité du droit américain est de savoir si la garde, la possession ou le contrôle des données concernées relèvent d'une société soumise au droit américain. Selon le *Cloud Act*, un responsable de traitement ou un fournisseur de communications électroniques ou de services informatiques distants, dont les traitements sont soumis au RGPD, pourrait devoir répondre à un mandat des autorités américaines en vertu du *Cloud Act*. Un sous-traitant de responsable de traitement américain, établi dans l'Union européenne, peut être destinataire d'un mandat des autorités américaines pour les données qu'il sous-traite.

La section 702 du *FISA* n'apporte pas de précision sur la portée extraterritoriale des ordres à produire, mais elle ne restreint pas ces demandes aux seules données stockées sur le territoire américain, ce qui implique un possible accès à des informations en dehors du territoire américain. Il n'y a donc pas de doute sur le caractère extraterritorial des acquisitions et des interceptions fondées sur l'*Executive Order* 12333.

L'utilisation des logiciels et de solutions techniques brevetés par des sociétés américaines n'est pas déterminante de la possibilité pour les autorités américaines de contraindre des sociétés à divulguer des données, dès lors que ces solutions sont utilisées par des responsables de traitements qui ne sont pas soumis à la juridiction américaine. Il suffit de s'assurer que ces solutions techniques ne permettent pas un accès aux données par le biais de portes dérobées, intégrées par des développeurs à la demande des autorités américaines, notamment en application de la section 702 du *FISA*.

M. Philippe Latombe, rapporteur. Concrètement, Watson, un logiciel d'intelligence artificielle d'aide aux commerciaux, qui a accès aux bases de données pour préparer les réponses aux consultations des clients, est breveté par IBM Corp aux États-Unis et mis à la disposition de l'ensemble de ses filiales dans le monde. Watson constitue-t-il une porte d'extra-territorialité en Europe pour les États-Unis ? Watson est-il soumis au *Cloud Act* et éventuellement à la section 702 du *FISA* ?

M. Gwendal Le Grand. Pour répondre précisément, nous devrions observer la mise en œuvre de ce logiciel. D'une manière générale, si Watson est une solution logicielle mise en œuvre par un responsable de traitement européen non soumis à la législation américaine, la réponse est négative.

En revanche, si Watson traite de données par lui-même, la réponse est affirmative. Il convient de définir précisément la nature du logiciel et s'il est mis en œuvre, sans transfert de données, dans des systèmes informatiques d'une société européenne ou si des données sont adressées à l'intelligence artificielle de serveurs pouvant se situer aux États-Unis.

M. Philippe Latombe, rapporteur. Quelles sont les conséquences de l'arrêt *Schrems* appliqué aux données de santé ? Sur une sollicitation du Conseil d'État, vous avez émis un avis en faveur de migrations vers un *cloud* souverain, alors même que le Health Data Hub (HDH) applique les clauses contractuelles-types et des addenda signés avec Microsoft, sous couvert d'une localisation en Europe et d'une clé de chiffrement à laquelle Microsoft n'a pas accès.

M. Gwendal Le Grand. L'avis du Conseil d'État sur ce cas est très intéressant et il confirme l'analyse de la CNIL. Il convient de distinguer la question des transferts et le traitement des données par une société susceptible de recevoir des requêtes de la part des autorités américaines. Le Conseil d'État estime qu'il existe un risque d'accès par les autorités américaines, y compris en l'absence de transfert de données, du fait de la loi d'extra-territorialité américaine. De nombreux échanges ont ainsi porté sur la nécessité d'assurer un hébergement des données de santé, qui sont particulièrement sensibles, afin de garantir l'absence de risque d'accès par les autorités américaines.

M. Philippe Latombe, rapporteur. J'en déduis que cette décision serait applicable à d'autres données et d'autres systèmes utilisés par l'État et la sphère publique. Nous pouvons citer les *smart cities*, dans lesquelles une municipalité placerait les données des citoyens pour calculer le coût de la cantine ou de l'EHPAD.

M. Gwendal Le Grand. Le HDH concerne normalement un large volume de données particulièrement sensibles. Le raisonnement sur les possibilités d'accès par les autorités américaines du fait que le HDH est hébergé par un prestataire américain peut effectivement être appliqué à d'autres systèmes d'information.

M. Philippe Latombe, rapporteur. Le Conseil d'État a été saisi à propos de Doctolib. Considérez-vous également que les données de prise de rendez-vous pour la vaccination contre la Covid ne sont pas des données de santé ?

M. Gwendal Le Grand. Le Conseil d'État estime que la gestion des prises de rendez-vous, assurée par trois sociétés, dont Doctolib, et le fait d'être prioritaire pour la vaccination ne sont pas des données de santé. AWS et Doctolib ont conclu un addendum définissant une procédure précise en cas de demande d'accès aux données par une autorité publique. Cette procédure prévoit notamment la contestation de toute demande générale ou ne respectant pas la réglementation européenne. Ces sociétés ont, par ailleurs, mis en place un certain nombre de mesures techniques, dont un système de chiffrement fondé sur un tiers de confiance basé en France.

Le Conseil d'État a conclu que le niveau de protection des données ne pouvait pas être considéré comme manifestement insuffisant au regard du risque de violation du RGPD.

M. Philippe Latombe, rapporteur. Ma question était de savoir ce que le Conseil d'État considère comme une donnée de santé.

M. Gwendal Le Grand. Le Conseil d'État n'a pas expressément indiqué que les données relatives aux prises de rendez-vous ne sont pas des données de santé. Le communiqué de presse précise que le juge des référés du Conseil d'État relève que les données transmises

à Doctolib dans la campagne de vaccination ne comprennent pas de motifs médicaux d'éligibilité à la vaccination, mais portent uniquement sur l'identité des personnes et la prise de rendez-vous. La définition d'une donnée de santé est donnée par l'article 4 du RGPD.

M. Philippe Latombe, rapporteur. Certains juristes considèrent que la décision du Conseil d'État n'est pas cohérente avec cette définition.

Vous avez récemment utilisé un procédé particulier pour sanctionner Google à propos des cookies au moyen d'un texte ancien, qui présente l'intérêt de ne pas entrer dans le champ de la régulation des CNIL européennes, dont le chef de file aurait été la CNIL irlandaise. Selon vous, celle-ci est-elle mal à l'aise vis-à-vis de grands groupes, qui se sont installés sur son territoire pour des raisons fiscales ? N'est-elle pas soumise à un conflit d'intérêts, qui l'empêche de sanctionner les GAFAM ?

M. Gwendal Le Grand. Fin décembre 2020, la formation restreinte de la CNIL a prononcé une sanction de 100 millions d'euros à l'encontre de Google LLC, Google Irlande et Amazon pour l'utilisation de cookies sur la base d'une législation largement appliquée. Cette directive de 2002 avait été révisée en 2009, puis en 2018 sous l'effet de la mise en application du RGPD. Cette législation n'est donc pas ancienne. Un accord a même été conclu récemment au Conseil pour qu'elle devienne un Règlement européen.

Cette directive traite notamment du stockage de cookies sur le terminal d'un utilisateur. Ce stockage doit faire l'objet d'une information et d'un consentement préalable. Cette directive est transposée en droit national dans tous les états membres. En France, la CNIL est chargée de contrôler l'application de cette règle et de sanctionner les éventuels manquements. Beaucoup d'actions ont d'ailleurs été engagées par la CNIL pour clarifier les règles en matière de dépôt de cookies. Des lignes directrices, qui ont d'ailleurs été attaquées devant le Conseil d'État, et une recommandation ont été édictées. Les entreprises ont jusqu'à la fin du mois de mars 2021 pour se mettre en conformité.

La décision a été attaquée en référé par Google devant le Conseil d'État. Dans l'ordonnance du 4 mars 2021, le juge a rejeté la demande de suspension de l'exécution formulée par les sociétés Google LLC et Google Irlande d'une injonction prononcée par la formation restreinte des CNIL dans sa décision de décembre 2020.

Dans sa décision de référé, le Conseil d'Etat a confirmé que le mécanisme du guichet unique, institué par le RGPD, n'est pas applicable en matière de dépôt de cookies, dans la mesure où les règles qui le régissent sont prévues par la directive *ePrivacy*. L'autorité de protection des données nationales n'est, en effet, pas toujours compétente pour faire appliquer l'*ePrivacy*. L'autorité compétente peut être l'équivalent de l'ARCEP dans les autres pays européens. Il n'existe pas de coordination européenne dans les textes actuels. Seule une autorité nationale est compétente pour vérifier le respect de cette directive.

S'agissant de l'Irlande, l'organisme de régulation est face à un enjeu de crédibilité du modèle. Un certain nombre de décisions a déjà été pris pour activer tous les échelons du RGPD. Certains observateurs estiment que nous n'aboutissons pas suffisamment rapidement sur des projets de décisions irlandaises portant sur les acteurs majeurs de l'écosystème numérique. Certains estiment qu'il convient de changer les règles de gouvernance du RGPD.

Quant à elles, les autorités européennes pensent que le RGPD est un texte solide, qui mérite d'être conservé et accompagné dans son application, en renforçant la coopération entre les autorités et en leur donnant davantage de moyens. Si certains droits nationaux rendent

difficile l'aboutissement à des décisions nationales, il appartient à la Commission européenne d'intervenir.

En tout état de cause, la CNIL souhaite renforcer l'efficacité de la coopération européenne en continuant à s'appuyer sur le RGPD, qui constitue une force de l'Europe dans toutes les négociations au niveau international. La CNIL contribue au renforcement de la coopération en utilisant tous les outils à sa disposition, comme les lignes directrices du CEPD sur la coopération européenne, qui clarifient les procédures, le RGPD ou les demandes d'assistance. En dernier recours, elle a la possibilité d'adopter des mesures d'urgence en cas d'atteinte grave au droit des personnes.

M. Philippe Latombe, rapporteur. De nombreux observateurs craignent l'existence d'un problème par rapport à la CNIL irlandaise et aux GAFAM, du fait de leur proximité et de l'intérêt économique que ces dernières représentent pour l'Irlande.

Les GAFAM ont l'habitude de faire de l'entrisme ou du lobbying. Le ressentez-vous à la CNIL ? D'autres CNIL européennes l'ont-elles évoqué ?

M. Gwendal Le Grand. Ces sociétés pratiquent évidemment du lobbying sur notre doctrine. Elles cherchent à participer aux consultations publiques, lors de la publication de lignes directrices par exemple, pour faire valoir leurs positions, mais les autorités de protection sont indépendantes dans la prise de leurs décisions. Les montants des sanctions sont d'ailleurs nettement plus élevés qu'avant 2018, puisque le plafond est passé de 150 000 euros à 3 millions d'euros, voire 4 % du chiffre d'affaires mondial d'une entreprise.

Il est essentiel d'assurer la solidité de nos décisions devant les juridictions, y compris pour l'Irlande. J'en veux pour preuve que nos décisions sont de plus en plus attaquées devant le Conseil d'État, voire la Cour de justice de l'Union européenne. Chacun respecte sa procédure nationale et peut être contraint par ses propres difficultés. La Commission européenne a aussi son rôle à jouer si des procédures nationales font obstacle à l'application du droit de l'Union européenne.

M. Philippe Latombe, rapporteur. Une suite d'arrêts de la Cour de justice de l'Union européenne, *Tele2 Sverige* et *Prokuratuur*, est actuellement devant le Conseil d'État. Même si elle concerne essentiellement l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP), quelles conséquences en tirez-vous à la CNIL ?

M. Gwendal Le Grand. La CNIL se charge de faire appliquer les décisions de la Cour, qui relèvent de son champ de compétences. Une décision a, par exemple, été prise sur le droit à l'oubli par la Cour de justice de l'Union européenne. La CNIL applique la jurisprudence de la Cour. Elle n'a pas de position à émettre sur les décisions de la Cour de justice de l'Union européenne. Elle n'a d'ailleurs pas produit d'écritures en observations.

Concernant les cas de conservation des données de connexion, nous pouvons relever la constance des arrêts de la Cour, qui s'est prononcée de façon cohérente à plusieurs reprises, à plusieurs années d'intervalle, sur des sujets similaires.

M. Philippe Latombe, rapporteur. Si le Conseil d'État confirme la décision de la Cour de justice de l'Union européenne, vous serez *in fine* chargé de vérifier l'application de l'arrêt.

M. Gwendal Le Grand. Bien sûr, nous sommes dans un État de droit, dans lequel le législateur détermine des règles, qui peuvent être attaquées de différentes manières. La CNIL est chargée de faire appliquer la législation, parfois éclairée par des décisions de la Cour de justice de l'Union européenne.

M. Philippe Latombe, rapporteur. Compte tenu du volume, ne craignez-vous pas une rapide augmentation de la charge de travail ? Si le Conseil d'État confirme la décision de la Cour de justice de l'Union européenne, un certain nombre de procédures judiciaires s'en trouveront affectées. Les personnes mises en cause dans ces procédures pourraient saisir la CNIL pour demander l'application de l'arrêt du Conseil d'État.

M. Gwendal Le Grand. Je ne peux pas anticiper cette situation, qui est conditionnée par de nombreuses questions.

D'une manière générale, la CNIL continue de demander des moyens supplémentaires pour exercer convenablement ses missions. Nous sommes aujourd'hui 225 agents. À la fin de l'année 2021, nous serons 245, alors que les Anglais comptent entre 600 et 700 agents. Selon la Commission européenne, la France présente le troisième plus mauvais ratio pour son nombre d'agents de la CNIL rapporté au nombre d'habitants. Nos missions sont extrêmement larges, car la problématique des données personnelles est commune à toute l'économie numérique. Il est donc essentiel que l'autorité soit suffisamment dotée pour protéger les droits fondamentaux des citoyens.

M. Philippe Latombe, rapporteur. Comment entrevoyez-vous la suite avec vos homologues anglais après le mois de juin 2021 ? Le RGPD continue à s'appliquer jusqu'à cette date, mais la Grande-Bretagne pourra ensuite modifier son système de protection des données, en se rapprochant, par exemple, du modèle américain.

M. Gwendal Le Grand. Un projet de décision d'adéquation est en cours de discussion entre l'Europe et le Royaume-Uni pour pouvoir continuer à transférer des données sans formalité. Le CEPD a été saisi du sujet et doit se prononcer prochainement.

À ce jour, les données peuvent continuer à transiter, même si le Royaume-Uni ne fait plus partie du CEPD et ne relève plus du guichet unique. Une période de transition a été aménagée dans l'attente de la mise en œuvre de cette décision d'adéquation.

M. Philippe Latombe, rapporteur. En France, la carte nationale d'identité électronique et l'identité numérique sont largement évoquées. La CNIL est évidemment à la pointe sur cette question. Elle a rendu des avis sur la carte nationale d'identité et le système des titres électroniques sécurisés (TES) il y a quelques jours. Comment jugez-vous l'état d'avancement de la France dans ce domaine par rapport aux autres pays européens ?

M. Gwendal Le Grand. L'identité électronique recouvre plusieurs sujets. Un Règlement européen impose aux États membres de déployer une carte d'identité électronique avant août 2021. Dans ce contexte, le décret TES a été modifié pour permettre à l'État de créer de nouvelles cartes d'identité intégrant un composant électronique, dans lequel se trouvent des données biométriques en application d'un Règlement européen.

La question de l'identité numérique est plus large. Le gouvernement a porté plusieurs initiatives telles que FranceConnect et Alicem, sur lesquelles la CNIL a été amenée à se prononcer. Des textes ont ensuite été publiés pour contrôler leur application.

Un certain nombre de critères sont importants par rapport à l'identité numérique. Premièrement, une personne n'a pas besoin d'avoir une identité unique en ligne. Dans le monde réel, elle peut interagir avec un certain nombre de personnes, qui n'ont pas besoin de connaître l'ensemble des données de son état civil pour lui faire confiance et réaliser des transactions avec elle.

Deuxièmement, il existe un certain nombre de principes en termes de protection des données. Il s'agit tout d'abord de se demander qui peut voir les transactions que la personne réalise avec un acteur du privé et quelle est la nature des données présentées lors d'une authentification. Par exemple, pour s'inscrire à la bibliothèque, une personne doit seulement prouver qu'elle habite la commune sans forcément donner l'ensemble des attributs de son identité. De la même manière, pour accéder à certains services, elle aura besoin de fournir une preuve d'âge sans pour autant décliner son identité complète.

Ces principes doivent être portés par les solutions d'identité électronique. La CNIL n'est bien sûr pas opposée à un renforcement de la sécurité en ligne, qui est essentielle pour protéger les données personnelles et prévenir les risques d'usurpation d'identité, mais les solutions d'identité électronique ne doivent pas aboutir à une identité numérique unique, quel que soit le service auquel la personne souhaite accéder. Le respect des règles du RGPD et de la Loi Informatique et Libertés est indispensable.

M. Philippe Latombe, rapporteur. Pensez-vous que l'État à une bonne connaissance et un respect correct du niveau de protection des données ?

M. Gwendal Le Grand. Cette question est extrêmement large. Dans un État de droit, les textes sont appliqués, après avis du Conseil d'État et de la CNIL. En outre, des autorités contrôlent les fichiers mis en place par l'État.

Pendant la crise sanitaire, la CNIL a mené un travail spécifique pour accompagner à la fois les acteurs privés et les pouvoirs publics, en se prononçant sur SI-DEP, Contact Covid, le système d'information Vaccin Covid et à plusieurs reprises sur TousAntiCovid.

Courant 2020, la CNIL a ensuite réalisé une trentaine de contrôles sur les systèmes d'information mis en place par l'État dans la crise sanitaire. Elle doit donc avoir suffisamment de moyens pour être en mesure de répondre rapidement aux demandes, dans sa mission de conseil. Cet impératif s'est illustré pendant la crise sanitaire, période pendant laquelle elle a été extrêmement sollicitée pour se prononcer sur le recours au télétravail, les caméras de comptabilisation des masques, les drones, etc.

La CNIL fait face à des attentes fortes de la part des pouvoirs publics, du secteur privé et des parlementaires, qui ont besoin de connaître rapidement l'avis de la CNIL pour prendre position sur des questions souvent inédites.

La CNIL est une autorité dont l'indépendance est garantie par les textes et la constitution de la CNIL. Il lui arrive également de prendre des sanctions, y compris vis-à-vis d'acteurs du secteur public. Si ses moyens sont renforcés, elle pourra encore mieux exercer ses missions.

M. Philippe Latomb, rapporteur e. Votre pouvoir de sanction vis-à-vis de l'État est-il suffisant ? Je prends l'exemple des drones, sur lesquels vous avez eu une position très ferme vis-à-vis du ministère de l'Intérieur. Celui-ci continue toutefois à les utiliser, en vous renvoyant à votre simple pouvoir d'injonction. Vos pouvoirs de sanction ou d'interdiction doivent-ils être renforcés vis-à-vis de l'État ?

M. Gwendal Le Grand. Nous avons déjà d'importants pouvoirs de sanction. Notre priorité est de disposer de procédures de sanction simplifiées, notamment pour doter le président de la formation restreinte de la CNIL de nouvelles attributions dont l'exercice ne nécessite pas nécessairement l'intervention de l'ensemble du collège des sanctions. Cette configuration serait applicable aux seules affaires simples et de faible gravité et le montant des sanctions financières serait limité.

Aujourd'hui, toutes les affaires sont traitées avec le même niveau d'assurance juridique par la formation restreinte au complet.

Nous avons aussi, au-delà du pouvoir d'injonction, un poids sur le débat public. Les positions de la CNIL sont entendues et relayées. Ses positions peuvent d'ailleurs appuyer des recours devant les juridictions.

M. Philippe Latombe, rapporteur. Quelles sont, selon vous, les principales atteintes aux données ? Quelles sont les évolutions technologiques dont les atteintes en résultant pourraient vous donner le sentiment d'être désarmés ? Quelles évolutions législatives et réglementaires devraient être adoptées en urgence pour que vous puissiez continuer à exercer votre activité ? Je pense, par exemple, à l'intelligence artificielle.

M. Gwendal Le Grand. Nous avons identifié trois priorités en matière de contrôles en 2021 par rapport aux enjeux de protection des données : les cookies, la sécurité des données de santé et la cybersécurité.

Les cookies entrent dans le champ des lignes directrices, de la recommandation et des sanctions déjà évoquées. À compter de la publication des lignes directrices et de la recommandation en octobre 2020, nous avons donné aux entreprises un délai de six mois pour se mettre en conformité avec les nouvelles règles. Ce délai expire donc fin mars 2021. Dès lors, nous contrôlerons le respect de ces textes en matière de cookies.

Concernant la sécurité des données de santé, nous constatons le développement de systèmes d'information dans le domaine de la santé. Ils figuraient déjà dans notre programme de contrôle l'an dernier, mais ce dernier s'est décalé du fait de la crise sanitaire. Nous les avons donc à nouveau inscrits dans notre programme de contrôle. En pratique, nous menons des investigations sur les violations de données signalées à la CNIL et sur l'évaluation de la sécurité des établissements de santé et des laboratoires.

Enfin, s'agissant de la cybersécurité, nous nous attachons en particulier aux sites web, qui touchent le quotidien numérique des Français. L'objectif de nos contrôles est de monter le niveau de sécurité des sites web français les plus utilisés dans différents secteurs et relevant d'organismes de toutes tailles, publics comme privés. Nous portons une attention particulière aux formulaires de recueil de données à caractère personnel, à l'utilisation de la technologie « https » et au recours à des mots de passe suffisamment robustes.

Face à l'intelligence artificielle, nous ne sommes pas désarmés, mais cette technologie nécessite une meilleure interrégulation. En 2017, nous avons publié un rapport sur la façon de permettre à l'Homme de garder la main face aux algorithmes et à l'intelligence artificielle. Il est consultable sur le site de la CNIL. Il a fait suite à une série de débats engagés en 2017 et permet de dégager les principes applicables à l'intelligence artificielle, qui ont d'ailleurs été repris par divers forums de discussion au niveau européen et international.

Sur la reconnaissance faciale, la CNIL avait publié un rapport fin 2019, car cette technologie peut faire appel à l'intelligence artificielle.

L'une des spécificités de la CNIL est de posséder une expertise technique très pointue, qui lui permet de comprendre comment fonctionnent ces systèmes, afin d'être en mesure de les réguler correctement en appliquant, avec l'aide de ses juristes, des principes technologiquement neutres inscrits dans le RGPD.

M. Philippe Latombe, rapporteur. Le CSA a émis un avis indiquant que l'accès aux sites pour adultes, à caractère pornographique, ne peut pas être rendu uniquement possible en cochant une case pour certifier de sa majorité. Elle demande que soit trouvé un système robuste pour contrôler la majorité des personnes souhaitant y accéder.

Le CSA préconise un système de paiement avec une carte bancaire, même si en posséder une n'est pas forcément une preuve de la majorité. Les sites concernés ont lancé une grande consultation pour savoir ce que leurs utilisateurs accepteraient pour prouver leur majorité, depuis la photographie de la carte d'identité au moyen de la webcam jusqu'à l'obtention d'un numéro dans une institution publique. Toutes ces pistes portent atteinte à la protection des données personnelles. Avez-vous échangé avec le CSA ? Plus généralement, quels sont vos rapports avec les autres autorités administratives, comme l'ARCEP, qui peuvent impacter les données ?

M. Gwendal Le Grand. Nous échangeons régulièrement avec les autres autorités administratives indépendantes. La CNIL est également saisie par l'autorité de la concurrence. L'interrégulation est primordiale, car les données personnelles sont utilisées dans tous les secteurs. L'interrégulation prend d'ailleurs corps dans les projets de texte au niveau européen.

Pour répondre à la question de la vérification de l'âge, le micropaiement n'est pas forcément efficace. En outre, le principe du RGPD de minimisation des données doit être respecté. Ainsi, les traitements nécessaires à la vérification de l'âge doivent être proportionnés aux risques pour les personnes concernées, en l'occurrence, les enfants.

Pour avoir vu le questionnaire de ces sites, j'ai pu constater que certaines méthodes proposées peuvent effectivement paraître très intrusives à leurs utilisateurs.

M. Philippe Latombe, rapporteur. À partir de ces exemples, pourriez-vous émettre spontanément des recommandations sur la méthode à employer auprès du CSA ?

M. Gwendal Le Grand. La question de la méthode de vérification de l'âge est actuellement étudiée par un groupe de travail, car elle se pose également pour l'accès des mineurs à des sites de réseau social.

Ce sujet est également européen. Une mesure d'urgence a été prise par notre homologue italien envers Tik Tok en ce qui concerne la vérification de l'âge. Il a été demandé à Tik Tok de modifier un certain nombre de paramètres par défaut pour vérifier que les utilisateurs ont l'âge requis pour s'inscrire à ce réseau social.

Cette question est techniquement difficile et la réponse dépend du contexte. En outre, ce sujet est de niveau européen.

M. Philippe Latombe, rapporteur. Vous avez été saisi par France Digitale d'une demande concernant Apple. Nous avons le sentiment que les « vilaines » GAFAM sont porteuses de tous les maux et que la souveraineté numérique serait de s'en affranchir. Capitalisent-elles vraiment le plus de risques et le plus de conflits ou s'agit-il d'un effet de loupe ? Est-il si difficile de leur faire comprendre la protection des données à l'européenne ? Sommes-nous si irréprochables vis-à-vis de nos entreprises ?

Nous entendons parler des Chinois uniquement par rapport à Huawei, mais peu par rapport à leurs applications de places de marché et de réseau social, alors qu'elles sont similaires à celles des GAFAM.

M. Gwendal Le Grand. En tant que régulateur, nous adoptons une approche indifférenciée vis-à-vis des acteurs. Les GAFAM sont majoritaires, tant en volume de données traitées qu'en nombre de plaintes qui nous sont adressées, leurs services étant massivement utilisés par les citoyens français. Nous traitons également les problématiques d'acteurs non américains. Tik Tok, par exemple, intéresse également les autorités nationales et européennes.

Encore une fois, des moyens dont nous disposons dépend le champ que nous sommes capables de couvrir au niveau européen. Vos exemples montrent la diversité des sujets auxquels nous sommes confrontés au quotidien, alors que nous ne sommes que 225 agents.

M. Philippe Latombe, rapporteur. Y a-t-il une question que nous n'avons pas abordée ?

M. Gwendal Le Grand. Non, je pense avoir couvert les principaux points.

Nous avons parlé du HDH, du développement d'un *cloud* souverain. La période nous offre une opportunité assez unique d'alignement des intérêts de politique industrielle et de protection des données. Ces problématiques se rejoignent, car le développement d'un *cloud* souverain nous permettra de conserver la maîtrise de nos données, de relever le niveau d'indépendance au niveau européen et de renforcer le niveau de cybersécurité des entreprises. Il servira ainsi nos droits fondamentaux et la protection des données. Toutes les déclarations des décideurs politiques sur la politique industrielle, la protection des données et le plan de relance vont dans le sens d'un meilleur contrôle, par la France et par l'Europe, des données traitées dans les infrastructures informatiques.

Nous devons profiter de cet alignement d'intérêts pour collectivement nous atteler au développement de solutions nous permettant d'être plus efficaces et plus agiles dans un environnement cyber plus sécure.

M. Philippe Latombe, rapporteur. Merci pour le temps que vous nous avez consacré et pour vos réponses. Nous sommes preneurs de vos futures contributions si vous avancez sur la protection des données de santé et d'autres sujets d'actualité.

M. Gwendal Le Grand. Nous nous tenons à votre disposition pour vous fournir des informations complémentaires sur les décisions de la CNIL. Nous vous adresserons les réponses au questionnaire dans les prochains jours.

M. Philippe Latombe, rapporteur. Lors des auditions avec les chercheurs en santé, ils ont formulé un souhait d'une plus grande rapidité et d'une meilleure fluidité dans le traitement de leurs demandes d'accès au SNDS. Il serait intéressant de leur transmettre un mode d'emploi simplifié.

M. Gwendal Le Grand. Dans le domaine de la recherche en santé, de nombreuses procédures simplifiées existent. Dans la plupart des cas, il n'est pas nécessaire d'obtenir une autorisation de la CNIL, tant que la demande est déclarée conforme à la méthodologie de référence. Des instruments génériques fluidifient effectivement les traitements.

Dans le cas de la crise Covid, nous avons mis en place une procédure spécifique pour autoriser les recherches le plus rapidement possible. Plus de 90 % des recherches impliquant

la personne humaine ont pu être mises en œuvre, sans avoir à constituer un dossier auprès de la CNIL, sous couvert de leur conformité à une méthodologie de référence. Par ailleurs, sur près de 50 % des dossiers, l'autorisation a été délivrée en moins de deux jours.

Je rappelle à ceux qui estiment que la CNIL se montre un peu trop tatillonne vis-à-vis des données de santé que les fuites de données ont des conséquences lourdes. Un fichier contenant les données de 500 000 patients de laboratoires a récemment été découvert libre d'accès sur Internet. Or le domaine de la santé est particulièrement sensible.

M. Philippe Latombe, rapporteur. Mon propos visait simplement à vous engager à rappeler les bonnes pratiques, pour que les chercheurs n'aient pas ce sentiment.

Audition de M. Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) *(25 mars 2021)*

Présidence de M. Philippe Latombe, rapporteur.

(Les propos tenus au cours de l'audition à huis clos n'ont pas fait l'objet d'un compte rendu.)

Audition, ouverte à la presse, de M. Fabrice Brégier, président de Palantir France, de MM. Olivier Tesquet, journaliste spécialisé dans les questions numériques à Télérama, et d'Olivier Laurelli, cofondateur de Reflets.info *(25 mars 2021)*

Présidence de M. Philippe Latombe, rapporteur.

M. Philippe Latombe, président et rapporteur. Nous auditionnons cet après-midi M. Fabrice Brégier, président de Palantir France et ancien directeur général d'Airbus. Notre mission d'information a répondu favorablement à la demande de Palantir d'échanger avec nous et de participer à nos travaux. Nous accueillons également deux spécialistes des questions numériques, M. Olivier Tesquet, journaliste à Télérama et auteur d'un ouvrage récent, « État d'urgence technologique : comment l'économie de la surveillance tire parti de la pandémie », et M. Olivier Laurelli, journaliste hacker et cofondateur du site Reflets.info.

J'aimerais évoquer trois sujets principaux.

Je voudrais d'abord savoir ce que recouvre, selon vous, la notion de souveraineté numérique. Cette question rituelle de la mission est importante. Le sujet fait l'objet d'une attention croissante des pouvoirs publics depuis la crise sanitaire. Lors des auditions passées, nous avons eu l'occasion d'entendre plusieurs définitions de cette notion très large, que certains rapprochent parfois d'une forme d'autonomie stratégique ou décisionnelle. J'aimerais comprendre comment, en tant qu'acteur privé américain spécialiste du big data, vous appréhendez cette notion.

Je souhaiterais également vous interroger sur les solutions technologiques que vous proposez, que vous nous les présentiez succinctement, nous fournissant à grands traits leur fonctionnement. J'aimerais aussi savoir ce qui fait leur spécificité par rapport à l'offre de vos concurrents. Alors que certains pays, dont la France, entreprennent de se doter d'outils souverains, je me demande comment vous analysez cette dynamique européenne et mondiale.

Enfin, je voudrais que nous revenions sur les critiques qui vous ont été adressées, concernant la protection des données et votre proximité avec certains acteurs étrangers. Je souhaiterais ainsi savoir quelles sont les garanties proposées à vos clients, notamment publics, pour éviter que des données sensibles ne fassent l'objet de captations indues. Ce point fait également le lien avec les enjeux d'extraterritorialité du droit américain, le *Cloud Act*, le *Foreign Intelligence Service Act (FISA)*, sur lesquels nous travaillons. J'aimerais savoir s'il existe des finalités pour lesquelles vous auriez déjà refusé ou vous pourriez refuser l'utilisation de vos solutions technologiques.

M. Fabrice Brégier, président de Palantir France. Vos travaux sont essentiels et portent sur un thème majeur. Palantir est un acteur important du big data dont beaucoup parlent alors que peu le connaissent. Ce n'est pas nécessairement de leur faute. Jusqu'à récemment, Palantir n'était pas une entreprise qui communiquait systématiquement sur ses produits et ses clients. Les règles ont changé dès lors que Palantir s'est introduite en bourse, en octobre dernier. Elle est désormais régie par une transparence très forte sur ses clients et ses produits, qui permettra de démystifier l'entreprise.

Le thème de la souveraineté est pour moi fondamental. J'ai travaillé dans l'industrie aéronautique pendant vingt-cinq ans. J'ai été à la tête d'entreprises souveraines de la défense

ou de l'aéronautique, dans des secteurs clés pour notre industrie, en concurrence notamment avec de grands groupes américains, des sociétés très fortes dans le domaine.

En matière de numérique, la question de la légitimité ne se pose pas. Nous nous cachons quelque peu derrière l'Europe pour parler de la France. Le numérique est un domaine qui devient prépondérant. Il l'est déjà dans nos vies personnelles et Palantir est un acteur *B to B* très spécifique. Il le devient dans la vie publique, les modes de travail, les modes de vie, les modes de société. Il est normal qu'il y ait des débats sur la façon de réguler ce développement du numérique, sur les règles qui doivent être établies au plan national et sur la confiance que l'on place dans les acteurs.

Le numérique devient un différenciant majeur. On l'a vu pendant la crise du Covid. Pris de court, nous avons du mal à coordonner les services, à gérer la pénurie, à préparer la logistique pour la vaccination. Des solutions existent et sont mises en œuvre pour permettre ce genre d'actions au niveau des États, pour la lutte contre la grande criminalité, la fraude, le terrorisme, la protection des personnes, avec des débats politiques sur l'utilisation de telles technologies sans lesquelles nos populations sont moins protégées. C'est le soutien à nos forces. Je crois que la ministre des Armées l'a rappelé, le numérique devient aussi important qu'un avion de chasse ou un missile dans un certain nombre de missions. C'est aussi le cas pour le compte des entreprises, qui n'ont pas d'autre choix que de protéger leurs données et de les valoriser.

Palantir reste une petite société. Vous n'êtes pas face au représentant d'Oracle, d'Amazon, de Google ou de Microsoft. C'est une entreprise qui a un peu plus de 2 500 employés. Elle a été créée en 2004 dans la Silicon Valley, à la suite des attentats de septembre 2001, avec la conviction des trois fondateurs, qui sont restés actionnaires, dont l'un est président du conseil d'administration et un autre directeur général, que les nouvelles technologies permettraient de prévenir de tels attentats en regroupant l'ensemble des informations, qui étaient très dispersées, mais qui existaient, afin de les mettre à disposition des services d'enquête pour éviter ces attentats. Il s'agissait du fondement même de la création de cette société. Depuis, elle s'est développée sur ce créneau sécuritaire, aux États-Unis, mais aussi dans de nombreux pays d'Europe. La France a choisi cette solution pour son efficacité, en 2016. À partir de 2013-2014, les technologies ont été développées pour permettre aux entreprises commerciales de disposer d'outils qui favorisent l'intégration et la valorisation de leurs données.

Malgré sa faible taille, environ 1,1 milliard de dollars, mais en très forte croissance, Palantir est l'un des acteurs reconnus comme majeurs dans le big data. Elle a développé des technologies qui sont en pointe et qui n'ont pas d'égal, dès lors que l'on gère une grande complexité de données. La communauté de la tech la reconnaît comme telle.

Palantir travaille à la fois pour des gouvernements, le gouvernement américain notamment, mais aussi les démocraties occidentales, les pays européens, le Japon et la Corée du Sud. Elle ne travaille pas avec l'ensemble des pays. Elle ne travaille pas en Chine, en Russie et dans des pays dans lesquels l'utilisation de tels logiciels pourrait ne pas respecter certaines règles d'éthique du point de vue des fondateurs de l'entreprise.

Les missions gouvernementales sont variées. Elles ne sont pas limitées aux domaines que j'ai mentionnés. Elles peuvent aller de la lutte contre la fraude et la criminalité à des missions de préparation de plans d'investissement pour la transition énergétique ou la préparation des transports de demain. Elles peuvent concerner le soutien à une politique de santé dynamique, à grande échelle. Les applications sont devenues nombreuses. Des missions sont également menées pour certains ministères de la Défense, comme la maintenance du

matériel, le regroupement des informations des capteurs du champ de bataille qui permettent aux troupes d'être davantage protégées.

Concernant l'entreprise, la plateforme Foundry – qui n'est pas spécifique, car nous ne sommes pas des experts d'un domaine particulier, nous sommes des experts de la donnée – valorise à très grande échelle les données fournies par le client lui-même, à partir d'un déploiement très simple, sur l'architecture qu'il a choisie. Cette plateforme couvre pratiquement tous les modules importants de la chaîne du big data. Elle se connecte aux données que le client souhaite intégrer. Elle en facilite la préparation, le nettoyage, la mise à jour. Elle donne ensuite la main aux opérationnels qui, par l'intermédiaire de modules, peuvent visualiser la donnée, faire du *reporting*, de l'analyse ou développer de l'algorithmie d'intelligence artificielle.

Nous ne sommes pas présents dans deux domaines. Le premier est l'algorithmie, qui doit être, selon nous, largement maîtrisée par le client et les entreprises avec lesquelles celui-ci souhaite travailler. Nous avons la chance d'avoir un grand nombre de *start-up* françaises extrêmement performantes et dynamiques. Le second domaine est celui de l'hébergement des données. Les solutions de Palantir fonctionnent avec de nombreuses solutions d'hébergement, des *clouds*, et, pour des usages stratégiques, gouvernementaux ou bancaires, des serveurs internes, ce que l'on appelle *on premise*. Ces derniers sont conservés et pilotés par le client. Les données ne sont pas diffusées à un tiers partenaire de *cloud.*

En d'autres termes, la spécificité de Palantir est d'avoir su intégrer dans une plateforme logicielle d'une grande simplicité d'utilisation, mais d'une grande complexité technologique, la continuité numérique, depuis la donnée source jusqu'à la mise à disposition de cette donnée aux opérationnels, y compris aux *data scientists*.

Les points forts sont cette capacité à se connecter à n'importe quelle source de données, de n'importe quel volume et n'importe quel niveau de complexité. Ce point a été démontré à de très nombreuses reprises.

Un autre avantage est la sécurité de la plateforme. Elle est essentielle dès lors que l'on regroupe des informations. Cela suppose qu'à travers cette plateforme, le client puisse établir une gouvernance de la donnée qui lui permette de vérifier les accès qu'il donne, pour quelle raison telle personne de l'organisation a accès à telle donnée. La plateforme permet aussi de tracer les *logs*, c'est-à-dire retrace qui utilise la plateforme et pour quel usage, de voir les modifications opérées par le client sur les données sources, avec une grande transparence sur les évolutions algorithmiques et logicielles mises en œuvre. L'objectif est de garantir une sécurité, une segmentation essentielle dès lors que l'on regroupe beaucoup de données.

À titre d'exemple, Airbus avait décidé de créer un écosystème pour être connecté à tous ses clients, compagnies aériennes, notamment pour améliorer la performance en service des avions. Des échanges de données sont acceptés entre les compagnies aériennes et Airbus, mais non entre les compagnies aériennes elles-mêmes, qui sont concurrentes. Cette plateforme a permis de le faire et de le démontrer à plus de cent reprises puisque 130 compagnies aériennes sont connectées à cette plateforme Skywise, pilotée par Airbus, qui est une première mondiale à cette échelle.

Une des autres spécificités de notre plateforme est que son *design* permet au client de respecter la loi et la protection des données personnelles. Vous me direz que c'est la moindre des choses, mais ce n'est pas partout évident. Il s'agit du *legal by design*. Nous n'avons pas eu à modifier le logiciel lorsque le Règlement général sur la protection des données (RGPD) a été édicté. Bien au-delà, nous permettons au client d'avoir une granularité beaucoup plus

fine que ce qui est demandé actuellement par la loi. Non seulement nous ne regrettons pas la mise en œuvre du RGPD, mais ce type de règle est essentiel pour combiner l'utilisation de technologies qui sont indispensables pour que la France se modernise et ne soit pas dépassée par rapport à d'autres pays. Nous continuons ainsi à obéir à des règles d'éthique qui peuvent être tracées, contrôlées et auditées.

De plus, je n'ai guère vu de solution qui permette à des non-experts d'utiliser les données sur une plateforme. Foundry le permet. Elle fait le lien entre le monde de la donnée, de l'analytique et le monde opérationnel. Par exemple, si je suis un technicien de maintenance, je sais, sans formation particulière dans le numérique, utiliser des modules qui ne nécessitent pas que je sache coder ou même utiliser des tableaux Excel. Si je suis un ouvrier d'Airbus, un compagnon sur la chaîne d'assemblage, je vais pouvoir m'assurer qu'en cas de problème de qualité, j'ai des aides à la décision qui viennent du logiciel.

Le logiciel permet à diverses équipes de collaborer sur un sujet donné. C'est un élément essentiel de ce que peut apporter l'intégration des données. Nous savons faire travailler des sous-traitants avec des clients, différents secteurs d'activité qui sont normalement dans des « silos » organisationnels, notamment dans de grands groupes.

Enfin, je n'ai pas vu de limite de taille ou de complexité dans la gestion de bases de données de nos clients.

Je présente souvent Palantir comme un anti-GAFA, non seulement par la taille, mais aussi parce que nous ne récupérons pas de données. Nous nous refusons à faire du *data crunching*, c'est-à-dire aller récupérer des données pour le client. Des données sont disponibles en *open source*, de l'*open data*, ce qui est différent. Tout le monde a accès à ces données et nous permettons à nos clients de les intégrer très simplement.

Nous l'avons fait à de nombreuses reprises auprès de nos clients industriels pendant la crise du Covid. Il y avait beaucoup d'informations publiques. Ces entreprises devaient pouvoir réagir, établir des scénarios, faire des simulations en fonction des évolutions de l'épidémie, qui impacte la demande, leur clientèle, mais aussi leur base de sous-traitance, leurs flux d'approvisionnement. Nous avons apporté ces éléments en temps réel.

En outre, nous ne stockons pas les données. Ainsi, ce que j'entends sur le fait que Palantir récupérerait les données, de santé ou d'autres domaines, de ses clients et deviendrait le « roi du monde » est faux. Palantir n'a pas accès aux données, sauf lorsque le client demande un soutien spécifique d'ingénieurs de Palantir pour l'aider à atteindre des objectifs opérationnels.

Dans le travail d'enquête sur la lutte antiterroriste, l'un des domaines sensibles, les ingénieurs de Palantir et les enquêteurs ne travaillent jamais « main dans la main ». Les enquêteurs ont été formés pour valoriser eux-mêmes leur travail. Lorsqu'il y a besoin d'un soutien technique particulier, les équipes de Palantir sont présentes. En France, ce sont des ingénieurs français sortant des plus grandes écoles, qui ont été habilités, avec le degré adéquat d'habilitation, par le ministère de l'Intérieur.

Nous ne manipulons pas les données des clients. Nous ne les vendons pas, nous ne les monétisons pas. Nous permettons au client de valoriser lui-même sa mine d'or constituée de toutes les données disponibles, beaucoup plus vite qu'avec toute autre solution. Il peut soit rattraper son retard, soit prendre de l'avance sur les solutions plus classiques du big data qui sont proposées par de plus grands groupes. Palantir a investi au total environ 3 milliards de dollars depuis sa création, dans seulement deux plateformes logicielles, l'une pour un usage

d'enquêteur gouvernemental, l'autre, générique, pour l'ensemble des autres activités, notamment commerciales.

Enfin, vous pouvez penser que si vous travaillez avec Palantir, vous serez « scotchés » à tout jamais avec nous, que si vous déployez la plateforme logicielle, vous serez pieds et poings liés, ce qui peut vous poser un problème de souveraineté. Vous ne voulez pas dépendre d'un partenaire dans la durée. Sachez d'abord que la plupart de nos clients étendent leurs contrats et que dans le domaine commercial, où la concurrence est forte, la durée moyenne de ces contrats s'établit à plus de six ans, ce qui montre une relation de confiance.

De plus, la plateforme logicielle n'est pas basée sur des codes propriétaires, que vous trouverez chez des éditeurs que je ne nommerai pas, dont certains sont français. Vous choisissez leur logiciel, il peut être excellent, mais ensuite, il est quasiment impossible d'en sortir. J'ai vécu cette expérience dans l'aéronautique, au moins auprès de deux grandes entreprises mondiales. Là, vous avez une plateforme logicielle dont la propriété intellectuelle appartient à Palantir, mais tout ce qui est développé peut l'être avec des codes du commerce, de l'*open source*. Tout ce qui est développé par le client lui appartient. Nous ne discutons pas de ces points.

Nous avons également démontré, à de nombreuses reprises, la réversibilité de la solution. Un client qui a développé son intégration et son analyse de données sur la plateforme peut, dès lors qu'il y aurait un concurrent meilleur ou français, changer simplement cette solution. Nous faisons évoluer en permanence les technologies et nous conservons une longueur d'avance sur la concurrence. Notre intérêt commercial est d'expliquer au client qu'il n'est pas bloqué avec nous et que nous travaillons dans un partenariat qui peut évoluer dans la durée. Nous espérons conserver le client, mais il peut sortir.

En France, nous sommes passés d'une trentaine d'ingénieurs, lorsque j'ai rejoint Palantir, fin 2018, à un peu plus d'une centaine. Nous sommes restés stables l'année dernière. Ce sont des ingénieurs de très haut niveau, qui ont une double compétence. Ils ont évidemment une compétence de *data science*. Ils sont capables de maîtriser parfaitement les outils, de former des utilisateurs. Ils ont aussi un sens *business* qui leur permet d'appréhender les enjeux opérationnels des clients. S'il s'agit, par exemple, de qualité de produits en usine, il faut être capable d'aller dans des usines et de s'interfacer avec de vrais opérationnels, les aider à comprendre ce qu'ils peuvent faire de cette plateforme.

Nous avons très peu d'équipes commerciales, ce qui est sans doute un point de faiblesse. Nous essayons de vendre notre produit à travers son excellence technique et notre approche de partenariat.

Nous avons la volonté de devenir, malgré la nationalité de la société mère, un acteur français de la tech – piloté par des ingénieurs français, lorsque cela est demandé. De plus en plus de groupes internationaux sont basés en France et nécessitent des équipes internationales, mais dans les cas de missions de souveraineté, il est bon de proposer des ingénieurs de talent, qualifiés, si nécessaire habilités et français.

Enfin, nous nous inscrivons dans un cadre où nous ne sommes pas un spécialiste de l'intelligence artificielle. Nous facilitons très grandement le travail des *start-up* qui, elles, pour la plupart, sont focalisées sur une application, sur des algorithmes qui permettent de donner de la valeur dès lors que les données sont disponibles. Nous sommes le catalyseur d'un écosystème. Je viens d'un grand groupe, le groupe Airbus. Il n'y avait pas que les avions dans ce groupe, il y avait aussi les activités de défense. Nous étions en discussion avec tous les autres « gros », ces grands groupes n'ayant ni l'ADN ni l'intérêt de développer un écosystème

de *start-up* françaises qui viendraient petit à petit montrer qu'elles sont plus dynamiques et casser leur monopole.

C'est d'ailleurs ce que Palantir a fait aux États-Unis. Pendant des années, elle a été rejetée du ministère de la Défense. Les « gros » là-bas s'appellent Northrop Grumman, Lockheed Martin, Boeing et bien d'autres. Ils étaient en relation privilégiée avec le ministère de la Défense et se lançaient dans de très grands programmes qui coûtaient des milliards de dollars, une somme à l'échelle américaine, alors que ces « zouaves » de Palantir venaient avec des solutions logicielles qui ne coûtaient même pas 10 % de ces sommes. Ils ont été rejetés pendant des années. Il a fallu qu'ils se battent avec persévérance pour faire changer les règles d'achat aux États-Unis et faire en sorte que les solutions logicielles soient démontrées avant d'être achetées. Si nous procédions ainsi en France, nous aurions beaucoup plus de *start-up* qui deviendraient des licornes.

Je n'ai pas la prétention de vous apporter la définition de la souveraineté du groupe Palantir. Je vous donne la mienne, en tant que président de Palantir France, citoyen et, je l'espère, acteur de la souveraineté, au moins pendant ma carrière dans l'aéronautique. Pour moi, être souverain, c'est être capable de maîtriser son destin, être capable, dans le domaine du numérique, de faire appel aux meilleures technologies pour atteindre nos objectifs. Ils peuvent être de protéger la nation française, de réformer l'État, d'avoir une politique de santé dynamique, en utilisant les meilleures technologies, tout en en contrôlant l'usage. La technologie numérique, si elle est bien faite, permet les deux.

Pour moi, la souveraineté numérique française ou européenne tient dans cette capacité à définir ses propres règles. La France et l'Europe n'ont pas tout à fait les mêmes règles que les États-Unis ou le Royaume-Uni. Il revient à l'Europe de définir ses règles, comme elle le fait dans GAIA-X. Elle doit dire ce qu'elle attend en tant que client, le *check and balance*, définir un cadre clair et faire en sorte qu'il soit toujours possible, par le politique, de vérifier comment l'administration utilise les solutions numériques.

M. Philippe Latombe, rapporteur. Ce n'est pas méchant, mais vous seriez une femme, je vous épouserais tout de suite. Vous avez toutes les qualités. Vous présentez la société Palantir comme respectant la totalité de toutes les règles. Vous dites que vous n'avez même pas eu besoin de modifier le logiciel au moment de l'arrivée du RGPD parce que vous aviez un *legal by design* d'une granularité extrêmement fine. Comprenez-vous les « levées de bouclier » à l'encontre de Palantir, notamment parce que vous vous êtes exprimé sur la souveraineté française et européenne dans une émission de télévision ?

Nous devrons aussi parler de vos origines et de votre capital. Vous dites que vous êtes petit, mais vous pesez quand même autour de 20 à 25 milliards de dollars de capitalisation. Vous générez 1,1 milliard de dollars de chiffre d'affaires. Comprenez-vous ce mouvement, qui est aussi lié à GAIA-X ? Le fait que vous vous associiez au projet a généré une levée de boucliers et une inquiétude très forte de l'écosystème numérique français et européen. On ne comprend pas comment une société américaine de votre calibre participe de la souveraineté française ou européenne.

M. Fabrice Brégier. La souveraineté, c'est bâtir cet ensemble de règles, ce n'est pas être opposé à toute évolution technologique, et je sais que vous ne l'êtes pas. C'est utiliser le meilleur de ces technologies, sans lesquelles la France sera définitivement dépassée, c'est une certitude, au plan militaire, de la réforme de l'État, de son efficacité et de la performance de ses entreprises. C'est aussi en définir les règles pour qu'elles soient compatibles avec nos règles d'éthique, pour qu'il y ait un espace de confiance, pour que cela puisse être bâti dans

une architecture de souveraineté, avec des supra-acteurs complètement souverains. C'est aussi stimuler un écosystème créateur de valeur pour la France.

La définition pourrait être autre, et j'ai parfois l'impression que c'est le cas. Votre question me le fait penser. Si pour vous, la souveraineté, c'est utiliser des solutions françaises, nous aurons des soucis, et je ne parle même pas de Palantir, je parle des GAFA, pour pouvoir les rattraper et faire en sorte que chaque Français puisse utiliser des logiciels purement français. Là, vous êtes soumis au lobbying des grands groupes franco-français. Ce lobbying est très simple : il consiste à dire que la souveraineté est un point tellement important qu'elle doit être pilotée par des acteurs français. Je pense que c'est une mauvaise définition. La souveraineté est très importante, vous en définissez le cadre. Il est évidemment nécessaire de faire en sorte que des acteurs français émergent, que des *start-up* se développent au plan national, qu'elles soient soutenues. Peut-être, dans certains domaines sensibles, faut-il seulement des acteurs français compte tenu de cette sensibilité, mais la souveraineté, ce n'est pas faire le lit des lobbyistes des grands groupes français, dont je faisais partie il y a peu de temps.

Je n'ai pas d'acteurs de lobbying chez Palantir. En ayant rejoint Palantir France, je pense que je contribue à la performance de mes clients, à ce que les clients commerciaux jouent d'égal à égal avec leurs grands rivaux. J'ai contribué à ce qu'Airbus, en s'appuyant sur Palantir, pourtant société américaine, relègue Boeing au second plan sur le digital. Demandez aux acteurs du monde de l'aéronautique ce qu'ils en pensent. Il y a cinq ans, Boeing était pourtant très en avance sur Airbus. L'avons-nous fait la « fleur au fusil » ? Non. Nous avons audité cette société, nous avons regardé sa façon de travailler. Dans ce cas spécifique, puisqu'il n'y avait que deux acteurs au plan mondial, nous avons demandé à Palantir d'exclure Boeing de ses clients potentiels. Le résultat est manifeste et démontre que cette association a permis à Airbus de gagner non seulement en performance, mais aussi en relation avec ses clients.

Cette souveraineté peut aussi être au service de l'État. Quand j'aide indirectement un État comme la France à lutter contre le terrorisme, je pense que c'est un acte souverain, que la nationalité du logiciel n'a aucun intérêt et que dans le cas où un logiciel français arriverait à réaliser cette performance pour d'autres raisons, il serait possible de nous remplacer. Nos solutions sont réversibles.

S'agissant de GAIA-X, je l'ai dit, nous ne sommes pas un acteur du *cloud*. Nous sommes en relation avec ces sociétés du *cloud*. Nous travaillons avec Amazon, Azure, Google, avec des systèmes propriétaires auprès de nombreux clients gouvernementaux. Nous ne souhaitons pas définir notre propre politique, mais partager notre expérience parce que notre intérêt est que l'Europe se dote de règles claires pour avoir des *clouds* dits souverains.

M. Philippe Latombe, rapporteur. Vous avez légèrement transformé mes propos. Je vous posais simplement la question de savoir comment vous perceviez ce qui est dit sur vous. Je n'ai pas posé de définition particulière de la souveraineté dans ma question.

Sur les *clouds*, nous avons des questions juridiques. Palantir est-elle soumise à des règles extraterritoriales américaines ? Si oui, lesquelles ? Y a-t-il eu des demandes de la part d'autorités américaines vis-à-vis de Palantir ? Qu'y avez-vous répondu ? Comment répondez-vous à ces demandes quand elles sont présentées ? Nous avons une vraie question sur l'extraterritorialité : le fait que vous soyez Palantir France n'exclut pas des règles extraterritoriales américaines.

M. Fabrice Brégier. Palantir n'a pas accès aux données de ses clients. Elle n'héberge pas les données. Elle n'est pas un acteur du *cloud*. Vous choisissez Palantir et, par exemple,

AWS pour la solution *cloud* ou Microsoft Azure, les deux grands *leaders* dans le domaine de l'entreprise. J'espère qu'OVH arrivera prochainement à ce niveau grâce à son partenariat avec Google. Le client décide qui héberge ses données, avec ses propres clés de cryptage. Palantir n'étant pas un acteur du *cloud*, elle n'est pas soumise au *Cloud Act*. À ma connaissance, depuis que je suis chez Palantir, nous n'avons jamais reçu une demande de la nature que vous évoquez.

M. Philippe Latombe, rapporteur. Vous ne répondez pas sur le *FISA*.

M. Fabrice Brégier. Je ne sais pas ce que vous évoquez. Nous déployons une plateforme logicielle totalement maîtrisée par le client. Même si nous étions sous pression de quelque autorité, nous ne pourrions pas transférer de données. Nous ne sommes pas dans une logique de *cloud provider* américain, qui, même avec un hébergement de données en France ou en Europe, peut être sous pression de son instance dirigeante puisqu'elles sont hébergées sur ses propres serveurs. Nous n'avons pas à être soumis à ces règles.

M. Olivier Tesquet, journaliste spécialisé dans les questions numériques à Télérama. À vous écouter, Palantir serait une entreprise franco-française. Il manque tout de même des éléments de contexte importants. Cette entreprise a été fondée après les attentats du 11-Septembre, avec des fonds d'In-Q-Tel, le fonds d'investissement de la CIA. Le palantir, pour une personne qui serait familière de l'univers du Seigneur des Anneaux, c'est cette pierre qui permet de voir partout, tout le temps. Ce nom signe tout de même un pedigree.

S'agissant de souveraineté ou de sentiment d'appartenance à une nation ou à une valeur, je relisais avant cette audition la documentation qu'avait fournie Palantir à la *Securities and Exchange Commission (SEC),* l'autorité des marchés financiers américaine, juste avant son introduction en bourse. Je lisais la lettre qu'avait transmise Alex Karp, le patron de l'entreprise. Il écrivait que les solutions logicielles de Palantir étaient utilisées par les États-Unis et leurs alliés. La formulation m'a quelque peu interpellé, parce qu'elle montre que nous sommes face à une entreprise américaine qui évolue dans un environnement constitué de pays considérés comme amis.

Après avoir lu cette petite phrase, me sont revenus immédiatement en mémoire les propos de Jean-Jacques Urvoas, qui n'était pas encore garde des Sceaux à l'époque, mais président de la commission des lois de l'Assemblée nationale. Il avait déclaré : *« Les États-Unis n'ont pas d'alliés, ils n'ont que des vassaux et des cibles. »* Il ne parlait pas spécifiquement du renseignement, mais c'est particulièrement vrai dans ce domaine.

Dans ces conditions, je m'interroge sur l'obédience d'une société comme Palantir, qui a comme membre fondateur Peter Thiel. Il est le grand argentier conservateur de la Silicon Valley, mais il a le droit d'avoir l'appétit et les affinités politiques qu'il souhaite. Nous ne sommes pas face à quelqu'un qui est anodin. Dans des écrits de 2009, il a, par exemple, fait des déclarations indiquant que la liberté et la démocratie n'étaient pas forcément des valeurs très compatibles. Il est un libertarien, avec une vision assez absolutiste. Je me souviens également d'une interview qu'il avait donnée sur Reddit en 2014. Il y expliquait que Palantir n'était pas une façade de la CIA, la CIA était une façade de Palantir. Il pouvait s'agir d'une provocation, mais ces propos interpellent malgré tout. Ils peuvent susciter une forme de méfiance.

M. Fabrice Brégier nous a également expliqué que Palantir était l'anti-GAFA, mais Peter Thiel siège au conseil d'administration de Facebook. Nous avons appris ces derniers mois qu'il avait financé la société Clearview, à hauteur de quelques millions de dollars, ce qui n'est certes pas grand-chose. Elle fait de la reconnaissance faciale. En aspirant des visages sur

Internet, elle a construit la plus grande base de données de reconnaissance faciale, vendue ensuite à des forces de police, ce qui a suscité plusieurs contentieux.

M. Fabrice Brégier. Vous n'interrogez pas Peter Thiel.

M. Olivier Tesquet. Je sais, mais vous êtes le représentant d'une entreprise dont le cofondateur est Peter Thiel.

M. Fabrice Brégier. Peter Thiel est quelqu'un de très respectable, mais nous n'allons pas passer une demi-heure sur lui. Nous pourrions passer une demi-heure sur le vrai dirigeant opérationnel, Alex Karp, qui a le profil opposé. C'est un juriste qui possède un doctorat de philosophie, qui est démocrate et pro-européen.

M. Olivier Tesquet. J'entends que le « pedigree » de M. Karp est différent. Je remarque d'ailleurs que chaque fois qu'il s'agit d'éteindre l'incendie, comme quand Palantir est accusé d'être le bras armé de la politique migratoire de Donald Trump et de favoriser l'expulsion de milliers de clandestins aux États-Unis sous la mandature précédente, on envoie Alex Karp pour faire un peu de relations publiques. Il n'aura échappé à personne qu'il était plutôt d'obédience marxiste, qu'il a étudié avec Habermas quand il était en Allemagne. Personne ne le conteste. Je me souviens toutefois d'une interview au *Financial Times*, à l'automne dernier, dans laquelle il expliquait que ce qui se jouait était une bataille pour l'Intelligence artificielle entre les États-Unis et la Chine et que l'hyperpuissance qui remporterait ce combat régnerait sur le monde.

Je sais que ce n'est pas l'audition de Peter Thiel, mais celui-ci dirige un fonds d'investissement, le *Founders Fund*. Il finance un certain nombre d'entreprises. Je pense à une autre société qui tire son nom du Seigneur des Anneaux qui s'appelle Anduril, fondée par Palmer Luckey. Il a créé les casques Oculus de réalité virtuelle. Parmi ses premières inventions, il avait mis au point un mur virtuel qui avait vocation à remplacer le mur physique que ne pouvait pas se payer Donald Trump.

Nous sommes donc quand même face à une entreprise qui vise une protection assez explicite des intérêts américains, qui est présentée comme telle. Il me semblait important de le rappeler. Par ailleurs, je pense que ces interrogations infusent assez haut dans l'appareil d'État en France. La DGSI travaille depuis longtemps sur des alternatives à Palantir pour essayer de s'en dégager. Je crois savoir, et je ne suis probablement pas le seul dans cette réunion, que la solution ne fait pas l'unanimité au sein de l'état-major français.

M. Fabrice Brégier. Je ne sais pas ce qui vous permet de dire cela.

M. Olivier Tesquet. Un projet qui s'appelle OTDH a vocation à remplacer Palantir.

M. Fabrice Brégier. Je ne peux pas vous laisser dire cela. Le partenariat est suffisamment confidentiel pour que je n'en divulgue pas les détails. Il a été exemplaire, après un début difficile. Tout le monde est « tombé » sur le choix de la solution américaine, « Palantir agent de la CIA », début 2016, notamment toutes les entreprises françaises qui, à l'époque, en échange d'une somme de l'ordre de 500 millions d'euros, étaient prêtes à développer, en trois ans, un logiciel pour le compte de la DGSI. Ainsi, pendant trois ans, nous ne faisions rien, nous ne luttions pas efficacement contre le terrorisme. Or, trois ans après, il n'y a toujours pas de solution disponible et notre contrat, lui, a été prolongé pour au moins trois ans. Prendre ce contrat juste pour ses propres intérêts, à coups d'argent public, pour essayer de développer une solution nationale qui ne marche toujours pas, six ans après, je considère que c'est agir contre la souveraineté de la France.

M. Philippe Latombe, rapporteur. Cette question fait partie de celles que cette mission a soulevées depuis de nombreuses auditions.

M. Fabrice Brégier. C'est pourquoi je suis ravi de pouvoir m'exprimer sur le sujet.

M. Philippe Latombe, rapporteur. Vous vous présentez comme un anti-GAFAM. Or, nous savons qu'il y a eu une volonté hégémonique des GAFAM de prendre commercialement la place, de prendre le marché et d'instaurer leurs propres standards. Qu'est-ce qui rassurerait et montrerait que Palantir ne ferait pas la même chose à terme ?

Vous nous dites également que vous stimulerez l'écosystème. Vous l'avez dit vous-même, Palantir a été retenu par la DGSI pour le premier appel d'offres de trois ans, renouvelé par un deuxième appel d'offres de trois ans. Pendant ce temps-là, qui peut prendre votre place et qui peut avoir la surface technologique et l'expérience pour développer une solution ? N'est-ce pas antinomique d'être le *leader* et de dire que vous permettrez l'émergence d'un écosystème ? C'est une question ouverte, qui serait valable pour d'autres acteurs américains, pas simplement Palantir.

M. Fabrice Brégier. La phrase concernant les États-Unis et ses alliés correspond à ce que j'ai dit en d'autres termes : États-Unis et démocraties occidentales. J'y ai ajouté le Japon et la Corée du Sud, qui n'ont rien d'occidental, mais qui sont des alliés des États-Unis. L'image vise à rappeler que nous ne vendons pas ces logiciels au monde entier. Regardez les entreprises françaises d'armement : elles vendent à un spectre beaucoup plus large, sans savoir ce que sera l'utilisation finale de ces armements, avec l'accord de l'État. Là, c'est une autocensure de Palantir. Vous pouvez l'interpréter et faire de la genèse de texte pour savoir si la France est un véritable allié des États-Unis, mais arrêtons. La France, l'Allemagne, les pays nordiques, le Royaume-Uni, l'Europe du Sud, le Japon, la Corée sont clairement dans cette catégorie. Ce n'est pas une demande des États-Unis, c'est une autocensure décidée par Alex Karp, compte tenu de l'importance de telles technologies et des garde-fous qui doivent être prévus. Elles doivent être utilisées par des démocraties, qui définissent ensuite leurs propres règles.

Palantir assume de travailler pour les gouvernements, contrairement aux GAFA. Les GAFA ont pris l'argent des États-Unis et ont tourné le dos au gouvernement américain. C'est en tout cas ce qu'affirme Alex Karp. Nous, nous assumons totalement d'avoir des missions de souveraineté pour les gouvernements, et pas seulement pour le gouvernement américain. Travailler dans les pays d'Europe du Nord n'est pas simple. Il faut leur démontrer tout ce qui doit être fait pour la protection des données personnelles. C'est au moins aussi sévère qu'en France.

Nous l'avons fait dans tous les pays, si ce n'est qu'en France, nous avons des entreprises qui n'acceptent pas qu'une *start-up* de cette nature, qui, certes, emploie maintenant 2 500 salariés, prenne leur place. Elles ont des capacités de *lobbying* et font jouer la fibre nationale, pour ne pas dire nationaliste, et celle concernant In-Q-Tel et la CIA. Or, la France doit agir de la même façon.

Le métier d'In-Q-Tel est de dénicher des pépites qui peuvent aider à la sécurité nationale des États-Unis. Palantir a été un bon choix de ce point de vue. Je ne sais même pas si In-Q-Tel est toujours au capital. Le fonds n'apparaît pas dans les rapports dans la mesure où le capital est désormais détenu en totalité par des investisseurs privés. Les règles de marché régissent Palantir, mais ces fonds ont permis à la société de prendre des risques et de se développer au-delà de ses investisseurs d'origine.

En France, il me paraîtrait intéressant que Bpifrance continue son travail remarquable d'investissement dans des entreprises de taille intermédiaires (ETI) ou même des grands groupes stratégiques, mais aussi dans les fonds d'investissement à l'usage de la tech et des *start-up*. J'ai également en tête le fonds Definvest, piloté par le ministère des Armées, qui investit dans des *start-up* de la tech. Dirions-nous que ces *start-up* sont dans la main du ministère de la Défense français, ne peuvent pas travailler à l'étranger, ne peuvent pas exporter ? Certainement pas. Un coup de pouce leur est donné et cela s'arrête là. Le parallèle doit être fait avec Palantir, qui assume de travailler pour les États, contrairement aux GAFA.

La capitalisation boursière des GAFA se situe autour de 1 000 milliards de dollars. Nous n'en sommes pas encore là. Nous ne sommes pas du tout comparables à la taille d'un GAFA. Nous n'avons pas les mêmes pouvoirs de *lobbying*, en France, en Europe ou à Bruxelles. Nous n'avons personne. Nous sommes une petite structure.

Nous aidons les clients à valoriser leurs données, nous n'y avons pas accès et nous n'avons pas l'intention de les monétiser, de les transformer ou de les vendre. Je ne peux pas le dire plus simplement. C'est un schéma établi. Même quand on nous demande si nous pouvons faire du *crunching* de données, sur Facebook ou autres, nous nous y refusons. C'est au client de le faire. D'autres entreprises ont moins de scrupules et le font pour lui. Nous, nous prenons les données de nos clients et nous les aidons à les valoriser et à les intégrer. C'est pour ces raisons que cette appellation d'anti-GAFA fait sens quant aux règles de comportement.

M. Olivier Tesquet. Je suis d'accord avec vous sur plusieurs points, mais je n'ai pas particulièrement de fibre nationale ou nationaliste sur ces questions. Je ne suis pas lobbyiste. Je crois que mon travail sur ces sujets me confère un certain totem d'immunité sur ce point.

M. Fabrice Brégier. Absolument.

M. Olivier Tesquet. Je vous rejoins sur le fait que, contrairement aux GAFAM, votre actif principal n'est pas publicitaire. Il ne provient pas de données personnelles que vous vendriez au plus offrant pour garantir votre hégémonie commerciale. En revanche, la manière dont vous présentez les choses donne presque l'impression que vous êtes une entreprise caritative et je ne vois pas très bien comment vous créez de la valeur.

M. Fabrice Brégier. Nous vendons notre logiciel.

M. Olivier Tesquet. Oui, des entreprises achètent le logiciel et paient des licences. En revanche, que se passe-t-il concrètement quand une entreprise, une administration ou un ministère veut se désengager ? Je me souviens d'un contentieux avec la police de New York. Quand elle a voulu se désengager de Palantir, elle a eu toutes les peines du monde, non pas à récupérer ses données, puisque celles-ci lui appartenaient, mais l'interprétation qui en avait été faite. Qui est propriétaire de cette analyse ? Quand Palantir signe avec le *National Health Service (NHS)*, le système de santé publique britannique, celui-ci fournit ses données hospitalières dans un contexte sanitaire compliqué, avec gradation du contrat d'une livre symbolique, puis à un million de livres et jusqu'à vingt-trois millions de livres. Je suppose que des simulations sont réalisées à partir de ces données : ces données sont-elles alors entre vos mains ?

M. Fabrice Brégier. La réversibilité est un sujet fondamental. Les développements réalisés par le client, que ce soit les travaux sur la donnée, les algorithmes, tout ce qui « tourne » sur la plateforme, lui appartiennent. Il n'y a pas de problème de propriété intellectuelle. Cette garantie est contractuelle. Ensuite, tous les développements dans des langages ouverts peuvent être réutilisés tels quels par une plateforme du même acabit, sans

difficulté. Nous avons aussi démontré à des clients qui souhaitaient changer de société de *cloud* que nous pouvions les aider à transposer toutes leurs données de la société A à la société B, en quelques semaines, ce qui constitue un exploit dans le cas d'un très grand groupe. Cette réversibilité existe donc.

Je suis dans le camp du pragmatisme. À supposer que la définition que vous retenez de la souveraineté soit d'en faire le maximum en France, dès lors qu'une solution française serait disponible, elle pourrait se substituer à celle de Palantir. Entretemps, que faisons-nous ? Rien ? Il y a des domaines considérables d'amélioration de la performance de l'État grâce à des solutions comme la nôtre.

Vous avez cité celui de la santé. Il est très sensible dans la mesure où il agrège des données personnelles et des données de santé. Sur nos plateformes, il n'y a pas de données personnelles. Elles sont regroupées et anonymisées. Une telle plateforme sert à suivre le comportement de l'épidémie. Vous n'avez pas besoin de savoir que Fabrice Brégier ou M. Dupond est dans telle ou telle catégorie. Généralement, le client lui-même prend ses propres protections, car il est, à juste titre, sous la supervision d'équivalents de la commission nationale de l'informatique et des libertés (CNIL). Les éléments sont utiles aux chercheurs, aux épidémiologistes pour suivre l'évolution de l'épidémie en temps réel à l'échelle du pays, de la région ou du quartier. La granularité forte maintient cette anonymisation.

La plateforme sert aussi à tout ce qui a trait à la chaîne logistique, autour de l'organisation des moyens de secours, des hôpitaux, de la vaccination. Ce n'est pas Palantir qui décide qui sera vacciné. Nous n'en savons rien. Les services de l'État coopèrent et décident quelle catégorie de population doit l'être. Ces personnes sont cependant pré-identifiées grâce aux bases de données et la diffusion peut être immédiate. En cas de changement, si une région devient beaucoup plus touchée, il est aussi possible de prendre des décisions immédiates et toute la chaîne logistique se met en œuvre.

Nous n'avons pas accès aux données personnelles, aux données de santé. Il n'y a pas de complot de Palantir qui nous permettrait de récupérer les données aux États-Unis, en Angleterre et dans d'autres pays du monde pour devenir le super connaisseur du domaine de la santé. Ce n'est pas ce que nous faisons et ce n'est pas ce que nous cherchons. Nous vivons en apportant des solutions immédiates, dans ce cas précis à une gestion de crise, en rendant service et en valorisant ce service à travers la vente d'une licence et le soutien d'équipes pour intégrer les données. Le seul lien qu'il peut y avoir avec des données intervient lorsque le client demande le soutien des ingénieurs de Palantir pour intégrer des données, toujours sur la plateforme d'hébergement du client. Ces éléments ne vont pas sur un serveur de Palantir. J'imagine qu'aux États-Unis et au Royaume-Uni, si ces ingénieurs répondent à des demandes de souveraineté plus poussée, ils seront aussi habilités.

Mes ingénieurs sont des ingénieurs de premier plan, qui ont la mission pour l'État chevillée au corps. Cela me fait mal au cœur pour eux qu'on suspecte qu'ils pourraient voler des données pour le compte de puissances étrangères alors que, par ailleurs, les portes sont grandes ouvertes pour des ingénieurs indiens, en sous-traitance de SSII françaises qui travaillent pour le Gouvernement français. Ce sont deux poids, deux mesures et vous devriez regarder ces aspects.

M. Philippe Latombe, rapporteur. Vous vendez des licences du logiciel Palantir. Vous n'êtes pas en langage propriétaire. Pour quelle raison personne ne vous a-t-il copié et n'arrive-t-il à avoir le même niveau que le vôtre ?

M. Fabrice Brégier. Le fait que toutes les interfaces ne soient pas en langage propriétaire ne veut pas dire que nous confions la propriété de ce que nous avons créé au monde entier. Nous protégeons notre savoir-faire. Si vous travaillez sur la plateforme de Foundry, vous n'êtes pas piégé parce que vous le faites avec des langages du commerce, que je ne vais pas énumérer. Ce sont les langages les plus classiques. Il s'agit d'un choix délibéré et raisonné. C'est le moyen d'avoir les logiciels les plus communs, donc sur lesquels la communauté d'ingénieurs travaille pour qu'ils soient les plus performants.

Selon notre vision, la vente de logiciels numériques se normalisera : d'ici quelques années, cinq ou dix ans, je ne sais pas, plus personne n'acceptera d'acheter des morceaux de logiciels qui ne se parlent pas entre eux et d'être obligé de faire un travail d'intégration. Quand vous achetez une voiture, on ne vous livre pas le moteur d'un côté et la boîte de vitesse de l'autre. Vous achetez un véhicule, avec l'intelligence intégrée à bord. Pour le numérique et le digital, ce sera la même chose. Vous ne pourrez le faire que si les briques sont basées sur du logiciel du commerce.

Pourquoi restons-nous à part ? Pourquoi même Microsoft ou Google ne font-ils pas ce que nous faisons ? Ils n'ont pas eu la même stratégie. Ils se sont surtout concentrés sur le *cloud*, qui est très profitable et nécessite d'énormes investissements. Ils possèdent cette capacité financière et de très bonnes technologies. Ils ont aussi misé sur l'Intelligence artificielle, l'analyse de la donnée, la création de la valeur, indépendamment de leur métier de GAFA. Palantir a travaillé sur l'amont, sur ce qui est aride, ce qui ne se voit pas : comment aider les clients à intégrer des sources de données disparates, de mauvaise qualité, pour leur permettre de remplir leur mission. Très peu d'entreprises l'ont fait de façon systématique. Nous avons une multitude de concurrents sur chacune des sous-briques, mais nous n'avons pas de concurrent frontal capable d'offrir cette solution. Cela ne veut pas dire que des clients ne peuvent pas développer leur transformation numérique sans Palantir, mais relier l'ensemble de ces sous-briques entre elles pour en tirer une véritable valeur suppose beaucoup plus d'efforts. Voilà le réel savoir-faire de Palantir, qui est le maitre d'œuvre de cette intégration de données.

Nous avons quand même investi trois milliards de dollars en R&D depuis la création de l'entreprise. L'avantage de ces sociétés américaines est que des investisseurs y croient. Dans notre cas, ils ont eu raison, mais ils auraient pu perdre leur investissement. Palantir reste un *leader* dans ce domaine.

M. Thomas Gassilloud. Le dilemme pour la France est de savoir si nous dépensons notre énergie en faisant confiance à une solution tierce, pour une efficacité à court terme, ou si nous faisons des efforts en interne, tout de suite, avec moins de résultats immédiats, mais en capitalisant sur le long terme. Nous pourrions énumérer le nombre de solutions technologiques pour lesquelles nous avons choisi d'investir dans nos propres solutions, avec des outils moins efficaces dans un premier temps, mais une autonomie stratégique par la suite. Plus nous attendons, plus il est potentiellement difficile de rattraper le retard. Le défi opérationnel pousse à développer des solutions.

Pour ma part, j'ai un peu plus de doutes sur la réversibilité de la solution de Palantir. Elle a l'air très efficace, mais elle impose quand même, en interne, dans les organisations, beaucoup de formations, de l'intégration. Elle ne serait donc pas immédiatement transposable.

En outre, je n'ai pas la vision complète des effectifs de Palantir en Europe, mais j'ai lu par ailleurs qu'il y avait 600 chercheurs en Angleterre et une centaine en France. J'aimerais connaître les effectifs au niveau de l'Union européenne. Je pense qu'il faudra une répartition si vous avez une ambition en Europe.

Je voudrais également modérer vos propos sur le fait que vous feriez peu d'efforts commerciaux. Je pense plutôt que vous faites des efforts gratuitement, en avant-vente, pour rencontrer des gens et leur demander leurs données pour voir ce que vous pourriez en faire. Je pense qu'avant de signer le contrat avec Airbus, Palantir a mis des ingénieurs à disposition pour faire parler les données. Avec les entreprises françaises, il y a peut-être un déficit quant à la capacité à investir de l'argent avant même de signer des contrats.

Enfin, j'aimerais votre avis sur Artemis.

M. Fabrice Brégier. Pourquoi opposer court terme et long terme ? Il faut être pragmatique. Les besoins sont flagrants. En tant que politiques, vous les voyez tous les jours. Ce n'est pas que la France est en retard, la situation est la même dans beaucoup de pays, y compris aux États-Unis. Des technologies existent pour faire un bond en avant. Il faut s'assurer qu'elles sont réversibles, que les données sont protégées. Ce point doit faire l'objet d'approbations par les services compétents. En revanche, pourquoi avoir une vision de long terme qui empêche d'agir pendant des années ? Si nous avions procédé ainsi dans l'aéronautique, nous n'aurions pas eu Eurocopter, qui s'appelle maintenant Airbus Helicopters, que j'ai eu l'immense honneur et plaisir de diriger pendant quatre ans. Nous n'aurions peut-être même pas eu l'aventure nucléaire. Il faut donc être pragmatique, répondre à des besoins qui sont très importants pour l'État français, en ayant la certitude que l'on peut changer de solution.

Dans une entreprise, si j'ai un logiciel Microsoft et que je veux passer à une suite Google, parce que Google a innové, ce n'est pas gratuit. L'entrepreneur le fait parce que c'est son intérêt et qu'il peut le faire. Il faudra cependant qu'il forme ses personnels à la nouvelle suite. Ce sont des coûts marginaux par rapport à ce dont nous parlons.

Ce n'est pas à moi de définir ce qui est à la fois souverain et français ou européen dans la souveraineté numérique, mais j'ai quelques pistes. Avec l'écosystème pour développer les *start-up* françaises, nous avons un atout fantastique. Ce n'est pas juste du marketing. Nous avons encore la chance d'avoir des ingénieurs de très haut niveau et reconnus comme tels par les Américains et les Britanniques. Beaucoup d'entre eux se lancent dans des *start-up*. Beaucoup échouent, certains sont sur le point de réussir. Il faut leur offrir un environnement qui ne soit pas seulement financier. J'ai la prétention de penser qu'une solution comme Palantir peut les aider à se développer, y compris à l'international, alors que nous ne sommes pas du tout sur ce créneau.

Le *cloud* souverain est une bonne chose. Doit-il exclure des solutions américaines ? Non, mais il revient à l'Europe et à personne d'autre de définir des règles. De même, nous avons des compétences de cyber, mais nous n'en sommes pas un acteur. La cybersécurité doit être nationale. On ne confie pas la protection d'un pan aussi important à des acteurs étrangers. Malgré mon côté européen, du fait de mes onze ans à la tête d'Airbus, j'aurais tendance à dire que ce domaine doit être français.

Voilà des thèmes, et il y en a d'autres, dans lesquels la France devrait investir massivement. Le peut-elle partout ? Peut-elle remplacer Palantir ? Peut-être. Peut-elle remplacer Google ? Vraisemblablement pas. Il faut choisir ses combats. En France, nous avons l'intelligence, mais nous n'avons pas tous les moyens. Le Quantique est un excellent exemple. Il n'y a pas de retard à rattraper. Nous avons des atouts. Nous investissons plusieurs milliards d'euros et le projet fonctionnera.

Il ne faut pas se tromper avec ce discours indiquant que la souveraineté correspond au tout français. Cela ne marchera pas, dans le numérique ou d'autres domaines. Prenez cette

réussite fantastique qu'est le groupe Safran dans l'aéronautique, que je connais encore mieux que le digital. La réussite de Safran vient d'une association à 50/50 avec *General Electric (GE)*, les vilains qui ont racheté Alstom. Cette association a permis à Safran de devenir *leader* des moteurs de l'A320 et du Boeing 737 et d'en faire un énorme groupe, si performant dans l'aéronautique. Quand j'étais Airbus et que j'achetais un moteur, je savais qu'il était 50 % américain et 50 % français. En 100 % français, il n'y aurait pas eu de moteur. Il faut donc être pragmatique dans ces domaines, avec les règles que vous avez évoquées.

Vous avez raison, notre développement en Europe a d'abord eu lieu au Royaume-Uni. Il y a environ 600 ingénieurs au Royaume-Uni. Ils développent une grande partie du logiciel Foundry. En France nous en sommes presque à une centaine d'ingénieurs, en Allemagne aussi. Nous avons des équipes dans d'autres pays européens, notamment en Europe du Nord. Sur les 2 500 à 3 000 employés de Palantir, je dirais que 1 000 employés sont européens. Nous sommes donc loin d'un groupe dirigé des États-Unis par les États-Unis. J'ai une très forte autonomie d'action, et j'espère de parole, dans ce groupe sur le périmètre de Palantir France.

Enfin, vous avez totalement raison sur la dimension d'efforts commerciaux. Je n'ai pas de vendeurs, mais j'ai une stratégie commerciale, c'est évident. Nous avons adopté celle-ci, car dans le big data, vous avez des dizaines, voire des centaines d'acteurs, vous avez de grands noms. Dire que Palantir peut aider les clients à faire mieux qu'avec ces acteurs est très difficile. Tout le monde a les mêmes explications : « On intègre les données, on vous les nettoie, on vous les met à disposition, vous en tirez de la valeur », si ce n'est que nous le faisons, rapidement, à grande échelle, sans limites. Notre but est de le démontrer d'abord au client. Que ce soit un gouvernement ou une entreprise, nous cherchons un cas d'usage autour de la donnée qui nous permette de faire la différence. À partir de là, nous commençons à discuter d'un partenariat éventuel.

Nous n'avons pas énormément de clients dans le monde. Nous en avons beaucoup plus que ce qui est cité, car il revient aux clients de divulguer leur relation commerciale avec nous, mais ils sont quelques centaines. Nous n'avons pas vocation à avoir un marché de très grande masse. Nous ne sommes pas Salesforce, qui vend des solutions adaptées, y compris à de petites entreprises. Nous nous adressons plutôt à des entreprises de taille assez importante ou pour des problématiques gouvernementales complexes.

M. Éric Bothorel. Appliquez-vous des traitements qui vous sont confiés par des clients à d'autres jeux de données ? Vous arrive-t-il aussi d'enrichir ces données de données en source ouverte, sur lesquelles vous « tomberiez » et qui n'auraient pas leur place en source ouverte ? Quel est votre comportement dans ce cas ?

M. Fabrice Brégier. Nous l'avons fait en situation de crise, sur le Covid. À ma connaissance, ce sont des données véritablement en source ouverte, elles n'ont pas été pillées de tel ou tel site et mises à disposition. Nous y veillons. Je n'ai cependant pas la capacité de vous dire que cela n'a jamais été fait par inadvertance, mais pour moi, la règle est simple : les données en *open data* peuvent être disponibles. Elles devraient d'ailleurs l'être afin de permettre à certaines *start-up* de faire un bond en avant. En revanche, il faut s'assurer qu'il s'agit véritablement de données ouvertes et non piratées.

Par ailleurs, nous vendons un logiciel, d'une grande complexité, avec de nombreux modules mis à disposition de tous nos clients. Nous ne vendons pas d'application spécifique verticale. Nous avons maintenant une bonne connaissance de l'industrie, des problèmes de maîtrise de la *supply chain*, de qualité, dans l'aviation, l'automobile ou de grandes industries, des problèmes de conformité dans le domaine bancaire ou de maîtrise de la relation totale d'un client. Nous avons de nombreux exemples de cette nature. Nous avons ce savoir-faire, mais

nous ne passons pas d'un client à l'autre avec l'étude que nous réalisons pour un client spécifique.

Je rappelle également que la plupart des analyses sont faites par le client lui-même. En tant qu'ancien entrepreneur, je considère qu'une entreprise et un service de l'État doit avoir ses *data scientists*, ses analystes capables de réaliser eux-mêmes leur propre analyse. Lorsqu'ils doivent traiter un sujet très pointu, ils peuvent faire appel à un sous-traitant, qui peut être Palantir, mais aussi Capgemini, Accenture, Sopra Steria et bien d'autres. Ils connaissent notre plateforme. Ils ont travaillé avec leurs ingénieurs, notamment pour le compte d'Airbus. Ils sont beaucoup plus introduits que nous auprès des entreprises françaises, car ils ont de nombreux clients. Personne n'est obligé de s'appuyer sur nos services.

En outre, ce n'est pas à moi de juger de l'opportunité d'Artemis. Je m'abstiens de commenter la nécessité pour la France de lancer un tel développement. La décision a été prise et il n'y a pas de raison de la mettre en cause, sauf si, après quatre années, on se rendait compte que le projet ne donnait rien et que c'était de l'argent public gaspillé. Ce n'est pas à moi d'en juger. Je pars du principe que cela doit progresser. Néanmoins, attendre qu'Artemis atteigne ses objectifs ambitieux et ne pas apporter de solutions aux militaires et aux opérationnels ne me paraît pas être la bonne option.

Par exemple, nos forces au Mali ont besoin de cartographies précises. Elles sont américaines. Elles viennent d'une société, Esri, qui a pignon sur rue. Faut-il attendre d'avoir une cartographie française pour leur apporter ce soutien ? Les yeux dans le ciel sont quelques drones qui, pour l'instant, sont d'origine américaine, alors qu'il y a un programme de drones européens. Offrons donc les bonnes solutions et basculons sur les solutions nationales si l'État le décide, qu'elles sont matures et efficaces.

M. Olivier Laurelli, cofondateur de Reflets.info. Je pense que nous resterons irréconciliables sur quelques points. Je souhaiterais revenir au tout début de votre présentation. Vous vous êtes clairement posé comme un marchand d'armes numériques en présentant Internet comme un champ de bataille, votre solution comme une solution de lutte contre la pédocriminalité, contre le terrorisme. Elle déborde forcément sur d'autres données, qu'on n'avait pas forcément prévu de vous confier, aujourd'hui à l'occasion d'une crise sanitaire avec des données de santé, demain peut-être d'une autre crise portant sur un autre aspect.

Seriez-vous en mesure d'affirmer que votre solution ne peut pas être *backdoorée* ? Pouvez-vous donner à vos clients, aux États et aux organisations diverses un accès au code source de vos applications pour qu'elles-mêmes auditent votre code ? La carte algorithmique voudrait que vous confiiez aussi vos « recettes de sorcier » à des clients qui vous confient des données stratégiques.

En outre, vous avez dit que vous ne vendiez qu'à de grandes démocraties. Je ne vais pas rappeler que ce n'est pas une grande démocratie qui a lâché la première bombe atomique. Êtes-vous en mesure de me jurer qu'on ne retrouvera pas dans les un, deux ou trois ans à venir votre solution au Moyen-Orient ou en Afrique ?

M. Fabrice Brégier. Sur votre premier point, vous partez du principe que ce que je dis est vrai. Vous me faites confiance puisque si vous imaginez des systèmes cachés pour voler les données, c'est que vous admettez que nous n'avons pas accès aux données.

M. Olivier Laurelli. Je n'aurais pas besoin d'accéder aux données. J'aurais simplement besoin d'accéder à un fichier de configuration, par exemple XML, avec les clés

API en clair stockées par votre logiciel. Je n'ai pas besoin d'accéder directement aux données quand je peux me servir où je veux.

M. Fabrice Brégier. Nos clients, gouvernementaux ou entreprises, sont parmi les plus performants dans ces domaines. Nous ne nous adressons pas à de petites entreprises qui n'ont pas de compétences. Les logiciels de Palantir ont été audités des dizaines, voire des centaines de fois. Aucun client n'a été capable de détecter des failles. Il n'y a jamais rien eu contre la sécurisation de ce logiciel, d'aucune agence de renseignement non américaine, d'aucun grand groupe. Airbus et nous-mêmes avions demandé à l'ANSSI de réaliser des audits. Le retour était quand même plutôt flatteur pour la solution Palantir. L'ANSSI aurait naturellement préféré une solution française, c'est son métier, mais elle n'a rien trouvé à redire du point de vue de la sécurité. C'est même plutôt l'inverse, nous aidons les entreprises à prendre conscience de la valeur de leurs données et à définir elles-mêmes des règles de sécurité beaucoup plus dures que celles qu'elles auraient imaginées, parce que la plateforme le leur permet.

Est-il arrivé qu'un client se plaigne d'une fuite de données ? Je ne le pense pas. Je n'en ai aucun exemple depuis que j'ai rejoint cette société. La réponse vous suffit-elle ? Quand on est sceptique, il en faut plus. Par votre métier, il est normal que vous fassiez contrepoids. Des labellisations, des audits par des tiers indépendants permettront de valider ce que vous dites.

De plus, le problème n'est pas de divulguer les codes sources à des personnes compétentes, mais de ne pas se faire voler ses secrets. Je ne vais pas vous les donner maintenant pour que vous les donniez ensuite à un tiers parce que Palantir ne vaudrait alors plus rien. En revanche, les audits de sécurité peuvent être faits à tout moment par les clients. Ce point est évidemment prévu dans nos contrats.

M. Olivier Laurelli. Je partage en partie avec vous la définition de la souveraineté numérique. Je fais une dichotomie entre la souveraineté numérique d'un côté et le « franchouillardisme » numérique de l'autre. Je ne suis cependant pas d'accord avec vous sur la solution à y apporter. La souveraineté de l'Europe passera quoi qu'il arrive, que ce soit dans l'IA ou dans les solutions logicielles, par du logiciel libre parce que nous ne pourrons pas rattraper le retard qui a été accumulé. Nous avons déjà des briques pour ne pas réinventer la roue.

J'aime bien votre manière de vous présenter en périphérie des GAFAM. Elle vous rend sympathique.

M. Fabrice Brégier. Je ne le fais pas pour cela.

M. Olivier Laurelli. C'est touchant. En revanche, d'un côté plus pragmatique, je retiens que vous êtes un vendeur d'armes numériques, et vous l'avez bien expliqué. Vous êtes conscient de ce que vous vendez. Vous vous êtes d'ailleurs comparé à des groupes qui vendent des armes numériques à des puissances. Je reviens à ma première question : si votre solution est *backdoorée*, vous ne pouvez pas vous porter garant. Vous n'avez pas donné le code source pour qu'il soit audité. Les résultats ont été trouvés en audit « black box », c'est-à-dire sans le code source. Si malheureusement un jour votre code est *backdooré*, cette *backdoor* se retrouvera sur Internet, avec ensuite une fuite de données. J'imagine que vous comprenez les inquiétudes que peuvent avoir certains de vos gros clients, certains des États à vous confier non pas directement des données, mais une solution logicielle permettant d'accéder à ces données.

M. Fabrice Brégier. Très honnêtement, je n'ai senti ces inquiétudes chez aucun des clients. Quand ils auditent le logiciel et qu'ils vérifient ce qu'il permet de faire, la traçabilité est telle qu'ils sont au contraire surpris de sa sécurité. Quand on y ajoute des audits techniques, comme je l'avais fait lorsque j'étais directeur général d'Airbus, les retours proviennent de plusieurs centaines de très grands clients dans le monde. C'est une référence.

Ensuite, ce que vous avez dit est assez vrai, le monde se dirige vers de plus en plus de logiciels ouverts, ce qui ne veut pas dire que des entreprises ne peuvent pas avoir leur propre know-how, que tout doit être sur le net et que l'on fait ce que l'on veut. Il y aura un développement beaucoup plus fort et les États devront d'ailleurs réguler ces initiatives.

Enfin, je ne parle pas d'armes numériques, mais de souveraineté. Ce sont des logiciels qui comportent des garde-fous, dès lors qu'ils sont utilisés par des clients qui les respectent. C'est pour cette raison que Palantir s'est refusé à travailler avec certains États.

M. Olivier Laurelli. Vous travaillez avec la Corée du Sud. Vous avez vu ce qui s'est passé là-bas avec l'équivalent de l'application de TousAntiCovid. Ils ont juré que jamais les données de santé ne seraient utilisées pour autre chose que la lutte anti-Covid. Or, elles ont été exploitées par la police locale dans des enquêtes judiciaires. On constate donc une dérive.

M. Fabrice Brégier. Je vous rejoins : le risque de dérive existe. C'est à la loi coréenne de s'appliquer en Corée du Sud. Je pense d'ailleurs qu'elle est une démocratie qui n'a rien à apprendre de la France. Peut-être que, dans le cas présent, sur lequel Palantir ne travaille pas, la loi a été violée. Il faut des garde-fous et des contrôleurs. Pour moi, c'est cela l'objectif principal de cette souveraineté. Ces plateformes logicielles, ces solutions numériques sont fantastiques, offrent des services que personne d'autre ne peut offrir, mais si les règles de déontologie, d'éthique, de protection des données personnelles ne sont pas respectées, il faut être capable de le vérifier et d'arrêter les dérives.

Par ailleurs, faire référence à la première bombe atomique est peut-être un peu excessif pour dire que les États-Unis ne sont pas une démocratie.

M. Olivier Laurelli. Il n'y a pas de règle. Malheureusement, les États-Unis ne jouent pas souvent avec les mêmes règles du jeu que nous.

M. Fabrice Brégier. Pendant l'administration Trump, il y a eu ces débats sur *l'Immigration and Customs Enforcement (ICE)* et les méthodes utilisées par l'administration Trump contre l'immigration illégale. En soi, cela n'est pas condamnable, mais la façon dont cela a été déployé l'a été. Nous avons été très clairs sur ce sujet : il revient à la justice américaine et au Parlement américain de définir des règles liées à cette démocratie et à l'application de telles solutions. Une bonne partie des salariés de Palantir n'étaient pas satisfaits de l'utilisation qui avait été faite. Il y a eu des débats en interne, auxquels j'ai pu assister. Chacun avait la possibilité de s'exprimer.

Nous assumons notre position. Nous travaillons pour ces gouvernements et les alliés ou les démocraties. C'est aux États, aux politiques, aux juges de ces gouvernements de définir les règles. Cette responsabilité n'incombe ni aux GAFA, ni à Palantir.

M. Olivier Laurelli. J'aimerais vous entendre dire que vous assumez que vous vendez des armes.

M. Fabrice Brégier. J'assume que nous vendons des solutions logicielles qui permettent à un État de devenir souverain ou d'acquérir une certaine supériorité. Nous ne

vendons pas des armes au sens missiles, avions de combat ou autre chose létale. En revanche, protéger des forces, faire en sorte que des menaces soient identifiées pour être détruites par d'autres acteurs, c'est du domaine d'un État souverain. Les solutions technologiques de Palantir le permettent.

M. Philippe Latombe, rapporteur. L'inquiétude de beaucoup de monde provient aussi du fait que des groupes, notamment américains, ainsi que l'État américain lui-même, se soient parfois affranchis des règles. Je pense aux révélations d'Edward Snowden sur des écoutes. Il existe un réflexe d'inquiétude. Ce n'est pas méchant, mais lorsqu'on sait que Palantir est à l'origine financée par des fonds provenant des services américains, ces questions sous-jacentes se posent forcément.

De manière plus technique, comment étalonnez-vous le succès de votre logiciel ? Vous nous dites que vous le vendez en licence à un gouvernement, à une société, et que vous n'avez pas accès aux données. Vous ne savez donc pas comment il apporte des résultats dans la pratique à l'entreprise ou à l'État qui vous l'a commandé. Comment l'étalonnez-vous, sur quelle base ? Avez-vous des retours d'expérience de vos clients ? Comment vérifiez-vous qu'ils sont le fruit des données qui y ont été introduites au départ ?

M. Fabrice Brégier. Nous avons ces retours. Des ingénieurs de Palantir sont en soutien sur des opérations ponctuelles, à la demande du client. Généralement, elles ont lieu au démarrage afin que le client prenne la main sur la plateforme.

Nous avons les retours de nos clients du monde de l'entreprise, parce qu'ils sont beaucoup plus ouverts. Nous ne parlons pas du tout de données personnelles. Il s'agit de données de capteurs d'avion, de problèmes de qualité en service des automobiles, d'optimisation de la maîtrise des sous-traitants, de la résolution de problèmes techniques. Vous avez des milliers de logiciels américains qui s'en occupent. Palantir n'a pas de raison particulière d'être suspectée par rapport aux autres.

Dans le domaine gouvernemental, nous n'avons pas de retour sur le travail d'enquête, qui est du strict ressort des analystes des services de renseignement. Ils appliquent leurs propres règles pour ceux qui ont à en connaître. En revanche, quand on me demande d'aider à mettre en place un dispositif particulier lors d'un événement international qui se tient en France, nous apportons notre contribution technique, mais le travail de ces agences est réalisé par leurs personnels.

Dans la très grande majorité, le travail d'analyse, le développement des algorithmes est réalisé par les clients eux-mêmes ou leurs sous-traitants. Nous ne sommes que 2 500, voire légèrement plus, à l'échelle mondiale, pour plusieurs centaines de clients. Nous ne pouvons pas nous permettre d'avoir des armées d'ingénieurs, dont le but serait de savoir ce qui se passe chez le client. Nous sommes là pour nous assurer qu'il comprend la valeur qu'il peut en tirer, qu'il sait parfaitement utiliser l'outil et qu'il prend progressivement la main avec une conscience de ce que le digital et la maîtrise de ses données lui permettent de réaliser.

Lorsqu'il s'est agi de connecter l'ensemble des compagnies aériennes clientes d'Airbus, ce qui représente un travail de titan, Palantir a eu pour mission de démarcher les compagnies aériennes et de réaliser la connexion à la plateforme d'Airbus avec leur accord. Il s'agissait d'une tâche spécifique.

M. Philippe Latombe, rapporteur. Je n'ai pas eu de réponse sur le *FISA*. Si vous avez, parmi vos 2 500 salariés, un juriste capable de contribuer par écrit sur ce plan, nous

serions preneurs. Ce n'est pas seulement le *cloud* qui nous intéresse, c'est la partie de l'extraterritorialité, du droit, qui nous pose de véritables questions.

M. Fabrice Brégier. Nous apporterons la réponse en complément de mes propos. Ils étaient imparfaits sur ce point, j'en suis conscient.

M. Philippe Latombe, rapporteur. Le sujet pourra faire l'objet d'une question supplémentaire aux questions écrites que nous vous avons adressées.

M. Fabrice Brégier. Très bien.

M. Olivier Tesquet. Nous savons que les ingénieurs de Palantir sortent des meilleures écoles. Ils sont des Polytechniciens, des X-Télécoms. L'entreprise se gargarise d'ailleurs à juste titre d'employer des salariés de très haut niveau. Ma crainte n'est pas tant celle d'un « siphonnage » que celle de la délégation de pans entiers de ce que j'estime être un pouvoir régalien, que ce soit des fonctions de police, des politiques de santé, à ce qui reste des boîtes noires.

Les audits sont évidemment imparfaits puisque Palantir est une société qui possède, selon ma comptabilité personnelle, un peu plus de 1 000 brevets. Ils sont autant d'obstacles qui se situent entre nous et une transparence sur la manière dont fonctionne le logiciel. J'ai l'impression que nous sommes face à une situation dans laquelle nous nous habituerions à manger un plat étoilé sans en connaître la recette. Comment pourrions-nous nous prémunir contre ce risque ? Je cite de nouveau l'exemple du NYPD, la police de New York, qui s'était vu opposer la propriété intellectuelle de Palantir au moment d'accéder à l'analyse des données qu'elle avait injectées dans le logiciel. Cette situation engendre des questions d'opacité.

De mon point de vue, le débat porte donc moins sur l'aspect français/pas français, et je n'ai pas de chapelle préférentielle, que sur ce qui est traçable et ce qui est opaque.

M. Fabrice Brégier. Je suis conscient que ce n'est pas en une heure et demie de débat que je vais vous convaincre que nos solutions sont transparentes, traçables, auditables. Cela doit être fait par des experts indépendants de Palantir. Je vous ai tout de même fourni quelques pistes qui montrent que nous sommes conscients des limites de l'usage du numérique et des risques, que nous avons intégré des garde-fous en interne, dans le *design*. Depuis douze ans, nous avons une équipe, *Privacy and Civil Liberties*, sur les libertés civiles et privées. Elle est constituée d'ingénieurs, de philosophes, de juristes qui guident les ingénieurs dans le développement des plateformes pour que celles-ci soient robustes à des usages malveillants.

Je vous rappelle également que les données de santé, notamment les données personnelles, n'arrivent pas à la connaissance de Palantir. L'inverse serait inadmissible. Vous pouvez vérifier auprès de vos collègues britanniques qui ont dû regarder le contrat britannique. Nous n'en avons ni l'intérêt ni l'usage. La force d'une société comme Palantir est que l'on peut lui faire confiance. Dès lors qu'il y aurait, non pas des suspicions, mais une réalité de fuite de données, cela tuerait purement et simplement notre modèle de *business*.

M. Olivier Tesquet. On ne peut se satisfaire de la présence du comité d'éthique. Je précise tout de même que les chercheurs sont rémunérés pour y siéger. Je tiens cette information de l'une des personnes que j'avais interviewées lors de mon enquête sur Palantir, en 2017, à une époque où l'entreprise était encore un peu « sous le radar ».

S'agissant des données de santé, je n'ai pas parlé de « siphonnage ». Je n'ai pas eu besoin de cette audition pour savoir qu'effectivement, vous n'aviez pas accès aux données en

tant que telles. En revanche, des questions se posent. Le partenariat signé avec le *National Health Service (NHS)* au Royaume-Uni fait l'objet d'une plainte d'ONG, qui veulent connaître les conditions d'attribution de ce marché. La question de la transparence et de l'opacité est quand même un point qui mérite d'être soulevé.

M. Fabrice Brégier. C'est vrai, mais elle appartient au client et non à ses sous-traitants.

M. Olivier Laurelli. Je reviens sur ma deuxième question : pouvez-vous nous promettre que d'ici un an, deux ans ou trois ans, on ne retrouvera pas vos outils au Moyen-Orient ?

M. Fabrice Brégier. Ce point n'est pas dans ma zone de responsabilité. Je pense qu'il y a eu quelques contrats avec des pays de la catégorie qui a été rappelée, les États-Unis et ses alliés, mais pas avec tous ces pays, certainement pas.

Je vous remercie d'avoir supporté mon élan parfois fougueux, car j'estime avoir eu une carrière industrielle au service de la France et de l'Europe et ne pas renier cette volonté d'aller de l'avant, d'aider à développer l'activité économique en France et d'aider mon pays à mener ses actions de souveraineté. Voilà ce qui m'anime. Depuis que j'ai rejoint Palantir, je n'ai aucun doute, aucune suspicion sur le fait que je suis soutenu dans cette démarche.

Audition, ouverte à la presse, de M. Éric Baissus, président-directeur général de Kalray
(30 mars 2021)

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. Nous auditionnons M. Éric Baissus**,** président-directeur général de Kalray, entreprise française et européenne spécialisée dans la production de microprocesseurs. Elle est un spin-off créé en 2008 au sein du Commissariat à l'énergie Atomique et aux énergies renouvelables (CEA). Nous avons souhaité répondre favorablement à votre demande d'audition au regard de l'origine de votre entreprise qui démontre la capacité de la France à soutenir la création technologique et son positionnement stratégique sur un certain nombre de marchés critiques en développement. Nous sommes très intéressés par votre vision de ce que pourrait être une forme de souveraineté numérique et technologique française et européenne à court ou moyen terme.

M. Philippe Latombe, rapporteur. En guise d'introduction, je souhaiterais évoquer avec vous trois sujets. Nous aimerions d'abord savoir comment vous définissez la notion de souveraineté numérique française et européenne. Ce concept revêt une forte dimension technologique, qui est aussi au cœur de votre activité puisque vous produisez des microprocesseurs intelligents.

Nous aimerions donc mieux connaître votre secteur d'activité. Quel est votre niveau de dépendance vis-à-vis des pays non-européens, en termes de composants par exemple, et comment les acteurs français et européens se positionnent sur votre marché par rapport à leurs concurrents internationaux. Nous sommes conscients que la maîtrise de la puissance de calcul est un enjeu décisif dans un nombre important de domaines comme l'industrie 4.0 ou le quantique.

Je souhaiterais également que vous puissiez nous présenter votre entreprise, en insistant sur son parcours original, qui dit quelque chose de notre système de recherche et développement technologique français. Le CEA y a joué un rôle important. Nous aimerions savoir comment vous jugez, en France, le niveau de soutien des pouvoirs publics à la création et au développement d'entreprises technologiques. Nous aimerions également vous entendre sur les difficultés que vous avez pu rencontrer, par exemple pour vous financer, lors de certaines phases de votre croissance. Vous êtes en effet bien placé pour partager avec nous l'existence d'éventuels obstacles à lever sur ce point.

Enfin, je souhaiterais aborder la question de la formation aux compétences numériques, notamment dans votre secteur d'activité. Comment jugez-vous le niveau des formations existantes ? Identifiez-vous des manques ? Avez-vous des difficultés à recruter des ingénieurs français pour réaliser, par exemple, les tâches les plus techniques ? Je soulève ces différents points qui renvoient aussi à la nécessaire féminisation des métiers du numérique, le sujet étant régulièrement revenu lors de nos précédentes auditions.

M. Éric Baissus, président-directeur général de Kalray. Je tiens à vous remercier de me donner cette opportunité de partager notre expérience. Je vous propose, après avoir présenté notre société, de partager deux éléments importants. Il s'agit d'un nouveau marché au cœur de la problématique de la souveraineté numérique et de l'accès à des composants permettant d'avoir de très grandes puissances de calcul. Cette industrie est au cœur de nos industries de demain, au cœur de pans de l'industrie européenne très importants. Ce marché

est extrêmement stratégique et fait l'objet d'enjeux géopolitiques monstrueux, en particulier entre les États-Unis et la Chine.

Nous sommes une spin-off, c'est-à-dire un essaimage du CEA. Nous sommes une *deep tech*, qui est issue d'un laboratoire, qui a une avance sur la concurrence, mais qui doit maintenant devenir leader mondial. Je vais partager notre parcours, pour pouvoir vous expliquer nos réussites et nos challenges de demain.

J'aimerais vous expliquer qui nous sommes et, personnellement, comment je me suis retrouvé à la tête de Kalray. Je suis ingénieur de formation. J'ai commencé ma carrière dans les années 90 chez Texas Instrument, une société américaine, dans un grand centre de développement basé dans le sud de la France. C'est dans ce contexte que j'ai appris à développer des processeurs. J'ai passé dix ans à apprendre ce métier.

Ensuite, j'ai créé ma propre société. Là, j'ai commencé à apprendre un nouveau métier, qui est le monde de l'entrepreneuriat. J'ai cédé cette société à Alcatel Lucent. Suite à ce rachat, j'ai passé quelques années dans la Silicon Valley. Quand je suis revenu en France, en 2014, j'ai eu l'opportunité de rencontrer Kalray. Kalray a été créée en 2008 par des personnes qui venaient du CEA et de STMicroelectronics. Kalray était en redressement judiciaire. Des actionnaires qui me connaissaient m'ont demandé de transformer cette société en une société qui puisse avoir son mot à dire sur le marché. C'est ce à quoi nous nous attelons avec toute l'équipe, depuis six ans.

Aujourd'hui, Kalray a un positionnement très intéressant sur un marché qui a de l'avenir. Nous avons maintenant une technologie mature, le temps est venu d'appuyer sur l'accélérateur pour la déployer commercialement, tout en continuant à investir en R&D.

Nous sommes une société qui développe un nouveau type de processeur, qui a vocation à « adresser » le marché des systèmes intelligents ou de l'intelligence artificielle embarquée. Pourquoi ce marché est-il aussi important ?

Je vais prendre l'exemple de la voiture autonome. Une voiture autonome est une voiture bardée de capteurs qui filment la route et qui envoient un flot d'informations. Il faut extraire de ce flot de données des informations pertinentes (un panneau de signalisation, un feu rouge, un piéton qui traverse…). Pour faire cela, nous avons besoin d'un nouveau type de processeurs, les processeurs intelligents, qui analysent en temps réel ce flot d'informations, souvent en utilisant des algorithmes d'Intelligence artificielle, pour pouvoir diriger la voiture.

Il s'agit d'un nouveau marché, qui correspond à un besoin de nos sociétés modernes, qui génèrent de plus en plus de données. Certains rapports montrent que ce flot de données a été multiplié par dix en deux ans. Dans beaucoup de cas, ce flot de données n'a de valeur que si on l'analyse tout de suite. L'exemple de la voiture est pertinent.

Cette problématique est valable pour un très grand nombre d'industries, qui sont importantes pour la France et pour l'Europe : le marché automobile, le marché des *data centers*, le marché des télécoms, de la 5 G, le marché de l'aérospatial. L'un de nos actionnaires est Safran, avec qui nous travaillons à implanter nos processeurs dans les moteurs d'avion de demain pour analyser à la volée ce qui se passe dans le moteur et améliorer de 30 % à 50 % la consommation du moteur.

Un autre pan de l'industrie est aussi très intéressant : l'industrie 4.0. Il y a une volonté de rapatrier dans notre pays des usines, mais cela nécessite des usines qui sont beaucoup plus

automatisées. Pour cela, il est nécessaire d'avoir des technologies qui vont analyser à la volée les chaînes de production pour prendre des décisions.

Enfin, un marché est évident : le marché de la défense. La défense a besoin de technologies comme celle-ci pour pouvoir fournir les solutions les plus performantes possible.

Aujourd'hui, Kalray est une société qui emploie à peu près une centaine de personnes. Nous sommes basés à Grenoble. Nous avons développé un type de processeur breveté qui amène des capacités de calcul et qui permet d'être au cœur de ces nouvelles technologies. Nous sommes le seul acteur aussi avancé en France et en Europe et nous nous confrontons à de gros mastodontes, qui sont essentiellement américains, israéliens et, de plus en plus, chinois.

Comment le « Petit Poucet » Kalray peut-il avoir la moindre chance par rapport à ces mastodontes ? Si vous regardez l'histoire du monde des processeurs, vous constatez qu'à chaque vague, à chaque nouveau besoin, émergent de nouveaux acteurs. La première vague est celle des processeurs pour les ordinateurs et les serveurs. Intel, le mastodonte américain, détient aujourd'hui 95 % du marché mondial.

La deuxième vague a été la vague des processeurs pour téléphones portables. L'Europe était très en avance dans les années 90 et la plupart des centres de développement des puces pour téléphone portable étaient en Europe. Il se trouve que, petit à petit, l'Europe a abandonné ce marché parce qu'il était très orienté consommateurs, *end-users*, *BtoC*. Petit à petit, les fleurons européens ont arrêté d'investir dans ce marché, estimant qu'ils ne pouvaient pas y conserver un rôle de leaders. Les leaders de ce marché des téléphones portables sont de nouveaux acteurs. Ils étaient de nouveaux acteurs dans les années 90 et sont devenus aujourd'hui des poids lourds : Qualcomm, Samsung, Apple.

Dans ce nouveau marché de l'Intelligence artificielle embarquée, du *edge computing*, les cartes sont rebattues, ce qui constitue une opportunité pour un acteur comme Kalray et, plus largement, pour la France et pour l'Europe de prendre le leadership. Pourquoi ? Parce que ce marché nécessite des technologies que l'Europe a aujourd'hui, qui sont proches de l'embarqué et qui sont poussées par des donneurs d'ordres français et européen.

Kalray est une *deep tech*, comme je vous l'ai dit. En dix ans, nous avons investi 100 millions d'euros pour créer notre produit. Nous sommes encore au balbutiement commercial puisque notre chiffre d'affaires est autour d'un million d'euros. Pourquoi seulement un million d'euros ? Parce que nous vendons nos microprocesseurs à des acteurs qui sont en train de les tester et de développer leurs propres produits. Pour cela, ils n'ont pas besoin d'acheter des milliers de puces. En revanche, une fois que ces clients se déploieront sur le marché, ils développeront leurs produits avec nos processeurs, ce qui générera de plus en plus de chiffre d'affaires. Aujourd'hui, nous avons essentiellement deux marchés : le marché des *data centers* et le marché de l'embarqué (aérospatiale, automobile). Nous avons également comme actionnaire l'alliance Renault-Nissan-Mitsubishi.

Kalray est au cœur de cette problématique de souveraineté, et ce, pour plusieurs raisons. La souveraineté numérique est essentiellement la souveraineté technologique. Être souverain, cela veut dire être libre d'accéder à cette technologie. Nous nous en apercevons tous les jours quand nous parlons à nos clients. L'accès libre à ces technologies est crucial pour déployer leurs produits. Les acteurs de la défense sont soucieux d'avoir la liberté d'accès à ces technologies.

Deuxièmement, la souveraineté numérique, c'est avoir l'accès à la compétence. On parle de technologies qui sont complexes. Il est important, pour avoir cette souveraineté numérique, de comprendre ces technologies, de les maîtriser, d'avoir de l'expertise locale.

Enfin, la souveraineté numérique, c'est contrôler ce que font ces technologies. Si l'on ne sait pas ce qui se passe dedans, cela pose un vrai problème de souveraineté.

Chez Kalray, nous sommes au cœur de ces problématiques, puisque nous sommes l'un des rares acteurs aujourd'hui à fournir ces puces de calcul intensif. Si Safran, Renault, le fonds Definvest, créé par la direction générale de l'armement (DGA), investissent dans Kalray, c'est pour s'assurer que ces technologies seront accessibles dans les cinq, dix, quinze ans qui viennent.

Dans notre approche, nous poussons un modèle ouvert (open source, open hardware), afin de créer un écosystème autour de nous et de permettre à nos clients d'avoir une garantie d'accès à ces technologies, quel que soit notre futur.

Enfin, nous avons un rôle en vue de préserver la compétence. Nous sommes l'un des rares acteurs à développer des puces de calcul intensif. Nous formons notre personnel. Nous avons créé une compétence que nous essayons d'élargir petit à petit, pour l'utiliser pour nos propres besoins et afin qu'elle soit disponible plus largement.

Sur le marché de l'intelligence embarquée, l'acteur le plus important est Nvidia, une société américaine. Quand vous utilisez une technologie de Nvidia, vous utilisez un langage propriétaire, qui a été développé par Nvidia : CUDA. Par conséquent, tous les acteurs qui utilisent les technologies de Nvidia développent un historique en utilisant un langage propriétaire. Si demain, ils passent à un autre fournisseur que Nvidia, ils devront tout redévelopper. Nvidia a une stratégie de « locker », en imposant aux différents acteurs de l'industrie d'utiliser un langage propriétaire. Je pense que, dans ce contexte de souveraineté numérique, il est très important d'aider nos industriels à disposer d'un accès ouvert à ces technologies, en particulier en sponsorisant des technologies ouvertes.

Kalray est une société *fabless*, qui n'a pas d'usine. Aujourd'hui, aucune usine en Europe n'est capable de fabriquer nos processeurs. Seuls Intel, TSMC *(Taiwan Semiconductor Manufacturing Compagny)* et Samsung en sont capables. Nous travaillons avec TSMC. Nous dépendons d'usines de fabrication qui ne sont pas sur le sol européen.

Il est très difficile de financer une société de semi-conducteurs comme Kalray. Jusqu'à il y a un ou deux ans, il était quasiment impossible de financer une telle société en Europe, car ce type de société était considéré comme trop risqué. Heureusement, il existe une vraie prise de conscience de l'importance de cette industrie. Dans notre cas, nous avons levé autour de 100 millions d'euros. Nous investissons 15 millions d'euros par an. Nous avons encore un chiffre d'affaires relativement faible. Ce ne sont pas des sociétés faciles pour des investisseurs parce qu'elles demandent un investissement à long terme, avec des risques associés.

Je tiens à signaler l'effort qui est fait par la Bpifrance pour que les *deep techs* françaises puissent devenir les champions de demain.

Sur la formation et sur la compétence, aujourd'hui, nous sommes à la croisée des chemins. Il existe encore de la compétence en France dans les semi-conducteurs parce qu'il y en avait il y a une vingtaine d'années. En revanche, je pense que, si l'on n'investit pas massivement aujourd'hui dans ce secteur, petit à petit, cette expertise va partir. Il est donc très

important d'investir, de faire que l'on ait des acteurs qui soient des leaders pour créer aussi des offres d'emplois et enclencher un cercle vertueux offre-demande.

M. Philippe Latombe, rapporteur. Vous avez beaucoup parlé des Américains, de Nvidia notamment, et de leur mode de fonctionnement avec un langage propriétaire qui permet de « locker » les industriels qui utilisent leurs technologies. Qu'en est-il des Chinois aujourd'hui ? Leur vendez-vous des puces ? On a beaucoup dit que la Chine copiait, puis développait. Où en sont-ils dans la R&D pour ces technologies ? Le marché automobile ne sera pas le seul à être intéressé par ces puissances de calcul, notamment en Intelligence artificielle embarquée. L'industrie de l'armement en a besoin, avec les drones, les avions, etc. L'industrie de défense chinoise est en train de se développer à grande vitesse.

Deuxième question, puisque nous parlons de puissance militaire, où en sont les Russes ? Ont-ils des compétences dans ce domaine ?

Quel est le risque pour vous d'être copié ?

M. Éric Baissus. Nous connaissons très bien le marché chinois, mais beaucoup moins le marché russe. Cela veut-il dire que les Russes sont moins actifs ? En tout cas, nous ne travaillons pas avec eux.

Aujourd'hui, les militaires ont compris qu'ils ont besoin de s'appuyer sur des acteurs civils pour récupérer ces technologies, compte tenu des investissements nécessaires. C'est la raison pour laquelle la DGA investit dans Kalray.

Dans cette stratégie, la Chine investit massivement pour créer ses leaders nationaux dans le monde du semi-conducteur. En gros, elle investit cinquante à cent fois plus que ce que nous faisons en Europe. Elle investit dans tous les domaines : la fabrication des puces, le design, etc. Les Chinois ont une stratégie de création de leaders nationaux en réservant le marché national à leurs leaders.

On se trompe quand on croit que nous sommes en avance. La Chine a quasiment rattrapé son retard. Bien sûr, il faut faire attention à ne pas être copié, mais la problématique n'est plus là : il faut faire en sorte que, dans cinq à dix ans, il y ait des champions européens. Pour cela, il faut que l'on ait des champions civils parce que seuls les marchés civils permettront de financer les investissements associés.

M. Philippe Latombe, rapporteur. Aujourd'hui, les Américains fonctionnent avec des licences pour la plupart. Les Chinois, eux, n'ont pas de licence. Sont-ils capables d'inonder le marché de leurs produits, ce qui rendrait la solution intermédiaire (la vôtre) difficilement commercialisable ?

M. Éric Baissus. La Chine, quand elle dépend de licences étrangères, développe sa propre technologie. La chance de la Chine réside dans la taille de son marché. Elle accepte que ses leaders nationaux ne soient pas aussi avancés que ce qui existe à l'étranger, en misant sur le fait que, petit à petit, ils rattraperont leur retard.

M. Philippe Latombe, rapporteur. Où les puces sont-elles fabriquées ? Faut-il recréer une industrie de la fonderie en Europe ou s'appuyer sur des pays tiers ? Existe-t-il un risque de voir les secrets industriels copiés en les confiant à des fondeurs non-européens ?

M. Éric Baissus. Aujourd'hui, nous utilisons des usines basées à Taiwan, chez TSMC, le plus gros fabricant au monde. Nous envoyons aux usines un fichier qui représente la position

des transistors dans la puce. La puce compte 9 milliards de transistors. Les risques d'être copiés par ce biais sont donc très faibles.

Il existe quelques usines en France et en Europe, mais pour des process de gravure qui sont très larges. Ces usines peuvent fabriquer des petits composants, des composants de puissance, mais ne sont pas capables de fabriquer des processeurs comme les nôtres, avec de fortes capacités de calcul. Aujourd'hui, nous sommes obligés d'utiliser des usines basées à Taiwan. L'autre acteur qui croît énormément est aujourd'hui Samsung en Corée. Il n'existe pas d'acteur en Europe.

Quelles sont nos recommandations ? Pourquoi les acteurs aujourd'hui sont-ils Intel et TSMC ? C'est essentiellement parce qu'ils ont un marché. Comme leurs usines tournent, ils ont les moyens de les financer. TSMC va investir une dizaine de milliards cette année.

Ma recommandation est de travailler sur ces deux sujets : rapatrier des usines en Europe et faire en sorte qu'un écosystème utilise ces usines.

Si je prends l'exemple des vaccins, qui est d'actualité, il faut avoir des usines qui sont capables de les produire et des sociétés qui sont capables de les développer.

Chez Kalray, nous sommes ceux qui vont développer les puces et utiliser les usines. Il faut supporter cet écosystème si l'on veut avoir un vrai rapatriement, une vraie souveraineté.

Concernant les usines, deux approches sont possibles :

– soit faire un leader européen, ce qui nécessiterait un très fort investissement ;

– soit inciter des fabricants actuels (Intel, TSMC, Samsung) à mettre en place des chaînes de production en Europe. Cela nous permettrait de valoriser leur expertise, de créer un pôle de compétences, de garantir des acteurs à la pointe du progrès.

M. Philippe Latombe, rapporteur. Vous dites aujourd'hui que Kalray est une partie d'une solution technologique future. Comment cet écosystème travaillerait-il ensemble ? Est-ce que vous construisez la puce dans votre coin et l'industriel s'en sert et s'adapte autour de votre puce ? Ou est-ce vous qui avez la connaissance de ce que les capteurs récupèrent comme informations, nécessitent comme calculs pour pouvoir ensuite l'envoyer vers le « cerveau » de la voiture qui prend la décision ? Le législateur ou l'État a-t-il un rôle de structuration à jouer ?

M. Éric Baissus. Quand on développe un processeur, il faut qu'il soit un minimum générique, pour pouvoir être programmé. Cependant, ce composant matériel doit être adapté à un marché. Nous travaillons dans notre coin à rendre notre processeur générique et nous travaillons aussi avec les donneurs d'ordres (Safran, Renault…), pour être sûrs que notre offre est pertinente.

Il est important de travailler main dans la main avec le donneur d'ordres. Je pense que les projets collaboratifs sont très importants pour que tout l'écosystème travaille ensemble.

M. Philippe Latombe, rapporteur. Y a-t-il des standards dans votre métier ? Participez-vous à leur élaboration ? Vous travaillez avec Renault, mais Mercedes, Audi, Jeep auront-ils les mêmes standards ?

M. Éric Baissus. Nos produits sont assez génériques pour être utilisés par plusieurs acteurs du marché. Ensuite, chaque client les programme différemment. D'ailleurs, la plupart des clients veulent profiter de l'effet de volume pour avoir de meilleurs prix.

Ensuite, il est important d'avoir des standards pour permettre à nos clients de ne pas dépendre uniquement de nous. Nous poussons notre technologie pour en faire un standard ouvert. Si nous voulons devenir un leader demain, il faut que notre technologie soit déployée le plus massivement possible et donc en faire un standard.

M. Philippe Latombe, rapporteur. Je souhaiterais aborder la partie financement. Vous avez dit que la Bpifrance vous a soutenus. Je voudrais revenir aux difficultés que Kalray a connues dans sa vie d'entreprise. Comment ces difficultés sont-elles perçues par l'écosystème, par les acteurs publics et privés ? Aux États-Unis, on dit qu'il faut dix échecs pour une réussite. Est-ce valable aussi en France et en Europe ?

M. Éric Baissus. C'est le jour et la nuit entre être un investisseur aujourd'hui et il y a vingt ans. Les progrès sont énormes ! Aujourd'hui, on est plus tourné vers l'innovation, l'écosystème est bienveillant pour permettre à des start-up de se développer. En termes de culture, le changement est réel. Il y a vingt ans, le monde des laboratoires et le monde de l'entrepreneuriat se haïssaient. Aujourd'hui, non. Le CEA invite les entrepreneurs à venir voir les technologies qui sont développées pour lui et qui pourraient servir à créer une société. Il faut continuer à supporter cette démarche, car on voit que l'innovation est issue du monde des start-up, puis doit être transformée en leader mondial.

En termes de financement, il est inutile de vous cacher que la vie de Kalray a été très difficile. Pendant quatre à cinq ans, je disais à mes collaborateurs que je n'étais pas certain de pouvoir payer leurs salaires le mois suivant. Nous avons levé 100 millions d'euros, ce qui est énorme par rapport à notre parcours. La plupart de nos concurrents ont levé 400 à 500 millions d'euros. Nous avons eu la chance de faire une très belle introduction en bourse, puisque nous avons levé 50 millions d'euros. Pourquoi est-il si difficile d'avoir des financements privés ou publics dans le marché des semi-conducteurs ? Parce que l'Europe considérait qu'elle n'avait aucune chance de réussir sur ce marché et l'avait abandonné. Aujourd'hui, il existe une prise de conscience et il existe des aides et des supports en France et en Europe. Je pense que ces soutiens sont nécessaires pour créer dans notre industrie des champions nationaux et européens.

M. Philippe Latombe, rapporteur. Aujourd'hui, pensez-vous que l'intégralité des partenaires financiers arrivent à s'aligner correctement ? Si Bpifrance apporte son soutien, les partenaires financiers suivent-ils ?

M. Éric Baissus. Je pense que Bpifrance effectue un travail remarquable. Ensuite, l'investisseur privé est naturellement moins intéressé par les investissements stratégiques, car il veut avant tout un retour sur investissement, avec le moins de risques. Comment peut-on abonder ou favoriser l'investissement privé ? Je pense qu'il ne faut pas que l'investissement soit uniquement public, parce que le public seul a du mal à repérer les bons entrepreneurs, les sociétés qui ont la capacité de devenir des champions. En tout cas, le lien entre investissement privé et investissement public est très important. De grands progrès ont été réalisés. Il existe certainement des mécanismes d'abondement pour favoriser les investissements privés dans des sociétés de la *deep tech* qui sont des sociétés plus difficiles à financer, avec des retours sur investissement plus longs.

M. Philippe Latombe, rapporteur. Vous êtes un spin-off. Est-ce le bon modèle ? Est-ce comme cela que l'on va créer les entreprises de demain ? Comment faire pour arriver à en créer plus, selon vous ?

M. Éric Baissus. Les spin-off sont un réservoir formidable de technologies. Il s'agit pour moi d'un mode de déploiement assez intéressant. Notre pays investit, l'Europe investit énormément dans les laboratoires. Pour valoriser toutes ces technologies, il faut les commercialiser et faire des champions nationaux et européens. Je pense donc que le modèle de spin-off est très intéressant. Il a beaucoup évolué, mais il doit encore être amélioré.

Aujourd'hui, en France, on croit encore que vous pouvez créer une société, quand vous avez une technologie. J'ai tendance à dire que, quand vous avez une technologie, vous n'avez fait que 20 % du travail, vous devez encore déployer un effort considérable pour transformer une technologie en une société commerciale pérenne, leader de son marché. L'effort à fournir est largement sous-estimé. D'ailleurs, beaucoup de financements aujourd'hui sont plus liés à de la technologie (même si les mentalités sont en train d'évoluer) qu'au positionnement produit, à la mise au point d'une offre mature, à l'accès au marché.

Vous mentionnez le rôle de l'État. J'ai senti dans les plans de relance un changement culturel : on insiste de plus en plus sur les débouchés, le travail avec les donneurs d'ordres et moins sur la rupture technologique. Jusqu'à présent, on demandait de montrer en quoi une technologie est différente. C'est bien d'avoir une technologie différente, mais la différence en soi n'a pas de valeur. Il faut avoir une différenciation sur le marché.

C'est pour moi très important. Spin-off, oui, mais avec un environnement qui va favoriser la transformation d'une technologie en un vrai acteur commercialement viable.

M. Philippe Latombe, rapporteur. Pour vous, ce n'est pas suffisamment fait. Est-ce lié à la formation ? Comment mixer les deux mondes, financier et technologique ?

M. Éric Baissus. Une société comme Kalray est la conjonction d'une compréhension technique et d'une compréhension *business*.

Nous avons un retard culturel, car la France a toujours valorisé les compétences technologiques par rapport aux compétences marketing. Cela dit, cette culture est en train de changer. Les écoles d'ingénieurs proposent de plus en plus de formations à la création de start-up et, inversement, les écoles de commerce sont de plus en plus orientées vers la *high tech*. Je pense qu'un rapprochement de ces deux mondes est crucial. Il est important que ces deux mondes se parlent et travaillent ensemble.

M Philippe Latombe, rapporteur. L'Europe prend-elle le bon chemin aujourd'hui ? Sentez-vous que l'Europe a décidé de prendre son destin numérique en main ? Commence-t-on à reparler de l'Europe comme étant un futur grand compétiteur, dans votre domaine et au-delà, dans le monde numérique ?

M. Éric Baissus. Aujourd'hui, il existe une prise de conscience, mais elle est récente, elle date d'il y a un an. La crise du Covid a accéléré cette prise de conscience, au niveau de la France et de l'Europe. Comment est-ce perçu par l'international ? Comme des mots. Tant qu'un champion national ne remporte pas de marché, ce ne sont que des mots.

Comment transformer ces mots en actions ? Je suis confiant. En tout cas, je suis très positif. Il faut encore travailler pour transformer ces mots et cette énergie en action. Nous,

Kalray, proposons notre collaboration pour constituer un champion national, voire mondial. Aujourd'hui, nous en sommes loin.

M. Philippe Latombe, rapporteur. Y a-t-il des points que nous n'avons pas encore évoqués et qui vous semblent importants ?

M. Éric Baissus. Si je dois résumer les points importants, il y a un nouveau marché, qui sera extrêmement stratégique dans un contexte de souveraineté numérique. Ce nouveau marché est au cœur de nos industries traditionnelles. Sur ce marché *B to B*, l'Europe a ses chances. Je pense que nous n'avons pas le choix. Si nous voulons notre souveraineté numérique, nous avons besoin d'être sur ce marché de l'Intelligence artificielle embarquée et du *edge computing*. Nous le pouvons. Il faudra transformer les mots en actions. De nombreuses actions sont en cours. Je suis donc très positif et confiant. Nous sommes très excités de voir comment nous pouvons faire de l'Europe un leader sur ce marché.

Audition, ouverte à la presse, de M. David Ofer, président de la Fédération française de la Cybersécurité
(30 mars 2021)

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. Nous recevons M. David Ofer, président de la Fédération française de la Cybersécurité, association ayant vocation à rassembler les professionnels de la cybersécurité, avec l'objectif de contribuer à la structuration de cette filière. Organisés en plusieurs collèges thématiques, vous assurez la promotion de la formation aux compétences cyber et innovation. Nous souhaiterions aborder avec vous les questions tenant à la certification et à la labellisation des solutions de cybersécurité.

M. Philippe Latombe, rapporteur. Comment appréhendez-vous la notion de souveraineté numérique ? De quelle façon les politiques menées peuvent ou doivent-elles évoluer pour mieux l'intégrer le cas échéant ?

Ensuite, je souhaiterais que nous puissions échanger à propos de l'écosystème des entreprises françaises de la cybersécurité. Comment ces entreprises se portent-elles dans le contexte actuel de crise sanitaire durable ? Quels sont leurs besoins et leurs attentes vis-à-vis des pouvoirs publics ? Quelles sont leurs propositions pour participer à la construction d'une forme de souveraineté numérique ? Comment faire en sorte que l'écosystème cyber français continue de se développer et de se renforcer ? Ce thème nous permettra d'aborder les annonces récentes du Président de la République et l'actualité européenne marquée par la révision de la directive *NIS (Directive on security of network and information systems)* et par la présentation d'une stratégie cyber par la Commission européenne, à la fin de l'année dernière.

Enfin, s'agissant de la diffusion d'une culture cyber au sein de la société, quel regard portez-vous sur le niveau de sensibilisation des entreprises, des administrations publiques, des collectivités territoriales et des citoyens ? Je souhaiterais aussi que nous évoquions la formation aux compétences cyber alors qu'un campus cyber est en cours de développement, avec l'appui, notamment, de l'agence nationale de la sécurité des systèmes d'information (ANSSI). Comment la France se positionne-t-elle par rapport aux autres pays ? Existe-t-il des segments sur lesquels nous devrions compléter notre offre de formation pour combler d'éventuelles lacunes.

M. David Ofer, président de la Fédération française de la Cybersécurité. La Fédération française de la Cybersécurité a pour objet de rassembler toutes les organisations, les associations professionnelles, les entreprises, les personnes et, plus largement, tous les acteurs directs ou indirects liés à la cybersécurité.

Comme vous le savez, il existe un grand nombre d'associations et d'initiatives qui parlent aujourd'hui de manière dispersée. Au regard de l'actualité et de l'évolution sociétale, il est important de coordonner les actions sur la cybersécurité, en consolidant une filière qui est marquée et représentée, beaucoup trop souvent, par la dimension technique du sujet. Notre ambition est bien de coordonner l'ensemble de ces actions.

La cybersécurité est un élément incontournable de la vie du citoyen et des entreprises. Elle doit d'inscrire dans la lignée de la responsabilité sociétale et environnementale des entreprises, car l'impact d'une cyberattaque pénalise gravement le tissu économique et la

souveraineté. La notion de souveraineté est liée à l'indépendance, celle de nos citoyens, de nos entreprises et plus largement de notre pays.

Ce qui devient aujourd'hui un véritable défi sur les sujets de cybersécurité ne peut se réaliser pleinement qu'en fédérant les acteurs existants, qui peuvent apporter, chacun dans son périmètre, des savoir-faire qui feront avancer cette souveraineté et la replaceront à l'ordre du jour. Si nous souhaitons aller dans cette direction, tous ensemble, il faut adapter notre vision et créer un cercle vertueux, où l'État jouera son rôle pour insuffler une politique, les agences techniques apporteront des garanties, les grands groupes pourront utiliser les moyens financiers et les PME créer de la valeur et une proximité avec le terrain. L'objectif doit être la protection du citoyen et du tissu économique et, par incidence, la protection des institutions.

La Fédération française de la Cybersécurité souhaite consolider cette filière en portant des messages représentatifs sur les problématiques rencontrées, mais aussi mener des actions de terrain pour remplir les objectifs que j'évoquais précédemment.

Parmi les actions que nous avons lancées pour le maillage territorial que nous souhaitons promouvoir, je citerai notre plan de création de 20 000 emplois sur la base d'un nouveau métier dédié aux jeunes non diplômés ou à des personnes souhaitant se reconvertir professionnellement. Ce nouveau métier d'assistant cyber a pour vocation de créer une proximité de terrain avec les utilisateurs du numérique, en informant et en complétant notamment le rôle des ingénieurs et des spécialistes techniques qui ont déjà fort à faire. Les premières formations vont débuter cet été.

Autre action concrète, la mise en place d'un soutien direct aux PME par la réalisation d'un diagnostic de cybersécurité gratuit qui permettra leur prise de conscience et les aidera, lorsqu'elles auront subi une cyberattaque, en les dispensant de payer la franchise d'assurance qu'elles auraient souscrite. Nous estimons le coût de cette opération de diagnostic à 20 millions d'euros environ, montant que nous espérons collecter auprès de l'État et des collectivités territoriales.

La Fédération française de la Cybersécurité mène des actions concrètes, de proximité, pour encourager au maximum la protection du tissu économique et la souveraineté française avec un esprit altruiste et citoyen.

Je peux poursuivre si vous le souhaitez avec un état des lieux et quelques chiffres qui permettraient d'avoir un peu de visibilité sur ce qui se passe aujourd'hui en France et à l'étranger.

M. Philippe Latombe, rapporteur. Très bien.

M. David Ofer. Les chiffres sur la menace cyber sont sous-estimés, et ce pour plusieurs raisons. D'abord, les chiffres sont basés sur les déclarations des attaques, sur les plaintes des victimes et sur les interventions de l'ANSSI et des forces de l'ordre. Or toutes les attaques ne sont pas déclarées. Un grand nombre de statistiques proviennent d'entités non indépendantes de type cabinets de conseils ou éditeurs.

L'ANSSI a réalisé 192 interventions en 2020, soit une augmentation de 200 % par rapport à 2019. Cybermalveillance de son côté a recensé 837 entreprises et 159 collectivités attaquées. Par ailleurs, les compilations de chiffres que nous avons de notre côté montrent que neuf organisations sur dix sont victimes de cyberattaques. Il faut noter qu'une cyberattaque n'est pas forcément une paralysie du système d'information. Selon une étude d'un spécialiste de la cybersécurité, 91 % des organisations françaises ont été la cible de cyberattaques cette

année et 60 % ont subi plusieurs actes malveillants. 75 % et plus des attaques sont faites par des *ransomwares* (rançongiciels) en France comme dans le reste du monde.

Dans le classement mondial du nombre de détections arrivent en premier les États-Unis, le Japon, puis l'Inde. L'Espagne est en 8ème position de ce classement mondial, l'Allemagne en 10ème, l'Italie en 11ème et la France en 16ème. Les pays européens les plus touchés par les rançongiciels sont l'Allemagne en tête, suivie de la France, de l'Italie et du Royaume-Uni.

Une unité du FBI aux États-Unis, l'*IC3* (*Internet Crime Complaint Center*) recense l'intégralité des plaintes liées au cybercrime. L'*IC3* a annoncé une moyenne de 791 790 plaintes pour 2020 et 4,2 milliards de dollars de pertes pour les États-Unis. Nous n'avons pas ce genre de chiffres en France, parce que nous ne les recensons pas de la même manière.

En nombre de plaintes déposées, le Royaume-Uni arrive en première position avec 216 000 plaintes, suivi par le Canada (5 300), l'Inde (2 930). La France est septième dans ce classement avec 1 640 plaintes déposées par des victimes en 2020. Il existe une différence colossale entre le nombre d'attaques non référencées et le nombre de plaintes déposées.

Enfin, selon un éditeur d'antivirus, la cybercriminalité coûterait environ 1 000 milliards de dollars à l'économie mondiale.

M. Philippe Latombe, rapporteur. En quoi la cybersécurité est-elle une composante essentielle de la souveraineté numérique ? A-t-on aujourd'hui les moyens de pouvoir être souverain dans ce domaine de la cybersécurité ?

M. David Ofer. Les chiffres d'affaires des entreprises françaises qui sont annoncés en cybersécurité incluent beaucoup d'assistance technique, le chiffrement, les matériels télécoms, l'identification des personnes. Les logiciels utilisés aujourd'hui sont américains pour la plupart, notamment les systèmes d'exploitation, la bureautique, les bases de données, le *cloud* et les usages grand public. Les éditeurs étrangers commercialisent auprès de nos entreprises des produits qui comportent des failles de cybersécurité. Ainsi, Microsoft corrige en moyenne 100 vulnérabilités par mois ces derniers temps.

Est-ce normal ? Accepterait-on de rouler avec une voiture dont les freins sont défaillants ? Je ne sais pas. Il nous manque en France des champions en cybersécurité dans les secteurs du futur, en associant notamment l'Intelligence artificielle.

Dans le domaine des produits de cybersécurité, nous avons un tissu économique qui est fort, mais nous sommes démunis ce qui concerne le socle technologique qui traite du numérique. Nous n'avons pas de système d'exploitation français. Nous n'avons ni système de bureautique ni système de base de données français. Le *cloud* est un grand débat. Aujourd'hui, nous utilisons pour cette visioconférence un logiciel américain alors qu'il existe d'excellents logiciels français de visioconférence.

La problématique de la souveraineté passe aussi par le soutien des entreprises françaises, par un certain nombre de mesures à mettre en place. Le plan cyber que le Président de la République a annoncé est, certes, une excellente avancée, mais il est insuffisant.

Pour donner des chiffres, Israël a levé l'an dernier 2,6 milliards de dollars pour la cybersécurité. Notre plan représente un milliard d'euros, dont un peu plus d'une moitié

financée par l'État et le reste par le privé. Au regard de notre population qui est dix fois plus importante que celle d'Israël, il nous aurait fallu *a minima* 26 milliards de dollars.

En Intelligence artificielle et en cybersécurité, nous sommes très loin derrière les investissements astronomiques chinois.

M. Philippe Latombe, rapporteur. Avez-vous des propositions à nous soumettre ?

M. David Ofer. Tout à fait. Il faudrait créer un *small business act*, c'est-à-dire inciter très fortement les mairies, les collectivités territoriales, les institutions publiques et parapubliques à acheter des logiciels et produits français en allant au-delà de la simple recommandation. Je peux vous donner des exemples très précis. L'aéroport de Nice choisit un produit américain pour sa cyberdéfense, Agirc-Arrco choisit des produits étrangers, la métropole de Nantes choisit des produits américains alors qu'en France, nous avons des produits de premier ordre qui sont aussi bons que les produits étrangers, notamment américains.

Souhaitons-nous une souveraineté, c'est-à-dire une indépendance ? Souhaitons-nous pousser notre industrie et favoriser notre tissu économique ou laisser la porte ouverte à des pays étrangers pour assurer notre cybersécurité ?

M. Philippe Latombe, rapporteur. Dans les exemples que vous avez cités, qu'est-ce qui a emporté le choix ? Le code des marchés publics ? Les acheteurs qui ne sont pas curieux et qui ont pris ce qu'ils avaient sur étagère ? Est-ce une forme d'entrisme des Américains ?

M. David Ofer. Le code des marchés publics oblige quasiment à mettre en place une grille tarifaire. Quand une société qui a des moyens colossaux accorde une remise de 90 % sur le prix de ses produits pour pénétrer un marché, une PME française n'a pas les moyens de s'aligner.

Il existe tout un écosystème américain. Les États-Unis ont mis en place depuis des années une politique visant à faire rayonner leur économie avec le *Small Business Act*. Il faut absolument créer un *small business act* à la française. Il faut absolument que l'on puisse, dès qu'une PME émerge dans la cybersécurité, lui proposer des marchés avec les services de l'État, des collectivités territoriales sans que cela soit un frein au développement.

M. Philippe Latombe, rapporteur. N'est-ce pas le rôle des intégrateurs d'être dans le conseil et dans le choix de solutions souveraines ?

M. David Ofer. Je ne rejoins pas tout à fait cette vision. Aujourd'hui, les grands groupes français intégrateurs de solutions de cybersécurité commercialisent des produits américains alors qu'il existe des équivalents français. Pour quelle raison ? Nous avons vécu la même situation avec les PC et la téléphonie mobile. On n'a pas aidé nos entreprises françaises parce que ces intégrateurs vont chercher la facilité et uniquement la valeur ajoutée sur le prix de vente. On n'a pas une vision de défense du tissu économique. On a des articles très intéressants sur le ruissellement économique. Quand vous achetez un logiciel français, vous créez de l'emploi en France, vous créez de la valeur ajoutée pour le tissu économique, vous créez de la proximité avec nos institutions, vous créez des capacités pour le tissu économique français à aller rayonner au-delà des frontières. Toute cette création de richesse, vous ne l'avez pas quand vous achetez un logiciel américain.

M. Philippe Latombe, rapporteur. L'État, les administrations publiques, les collectivités territoriales, les entreprises et les citoyens sont-ils suffisamment acculturés à la cybersécurité ?

M. David Ofer. Toutes les collectivités territoriales que je rencontre sont sensibilisées au risque cyber.

Il faut se poser la question de ce qu'est le risque cyber. Est-ce uniquement la paralysie par une attaque ou est-ce également la possibilité d'avoir accès à nos données ? Là se pose une question de politique : est-on prêt à laisser l'accès à nos données à tout le monde ? Ou veut-on avoir une politique souveraine sur la protection de nos données ?

Les collectivités territoriales sont parfaitement conscientes des enjeux de cybersécurité. Les directeurs des systèmes d'information (DSI) et les responsables de la sécurité informatique que je rencontre sont les premiers à essayer d'acheter des outils de cybersécurité. Ils font appel à l'ANSSI qui joue un rôle très important. Ils essayent de sensibiliser leurs utilisateurs, mais aujourd'hui, les collectivités territoriales n'ont pas toujours des moyens financiers et humains suffisants. Aujourd'hui, nous souffrons d'une pénurie forte d'ingénieurs : il manque trois à quatre millions d'ingénieurs en cybersécurité. On ne pourra pas former en France plusieurs centaines de milliers d'ingénieurs en deux ans. Il faut cinq, six, sept ans.

Cette problématique des moyens est un véritable sujet. Pour cette raison, la Fédération française de la Cybersécurité a prévu le nouveau métier d'assistant cyber, qui sera le relais entre la dimension technique de la cybersécurité et l'utilisateur, notamment dans les collectivités territoriales.

Je vais prendre un exemple simple. La plupart des agents dans les mairies ne savent pas changer leur mot de passe. Il faut un accompagnement pour ces personnels pour garantir la cybersécurité.

Oui, il y a une prise de conscience réelle dans les collectivités territoriales. Cela dit, les élus ne prennent pas toujours des décisions adéquates parce qu'ils manquent de connaissance en matière de cybersécurité. Ils ne voient que le risque de paralysie, et pas la problématique de l'exfiltration de données. La stratégie des *smart cities* peut être mise en péril à partir du moment où vous donnez un accès non autorisé à vos données à un tiers.

M. Philippe Latombe, rapporteur. Dans le plan de relance, le plan cyber est aussi dirigé vers les collectivités territoriales. Vous dites qu'elles manquent davantage de moyens humains que de moyens financiers.

M. David Ofer. Les deux. Vous avez de grandes collectivités territoriales qui ont des moyens, mais les petites mairies ont des ressources limitées. Dans une mairie que je ne citerai pas, ma rencontre avec les responsables de l'informatique a été fort intéressante. Par décision des élus, ils disposaient d'un budget de 5 000 euros pour la cybersécurité, contre 1,5 million d'euros pour la vidéosurveillance.

Au-delà de l'argent, il faut qu'il y ait cette volonté et cette prise de conscience que la cybersécurité est un enjeu de protection du citoyen. Nous l'avons vu avec la paralysie des hôpitaux.

M. Philippe Latombe, rapporteur. Ne faudrait-il pas parler davantage des cyberattaques et de leurs conséquences ? Quand les hôpitaux ont été attaqués, on s'est rendu

compte qu'ils n'avaient pas de plan de continuité d'activité. Suite à l'attaque de la ville d'Angers, une partie entière de l'activité est bloquée. Ils n'arrivent toujours pas à accéder aux données des horodateurs.

M. David Ofer. Communiquer sera toujours bénéfique, mais ne résoudra pas tout. La communication ne vous protégera pas des failles de sécurité que vous pouvez avoir dans les logiciels et dans les systèmes d'exploitation que vous achetez. Le seul moyen, c'est d'avoir une vision véritablement sociétale de la cybersécurité et peut-être d'avoir une approche à l'américaine, c'est-à-dire de quantifier très précisément le coût des cyberattaques. Aujourd'hui, des statistiques démontrent que plus de la moitié des entreprises qui ont vécu une cyberattaque sont absolument incapables de donner un chiffre précis du coût de celle-ci. 50 % des PME qui ont vécu une cyberattaque paralysante disparaissent dans les six mois qui suivent. Les grands groupes qui subissent des cyberattaques perdent, s'ils ne font rien, 20 % de leur valorisation, six à huit mois après. Ce sont des sommes colossales ! On ne pourra pas compenser ces problématiques uniquement avec de la communication, il faut des actions, il faut soutenir la filière de la cybersécurité, de manière à essayer de promouvoir ce tissu économique et de défendre nos institutions, nos entreprises et le citoyen.

M. Philippe Latombe, rapporteur. Il est communément admis que la France a un très haut niveau d'expertise en cybersécurité, que l'ANSSI est moteur dans la cybersécurité, que nous avons un écosystème de cybersécurité très à la pointe du progrès, qui suscite même des envies. Est-ce vrai ? Avons-nous des pépites qu'il faut absolument protéger ? À l'inverse, avons-nous des lacunes ?

M. David Ofer. Oui, nous avons un excellent écosystème français, parce que nous avons beaucoup d'entreprises qui développent de la technologie en cybersécurité avec des produits très innovants. L'ANSSI joue un rôle important pour les grandes entreprises.

Cela dit, quand on regarde la Suisse et la Grande-Bretagne, quand on regarde comment sont équipées les entreprises en termes de cybersécurité, les logiciels américains et israéliens dominent le marché.

L'écosystème français est bon et performant. Nous avons des logiciels et des ingénieurs de premier plan. Le vrai sujet est le suivant : comment promouvoir ces entreprises au-delà de nos frontières ? Je reviens à ma proposition de *small business act* à la française. Il faut aider nos entreprises à obtenir des marchés, il faut être capable d'investir massivement dans ces entreprises.

En 2016, un rapport américano-anglais présentait deux pépites françaises de la cybersécurité comme des licornes en devenir : Pradeo et ITrust. Ces deux entreprises ont levé respectivement un et deux millions d'euros, alors que deux entreprises américaines, Palantir et Tenable ont levé des centaines de millions et rayonnent sur le marché de la cybersécurité au niveau mondial.

Si l'on veut favoriser nos entreprises, il faut investir et aider les entreprises à accéder à des marchés, ce qui passe par la commande publique, par la génération de chiffre d'affaires et par un rôle d'accompagnement des autorités. L'ANSSI délivre des certifications qui sont utiles pour les grands groupes, mais elle devrait avoir un rôle de conseil et d'accompagnement pour les entreprises à l'export.

Il existe un grand nombre de certifications, mais aujourd'hui, la problématique est l'investissement dans les pépites et l'écosystème. Le plan d'un milliard est nécessaire, mais il faut aller au-delà. Pour faire une licorne, il faut investir dans une entreprise entre vingt et

cinquante millions d'euros. Je ne connais pas un fonds français qui est prêt à investir un tel montant sur une entreprise qui ne réalise pas de chiffre d'affaires. Toute la problématique se situe à ce niveau. Aux États-Unis, en Israël et dans quelques autres pays, vous avez des entreprises qui, avec quelques centaines de milliers d'euros de chiffre d'affaires, lèvent des centaines de millions et deviennent de véritables champions.

En France, nous avons laissé filer des pépites. Je veux vous donner l'exemple de Sentryo, qui a été créée par un entrepreneur français qui a développé une solution pour vérifier l'*IoT (Internet of the Things)*. Il a fait le tour des investisseurs français, qui ont regardé son dossier avec dédain. À cours de solutions, cet entrepreneur courageux a été obligé de passer sous drapeau américain. Malheureusement, les décideurs français regardent les dossiers d'investissement avec un œil de banquier, et non avec une prospective de souveraineté dans l'intérêt du tissu économique national.

M. Philippe Latombe, rapporteur. Voulez-vous dire qu'aujourd'hui, les entreprises de la cybersécurité sont trop petites et devraient se regrouper afin de pouvoir atteindre une taille critique qui leur permet d'avoir accès à des marchés plus gros et à des financements plus importants ?

M. David Ofer. Non, il faut qu'il y ait une floraison d'entreprises, parce que plus vous aurez d'entreprises qui vont émerger, plus vous aurez la chance d'avoir, au travers de l'une d'entre elles, des champions qui pourront créer de l'emploi, promouvoir notre économie et défendre notre souveraineté. C'est ce que nous n'avons pas aujourd'hui par manque de moyens.

M. Philippe Latombe, rapporteur. La floraison ne rend-elle pas plus difficile l'intégration de ces solutions dans le système d'information des clients ? Ne génère-t-elle pas un problème d'interopérabilité ?

M. David Ofer. La multiplicité des acteurs de la cybersécurité est liée à la multiplicité des outils informatiques. Un système d'exploitation ne se sécurise pas de la même manière qu'une base de données, qu'un réseau informatique, qu'un routeur, etc. Cette multiplicité de moyens demande une multiplicité d'outils de protection. Vous ne mettez pas un verrou sur une fenêtre, mais des barreaux.

M. Philippe Latombe, rapporteur. Si la cybersécurité est une conséquence d'une démarche d'ensemble (il faut que la cybersécurité soit présente sur l'ensemble de la chaîne numérique, de sa construction jusqu'à son utilisation), où faut-il investir aujourd'hui ? Où les entreprises de la cybersécurité doivent-elles être les plus proactives ?

M. David Ofer. Sur les systèmes d'information, la cybersécurité doit couvrir toute la chaîne. Vous ne sécurisez pas votre maison en laissant une fenêtre ouverte. C'est la raison pour laquelle aujourd'hui, des méthodes de R&D pratiquent la *security by design*, c'est-à-dire intègrent les problématiques de cybersécurité dès le début. Aux États-Unis, c'est devenu un standard. En France aussi. Néanmoins, ce n'est pas suffisant. On voit que même des géants se font aujourd'hui cyberattaqués et que certaines solutions américaines que l'on croyait sécurisées ne le sont pas du tout.

Il faut déployer ce *security by design* à chaque niveau d'utilisation. La partie *IoT* arrive, avec les outils connectés. Là se pose une problématique de sécurisation de l'un des maillons que l'on ne maîtrise pas. Cela fait partie des défis qui sont lancés aujourd'hui aux acteurs de la cybersécurité.

M. Philippe Latombe, rapporteur. Quelles sont les trois actions qui devraient être mises en place, qu'elles soient financières ou législatives.

M. David Ofer. Il faut savoir de quoi l'on parle. Veut-on de la souveraineté avec une indépendance ou veut-on partager notre data avec nos alliés ?

Aujourd'hui, nous sommes dans une position de faiblesse extrême. Comment peut-on vouloir une souveraineté européenne à partir du moment où l'on utilise des produits et des technologies non européens ? Je peux prendre des exemples pour être concret. L'OSCE (Organisme de la Sécurité et de la Coordination européenne) a passé il y a deux ou trois ans un appel d'offres pour sa cybersécurité. Il n'utilise que des produits américains !

Quand on parle de souveraineté et d'indépendance, il faut faire des choix difficiles. Sommes-nous prêts à jeter nos téléphones portables ? À jeter les systèmes d'exploitation ? À changer toutes les habitudes des utilisateurs que certains appellent des consommateurs ? Aujourd'hui, si vous voulez acheter un téléphone mobile français, un système d'exploitation français ou un ordinateur français, vous aurez beaucoup de mal. Cette problématique a un impact sur la cybersécurité, car il est très difficile de sécuriser des systèmes que l'on ne maîtrise pas de bout en bout.

Microsoft présente des failles de cybersécurité qu'il corrige régulièrement. Finalement, vous vous retrouvez dans la situation dans laquelle vous achetez des produits américains et, parce qu'ils ne sont pas sécurisés, vous devez acheter des antivirus américains. Ce faisant, vous appauvrissez votre pays, vous enrichissez les États-Unis et en plus, vous subissez quand même des cyberattaques.

Si j'avais le pouvoir, je mettrais en place un fonds de soutien pour les entreprises qui se font cyberattaquer et une contribution obligatoire pour les entreprises étrangères qui commercialisent leurs logiciels en Europe. Il faut qu'à un moment, ces entreprises payent une contribution qui soit reversée aux entreprises victimes des cyberattaques qui sont permises par les logiciels qu'elles nous vendent. C'est un sujet sur lequel nous travaillons à la Fédération. Nous espérons que nous pourrons le mettre en place en France, avec votre aide. Si cette contribution est mise en place, elle obligera les fournisseurs étrangers à déployer des efforts conséquents pour améliorer la qualité des systèmes qu'ils nous vendent.

M. Philippe Latombe, rapporteur. Y a-t-il d'autres sujets que vous voulez évoquer ou des sujets sur lesquels vous voulez remettre l'accent ?

M. David Ofer. Non, je suis là pour répondre à vos questions. J'ai donné beaucoup d'informations et d'exemples très concrets. J'ai martelé qu'il fallait favoriser la commande de produits français dans la commande publique. J'espère que le message est passé.

M. Philippe Latombe, rapporteur. Le message est passé. Le sujet a été identifié dès le début des travaux de la mission d'information.

Audition, ouverte à la presse, de MM. Pierre Lelièvre et Olivier Charlannes, vice-présidents de la société IDEMIA, et de M. Cosimo Prete, président fondateur de la société Crime Science Technology

(1er avril 2021)

Présidence de M. Jean-Luc Warsmann, président.

M. le Président Jean-Luc Warsmann. Avec MM. Olivier Charlannes, vice-président « Développement et marketing » de la société IDEMIA, Pierre Lelièvre, vice-président « Identité digitale » de cette même société et Cosimo Prete, président fondateur de la société Crime Science Technology, notre échange portera principalement sur l'identité numérique, qui s'entend comme la capacité à fournir aux citoyens et aux entreprises un moyen de s'authentifier avec un haut niveau de sécurité, lorsque ceux-ci accèdent à des services publics ou privés.

Nous nous intéressons aux enjeux de souveraineté technologique et de sécurité, afin de nous assurer que les solutions déployées sont les plus sûres et autonomes possible.

M. Philippe Latombe, rapporteur. Je souhaite d'abord que nous échangions sur les enjeux de l'identité numérique et sur la façon dont le déploiement de ces solutions, publiques ou privées, peut contribuer à renforcer la souveraineté numérique de la France et de l'Europe. À ce titre, j'aimerais vous entendre sur les choix faits, notamment dans le projet d'identité numérique régalienne, ainsi que sur le positionnement de notre pays par rapport à ses homologues européens. Le déploiement de ces identités numériques, qui devait intervenir à l'occasion du lancement de la carte nationale d'identité électronique (CNIe), suscite des inquiétudes sur lesquels vous nous donnerez votre avis.

J'aimerais ensuite que vous abordiez les conditions de réussite du déploiement de ces solutions auprès des citoyens et des professionnels, notamment sur les attentes et les besoins de ces utilisateurs, ainsi que sur les usages offerts par ces solutions. Nous pourrons ainsi prendre connaissance de l'état actuel du marché de l'identité numérique et échanger sur ses principales évolutions à venir. À cette occasion, nous évoquerons le modèle économique de l'identité numérique, qui a fait l'objet de nombreux débats. Concrètement, vous nous direz quelle doit être l'articulation entre l'action de la puissance publique et les solutions offertes par les acteurs privés dans ce domaine.

Je vous propose enfin de nous parler des enjeux de sécurité et de protection des données, qui préoccupent l'ensemble des utilisateurs de ce type de solutions. Vous nous indiquerez quelles sont leurs principales inquiétudes et comment les solutions d'identité numérique sont actuellement sécurisées.

M. Pierre Lelièvre, vice-président « Identité digitale » de la société IDEMIA. Je vous remercie de votre invitation. Pour IDEMIA, leader de la biométrie, il était important de pouvoir prendre part à ce débat.

De notre point de vue, l'identité numérique constitue la base de la souveraineté numérique de l'État, qui doit garantir une identité pour tous et assurer la sécurité de ses citoyens. Or, à l'heure actuelle, un citoyen sur six dans le monde ne dispose d'aucune identité. Ce point figure parmi les objectifs des Nations Unies pour 2030.

L'une des missions régaliennes de l'État est de garantir l'identité de ses citoyens, alors que notre économie se trouve actuellement en pleine transformation numérique, tirée par des

nouveaux usages en ligne. Ces usages imposent aux États de nouveaux enjeux de lutte contre la fraude, notamment à l'identité connectée. Selon nous, l'introduction de la biométrie demeure l'un des moyens les plus efficaces pour y répondre, car celle-ci fait le lien entre le document physique et l'identité numérique, en réduisant les risques de fraude à l'identité.

IDEMIA maîtrise la sécurisation de l'identité, notamment grâce à la biométrie. Il s'agit d'un Groupe international issu du rapprochement de fleurons de l'industrie française. Nous sommes présents dans cent quatre-vingts pays et investissons plus de 200 millions d'euros par an en recherche et développement (R&D). Nous possédons également plus de mille cinq cents familles de brevets actifs. Nous sommes donc un pilier du numérique français, engagé auprès du Gouvernement pour favoriser la recherche et l'emploi, notamment en France. À titre personnel, je suis responsable du développement de l'identité numérique dans le monde, pour le secteur public.

En tant que leader de l'identité augmentée, notre objectif est de contribuer à une identité pour tous. Nous fournissons une réponse technologique de confiance, avec pour mission de créer un écosystème pour servir tous les usages. Ces usages peuvent être aussi bien publics (disposer d'un document d'identité, accéder à des services en ligne tels que l'éducation, la santé ou les aides sociales) que privés (souscrire à une ligne téléphonique, ouvrir un compte bancaire).

Depuis plus de quarante ans, le Groupe IDEMIA agit auprès des gouvernements, les accompagnant dans leur stratégie vis-à-vis de l'identité civile, à la fois par le biais de documents physiques sécurisés et de solutions s'appuyant pour partie sur la biométrie. Dans les années 1970, nous avons créé le premier capteur et le premier moteur d'analyse biométrique au monde, pour le compte du *Federal Bureau of Investigation (FBI)*.

Depuis 2020, nous assistons l'agence européenne eu-LISA dans sa conception du système qui gérera les entrées et sorties du territoire européen. Il y a quelques jours seulement, nous avons été désignés, par le *National Institute of Standards and Technology (NIST)*, numéro 1 dans le monde sur l'un de nos algorithmes d'analyse biométrique.

Il ne peut pas y avoir de souveraineté nationale sans identité numérique. En effet, la multiplication des services en ligne appelle au renforcement du niveau de sécurité. À ce propos, la crise sanitaire aura prouvé que certains actes essentiels au bon fonctionnement de notre système ont dû être stoppés ou reportés, en particulier les élections de mars 2020.

De façon plus générale, nous avons besoin d'accéder à une multitude de services de façon connectée. Or l'État demeure le seul acteur en mesure de vérifier l'identité de la personne se trouvant en face de nous lorsque nous sommes connectés. En ce qui concerne notre échange par Zoom de ce jour, je n'ai pas pu prouver mon identité. Il est donc urgent que nous puissions disposer d'une identité numérique.

Certains acteurs, notamment les géants du net, ont pu collecter pendant des années les données des citoyens français ou d'autres pays dans le monde, sans aucun encadrement. En Europe, le Règlement général sur la protection des données (RGPD) a corrigé une partie de ce déséquilibre, mais celui-ci existe toujours. À ce sujet, la souveraineté implique de pouvoir solliciter des acteurs locaux partageant les mêmes valeurs, respectant les mêmes lois et les mêmes codes éthiques. Pour autant, l'égalité de traitement n'est pas respectée.

La donnée est nécessaire au développement d'un logiciel d'analyse biométrique. Or pour l'heure, il nous faudrait des années pour accéder au même volume de données que certains de nos concurrents Nord-Américains ou Asiatiques, car la réglementation européenne

actuelle ne nous permet pas de progresser à la même vitesse. Il est donc urgent de permettre à notre industrie de rester compétitive et d'avoir accès aux données de façon sécurisée, afin d'éviter les dérives observées dans d'autres régions.

Dans le secteur des télécommunications, certains acteurs européens comme Alcatel, qui ne disposaient pas du même appui gouvernemental que leurs homologues étrangers, ont vu leur position s'affaiblir. De la même manière que ce lien existe dans l'aéronautique, il devrait exister dans le domaine de l'identité, car il représente un enjeu majeur pour notre avenir.

Il est encore temps de renforcer le partenariat entre le public et le privé, pour compenser les déséquilibres. Notre intérêt n'est pas d'obtenir des subventions, mais de nous doter des moyens de rester dans la course. Pour y parvenir, IDEMIA souhaite la mise en place d'une réglementation permettant de protéger l'usager en respectant sa vie privée.

En parallèle, la compétitivité de notre industrie devra être soutenue. Nous pourrions par exemple nous inspirer de l'Allemagne, qui a transposé dans son droit interne la possibilité d'utiliser les données à des fins de R&D.

Nous devons protéger notre savoir et l'avance dont nous disposons encore. Plusieurs pistes existent, comme la création d'un label de fournisseur de confiance en matière d'identité numérique, dont la gestion pourrait, par exemple, être confiée à l'agence nationale de la sécurité des systèmes d'information (ANSSI). Il sera ensuite temps de définir ce que nous souhaitons mettre en place pour nos citoyens, en nous donnant les moyens de contrôler l'environnement mobile, de garder un droit de regard sur l'utilisation des données à des fins de recherche, ainsi que de disposer d'acteurs industriels supportant nos ambitions.

En France, un appel d'offres en cours devrait permettre de mettre en place la première étape de l'identité numérique. Si le retard pris s'explique en partie par la pandémie, tout retard supplémentaire n'enverrait pas un signal positif concernant notre capacité à nous doter d'un système d'identité numérique.

M. Cosimo Prete, président de la société Crime Science Technology. L'identité numérique et notre souveraineté sont des sujets qui me sont chers, car je suis un ancien expert de la police technique et scientifique.

Notre entreprise Crime Science Technology (CST) est spécialisée dans la fourniture de solutions de sécurité pour protéger les documents d'identité ou encore les billets de banque. Nous identifions également les personnes à partir de leurs empreintes digitales, grâce à des solutions déployées dans une vingtaine de pays dans le monde.

Chez CST, nous définissons la souveraineté numérique comme l'interaction harmonieuse entre l'État, les citoyens, les territoires et les acteurs économiques, dans l'intérêt du bien commun. Puisque la notion de frontière géographique n'a plus vraiment de sens dans le cadre du déploiement d'une solution d'identité numérique, il est important d'entretenir une relation de confiance entre les acteurs de l'industrie, les citoyens et l'État, afin de garantir l'identité de tous les individus.

S'il est désormais tout à fait possible de s'identifier à distance, rien ne dit en revanche que le support que vous tenez entre les mains est un document authentique. Il semble ainsi fondamental de combiner identité physique et numérique de manière harmonieuse, afin de pouvoir tirer le meilleur des deux mondes.

Les éléments déclinés à l'échelle européenne doivent pouvoir se retrouver au niveau national. Or nous sommes en droit de nous demander si le monopole régalien chargé de l'identité de confiance de tous les Français est en capacité de tirer le meilleur de ce que peut produire l'industrie française. Nous comptons des fleurons tels qu'IDEMIA ou Thales, plaçant la France dans le top 3 mondial des pays les mieux dotés en matière d'industrie de la sécurité. La question est de savoir si nous sommes en mesure de tirer le meilleur de tous les industriels et fournisseurs de solution, afin de garantir un niveau de sécurité maximal et une identité de confiance pour tous les Français.

Historiquement, la gestion des données n'a jamais été simple dans la culture française. Depuis l'après-guerre, une peur du fichage s'est même développée. L'enjeu est donc de regagner la confiance des citoyens, tant par une bonne gestion des données que par la manière dont celles-ci seront sécurisées sur les plans physique et digital. Chez CST, nous réfléchissons à cette relation de confiance, en prenant en compte les besoins opérationnels du terrain et les attentes des citoyens, tout en étudiant les meilleures façons de travailler avec les industriels pour déployer nos solutions.

L'organisation de l'aviation civile internationale (OACI) est une institution internationale chargée de formuler des recommandations de sécurité concernant les éléments électroniques, numériques et physiques des documents d'identité. C'est sur elle que s'appuie le Règlement européen pour concevoir nos titres français. Celle-ci produit également un état de l'art tous les trois ans. Je m'interroge toutefois sur la prise en considération de cet état de l'art dans notre identité numérique, tant sur sa composante physique que digitale.

En 2015, la Cour des comptes a affirmé qu'il était important de réfléchir à la façon de réguler le monopole d'État dans l'intérêt du bien commun. Or depuis la privatisation de l'Imprimerie nationale se pose la question de l'existence d'un conflit d'intérêts, car cette institution est devenue un centre de profits devant, dans le même temps, garantir la sécurité nationale. Il convient donc de s'assurer que nous disposons des outils de contrôle nécessaires pour tirer le meilleur de notre industrie.

M. Philippe Latombe, rapporteur. Vous avez indiqué que les géants du numérique avaient creusé leur avance, d'une part, en commençant à collecter les données plus tôt que nous, d'autre part, en bénéficiant d'un environnement juridique plus favorable à la poursuite de leur collecte. Quel type de données ont-ils collecté de manière massive ? Lesquelles vous seraient utiles en tant qu'industriels de la sécurité numérique ?

À ce jour, où en est la France par rapport à ses partenaires européens ? Existe-t-il des innovations apparues dans certains pays mais qui ne sont pas utilisées en France ? Connaissez-vous des pays situés hors de l'Europe présentant des niveaux de sécurisation de titres identiques ?

M. Cosimo Prete. Il y a environ trois ans, CST a été approché par la Bundesdruckerei (l'imprimerie nationale allemande), au sujet de notre solution de sécurisation *Optical variable material* (OVM). Cette technologie permet d'authentifier les documents en moins de trois secondes, aussi bien à l'œil nu qu'avec un simple appareillage. L'Allemagne a ainsi manifesté son intérêt lors du salon mondial de la sécurité de Londres en 2018. Depuis cette date, nous travaillons en toute confidentialité avec l'imprimerie nationale allemande, pour réfléchir au déploiement de cette technologie dans ce pays.

L'Allemagne pratique une véritable veille technologie, en s'appuyant sur des budgets colossaux. Ainsi, en 2015, le budget R&D de l'imprimerie nationale allemande était huit fois supérieur à celui de son homologue français, s'appuyant sur une politique très forte en matière

de propriété intellectuelle, ainsi que sur des partenariats tirant l'ensemble de l'écosystème vers le haut. Afin d'offrir le meilleur niveau de sécurité possible à ses documents, l'Allemagne ambitionne également d'aller chercher un certain nombre de solutions à l'extérieur. Ainsi, l'imprimerie nationale allemande construit et finance des programmes de R&D avec différents partenaires, notamment en collaboration avec les experts de la police allemande. Ces synergies ont permis à cette nation de mettre en place une identité électronique depuis une dizaine d'années. De son côté, la France reste l'un des derniers pays à déployer la sienne.

Le programme INES (identité nationale électronique sécurisée) a été lancé en 2005, posant les premiers jalons d'une CNIe. Du retard a ensuite été pris, probablement pour des raisons réglementaires quant à l'exploitation des données. Le projet de l'époque a alors été transféré sur le titre de séjour et sur le permis de conduire électroniques. Les technologies nécessaires étaient donc déjà disponibles, il y a une dizaine d'années. Avec les autres experts, nous ne comprenons pas comment autant de retard a alors pu être pris dans la conception de ce document, tant sur le plan physique que numérique. À l'inverse, les Allemands ont su mettre à profit ce qu'ils avaient accompli il y a une dizaine d'années, pour désormais évoluer.

Plusieurs centaines de milliers d'usurpations d'identité sont recensées chaque année en France. La fraude sociale se chiffre par exemple à 14 milliards d'euros pour l'État. Il est donc surprenant de constater que les moyens consacrés à la R&D demeurent limités, comparativement à ce que pratiquent nos voisins.

L'Allemagne scrute avec attention l'état de l'art triennal de l'OACI, dans lequel figure CST. À l'heure actuelle, une cinquantaine de technologies ont été identifiées à l'échelle mondiale, dont une quarantaine concerne la sécurité numérique et une dizaine la sécurité physique. Sur ces dernières, trois proviennent de chez CST. À ce stade, je m'interroge donc sur l'absence de ces solutions sur notre titre régalien, alors qu'elles profitent à des pays tels que l'Allemagne ou d'autres situés en Océanie. Il est en effet surprenant que la France ne soit pas capable de mettre en œuvre les meilleures solutions présentes sur son territoire.

La photo en noir et blanc figurant sur notre carte d'identité est fournie par une solution américaine, alors qu'IDEMIA ou Thales sont capables de produire une photo en couleur depuis plusieurs années. Une telle solution est déjà proposée dans des pays comme l'Estonie. Je m'interroge donc sur les choix technologiques ayant été faits, qui témoignent parfois d'un certain archaïsme. En effet, la moyenne d'âge des éléments de sécurité actuellement embarqués sur notre titre sécurisé dépasse la dizaine d'années, alors qu'il a paradoxalement été préconisé de limiter la durée de ce titre à dix ans, pour des raisons de sécurité.

Les innovations présentées par la presse n'en sont pas véritablement. Pour preuve, l'une des sécurités embarquées date d'il y a une trentaine d'années. Celle-ci a été préférée à une solution française figurant dans le dernier état de l'art. Cette tendance se vérifie également pour le cachet électronique visible (CEV), qui date d'il y a une dizaine d'années, alors qu'il serait possible de recourir à une norme universelle interopérable. Tous ces choix suscitent des interrogations sur le pilotage des projets, ainsi que sur l'articulation entre l'agence nationale des titres sécurisés (ANTS), l'Imprimerie nationale et l'ensemble des fournisseurs français.

M. Pierre Lelièvre. Il faut établir une distinction entre le volet lié au document et le volet numérique de l'identité française. Ce dernier a été lancé en 1974, avec l'initiative SAFARI (système automatisé pour les fichiers administratifs et le répertoire des individus), qui s'est conclue par la création de la CNIL (commission nationale de l'informatique et des libertés). Nous avons donc pris le temps de bien étudier les différents modèles dont il était possible de s'inspirer. Un certain nombre d'expérimentations ont ainsi été réalisées en France, nous permettant de tirer de nombreux enseignements des initiatives passées. J'espère à présent

que l'accélération dont nous avons besoin se produira dans les mois à venir, tant en matière de volume que de valeur apportée par l'identité numérique.

La qualité du résultat du développement d'algorithmes dépendra de la qualité de la donnée initialement injectée. Nous disposons encore d'une certaine avance en la matière mais sans accès à la donnée, cette avance finira par être remise en question. Or les GAFAM (Google, Apple, Facebook, Amazon et Microsoft) ont eu accès à un volume de photos sans précédent. L'enjeu est donc de pouvoir accéder à ces données, pour les transposer en informations biométriques et ainsi améliorer les performances de l'algorithme.

Dans le monde, il n'existe pas une façon unique de traiter un système d'identité numérique. En Europe, le modèle estonien sert de point de référence, avec une taille critique permettant de prendre des décisions plus facilement. Il a tout de même fallu près de vingt ans avant que ce système obtienne un taux de pénétration satisfaisant.

La vraie question pour la France est de savoir comment se donner les moyens d'une identité numérique accessible à tous. Pour y parvenir, le virage vers le « tout numérique » est souvent évoqué, mais celui-ci devra tout de même être accompagné, notamment de pédagogie. Des moyens humains seront nécessaires, afin de proposer des parcours alternatifs. Quoi qu'il en soit, l'utilisation d'un modèle complètement numérique ne nous semble pas réaliste et ne constituera pas un facteur clé pour créer la confiance entre les utilisateurs et la technologie.

L'Estonie se repose fortement sur son titre sécurisé équipé d'une puce permettant d'accéder à un panel de services en ligne. Dans ce pays, il est possible d'effectuer l'ensemble des opérations de la vie de tous les jours grâce à son identité numérique.

D'autres modèles étrangers s'appuient sur des infrastructures radicalement différentes. En effet, chaque pays où nous intervenons présente une législation et une population qui lui sont propres. En 2010 par exemple, l'Inde a démarré son virage vers l'identité numérique, en déployant le programme Aadhaar. L'État a alors demandé à ses citoyens de partager leurs informations biographiques et biométriques, dans un but de pratiquer la déduplication. Cette technique permet de valider qu'une même personne n'existe pas sous plusieurs noms différents. Plus de 90 % des 1,3 milliard d'Indiens ont été « embarqués » dans ce système. Équiper autant de personnes d'un titre sécurisé a toutefois représenté un coût très élevé.

En plus de disposer de documents sécurisés, certains gouvernements d'Amérique latine se sont par ailleurs dotés d'un système biométrique permettant aux différents acteurs des pays de vérifier l'identité des personnes.

De son côté, le modèle européen s'est tourné vers un titre sécurisé, pour des raisons historiques. Dans tous les cas, l'identité numérique implique de passer par plusieurs étapes. Il faut d'abord valider le document en lui-même, avant de s'assurer que sa date de péremption n'est pas dépassée. Seul le Gouvernement est en mesure d'effectuer ces opérations. Une fois le titre d'identité validé, ce même Gouvernement se charge d'y associer le porteur. Plusieurs technologies existent pour y parvenir. La biométrie est par exemple très largement déployée dans le monde, en raison de sa grande facilité d'utilisation.

M. Philippe Latombe, rapporteur. Le projet Aadhaar incluait effectivement les analyses biométriques des dix doigts et des deux iris. Le problème de la biométrie est que ces informations se retrouvent parfois à des endroits où elles ne devraient pas. Une partie des informations d'Aadhaar a ainsi été vendue par des pirates, pour se retrouver sur le dark web. Je me demande donc si la biométrie est suffisamment sécurisée ou si elle ne constitue pas au

contraire une nouvelle mine d'or pour certains hackers, y compris au titre de l'Intelligence entre pays.

M. Pierre Lelièvre. Les logiciels IDEMIA sont utilisés en Inde mais le programme est ensuite géré en local. Le stockage et la protection des données n'a donc pas fait partie de notre champ d'action. Notre rôle est d'accompagner les gouvernements et de leur montrer l'état de l'art pour collecter ces données, les stocker et les gérer de façon sécurisée. Nous insistons par exemple sur la nécessité de séparer et de rendre anonymes un certain nombre d'informations.

M. Philippe Latombe, rapporteur. En France, au sujet de la sécurisation du titre ou de l'identité numérique associée, vos interlocuteurs sont-ils en capacité d'accepter ce que vous leur proposez ? À cet égard, le fait de recourir à une technologie américaine pour mettre une photo en noir et blanc sur un titre d'identité, alors même que des sociétés françaises comme Thales ou IDEMIA sont capables d'offrir de la couleur, pose question.

M. Pierre Lelièvre. Nous n'utilisons pas les photos sur la partie biométrique, car le procédé consiste, dans un premier temps, à transformer la matière brute. Ainsi, la photo est transformée en un *template* qui permettra d'en tirer une analyse biométrique, mais celui-ci n'est pas directement exploitable. Il sera alors stocké, *via* plusieurs niveaux de chiffrement. Les premières informations dont nous disposons sont donc stockées dans le coffre-fort de l'État.

L'identité est prouvée au moment de sortir son document. Il existe ainsi un décalage entre les usages demandés en ligne et les moyens dont nous disposons à l'heure actuelle pour nous authentifier.

Sur les documents physiques, nous investissons plus de 200 millions d'euros par an. Nous investissons également massivement dans des technologies liées à la photo, notamment en couleurs, permettant de valider que le document en présence a bien été émis par un gouvernement. Sur ce point, nous proposons de nombreuses technologies différentes aux gouvernements du monde.

M. Philippe Latombe, rapporteur. L'État pratique-t-il le *sourcing* ? Accepte-t-il de se pencher sur les nouvelles technologies ou préfère-t-il se réfugier dans une forme de conformisme ? Sur certaines solutions totalement numériques, les acheteurs publics n'ayant pas le temps de pratiquer le *sourcing*, ces derniers se contentent de passer des marchés publics qu'ils connaissent déjà. Cette tendance conduit à conserver des technologies anciennes et généralement américaines, pour lesquelles l'ensemble des briques sont rassemblées en un même endroit. En toute logique, c'est l'ANTS qui devrait s'occuper de ces sujets. Quoi qu'il en soit, sommes-nous en capacité d'aller sourcer le meilleur de l'état de l'art, pour ensuite donner l'ordre à l'Imprimerie nationale de faire le nécessaire ?

M. Pierre Lelièvre. La sécurité s'apparente à une course contre des acteurs produisant des attaques et gérant de la fraude dans nos systèmes. Cette course ne connaît pas de fin et nous pousse en permanence à nous remettre en question et à développer des innovations. Par conséquent, ni la France, ni l'Estonie, ni aucun autre pays dans le monde ne se trouve à un niveau maximum de protection de ses documents d'identité, car il est toujours possible de faire mieux. Nous développons donc constamment des innovations, qui doivent ensuite accéder au terrain.

Au sujet de la CNIe, nous faisons partie des fournisseurs, notamment de la puce. Celle-ci permettra une évolution significative, en matière de niveau de sécurité, pour vérifier l'authenticité du titre. Cette puce respecte également tous les standards du marché.

M. Olivier Charlannes, vice-président « Développement et marketing » de la société IDEMIA. Il existe des technologies alternatives à celles ayant fait l'objet d'une décision du Groupe Imprimerie nationale. D'autres éléments de sécurité qui seront inscrits sur la CNIe ont en effet été sourcés sur le territoire français par le biais d'autres sociétés. Dans ce cadre, une évaluation est menée sur l'ensemble des fonctions de sécurité.

La sécurité d'un document physique dépend d'une combinaison de l'ensemble des fonctions de sécurité intégrées sur ce document. Or il nous est difficile d'affirmer qu'il aurait fallu ajouter telle fonction plutôt qu'une autre, car IDEMIA est actuellement partie prenante du projet de lancement de la nouvelle CNIe, en particulier au niveau de la puce et du logiciel embarqué. Ce dernier a été développé par nos équipes de R&D en France et a été certifié au plus haut niveau de sécurité par l'ANSSI.

M. Cosimo Prete. S'agissant de l'évaluation de la sécurité, les forces de l'ordre observent au quotidien les retours du terrain. Les agents disposent en moyenne de cinq secondes pour contrôler un document. Ils n'ont donc pas le temps d'examiner les changements de couleur, le nombre d'étoiles ou encore de tourner la pièce à quatre-vingt-dix degrés. Ils ont donc besoin de quelque chose d'intuitif, que tout le monde peut comprendre et mémoriser en moins de trois secondes. Les informations concernant l'évaluation de la fraude sont ensuite remontées au niveau de l'ANTS et de l'Imprimerie nationale, lorsque des réunions sont organisées, car la conduite du projet ne comporte aucun point d'étape.

La moyenne d'âge des éléments de sécurité est supérieure à une dizaine d'années. Hormis la puce, le package proposé s'avère ainsi plus ou moins équivalent à celui du permis de conduire ou du titre de séjour européen (TSE). L'année dernière, Europol a constaté que des falsifications de ces titres ont été retrouvées dans certaines officines de faussaires démantelées en France et en Europe. Or les spécialistes du ministère de l'Intérieur et les experts de l'Imprimerie nationale se sont aperçus que les mêmes techniques étaient employées pour le document d'identité nationale. Il semble donc surprenant que des combinaisons d'éléments de sécurité figurant sur des titres dits secondaires se retrouvent sur notre document régalien, qui se doit d'être le plus sécurisé de tous.

M. Philippe Latombe, rapporteur. Il me semblait que le ministère de l'Intérieur était le donneur d'ordre *via* l'ANTS et que l'Imprimerie nationale était l'exécutant. À cet égard, un marché public doit avoir été lancé avec un cahier des charges. Comment se fait-il que le ministère de l'Intérieur n'ait pas déjà été au courant de ces éléments ?

Par ailleurs, il avait initialement été convenu que la CNIe et l'identité numérique seraient disponibles en même temps, alors que les deux ont finalement été décorrélées. L'État n'est-il donc pas en capacité de gérer ce type de sujets en mode projet ? Le retard de l'un a-t-il entraîné le retard de l'autre ?

M. Cosimo Prete. L'absence d'appel d'offres pour la partie relative à la conception physique du document constitue une véritable difficulté. Cette situation est liée au monopole régalien de l'État, qui exclut toute forme de compétitivité technologique et économique.

Une autre difficulté majeure concerne les effectifs de l'ANTS, qui ne comptent plus qu'un seul ingénieur spécialisé. L'agence cherche donc actuellement à recruter un chef de projet pour le programme CNIe, ce qui paraît inquiétant.

Il n'est pas possible d'être expert à la fois de la partie juridique, normative et industrielle. Or il me semble qu'une seule personne est pour l'instant en charge du sujet et le porte à bras-le-corps. Au final, une forme de déséquilibre se crée entre le donneur d'ordre et

l'exécutant. Faute de pouvoir pleinement engager sa responsabilité, en raison d'un manque d'expertise, il me semble que le projet repose davantage sur l'exécutant.

Dans le même temps, l'avis des experts de la police et de la gendarmerie n'est plus écouté, car ces derniers s'autocensurent, faute de pouvoir exiger des technologies. Par conséquent, pour un élément de sécurité donné, l'ANTS affirmera que l'Imprimerie nationale ne lui a soumis aucune proposition, alors que l'Imprimerie nationale répondra que l'ANTS ne lui a pas demandé l'élément de sécurité en question. De fait, l'Imprimerie nationale finira par l'emporter, car c'est elle qui propose la combinaison figurant sur le document final.

Il n'existe pas de cahier des charges mais plutôt des cibles de sécurité posant une problématique opérationnelle de terrain, à laquelle une réponse tente d'être apportée sans y associer de nombre de sécurités. Tout le monde finit ainsi par se renvoyer la responsabilité, pour aboutir à une forme de raisonnement circulaire. À l'arrivée, une réponse est apportée à la cible de sécurité mais il n'est pas certain que celle-ci soit la meilleure possible.

Le Règlement de l'Union européenne formule des demandes très précises. Par exemple, pour une encre optiquement variable, différentes solutions existent sur le marché. Il est alors très simple de comparer les éléments de sécurité, au moins en ce qui concerne la partie physique. Ces éléments présentent trois niveaux de contrôle : à l'œil nu, avec un petit appareillage, en laboratoire. Un quatrième niveau sera bientôt ajouté, avec le téléphone portable. Lorsqu'un élément de sécurité retenu ne peut être vérifié que sur un seul niveau de contrôle alors qu'une autre technologie répondant à la même fonctionnalité peut se vérifier sur quatre niveaux de contrôle, je m'interroge sur la politique mise en œuvre. Il semble en effet que la politique du « moins-disant » soit privilégiée, par méconnaissance des éléments de sécurité et des technologies déployées sur le terrain.

En 2018, l'Imprimerie nationale a pris l'initiative, avec l'ANTS, de proposer notre technologie à la Commission européenne, pour sécuriser le TSE. La technologie a alors été éprouvée en profondeur par l'Imprimerie nationale. Nous avons ensuite été « retoqués », au motif que l'ANTS et l'Imprimerie nationale considéraient que notre technologie ne répondait pas à la norme. Trois ans plus tard, nous avons pourtant appris que la norme avait mal été interprétée. Ironiquement, notre technologie en question est désormais classée dans le top 50 de cette norme.

M. Pierre Lelièvre. Je suis d'accord avec M. Cosimo Prete concernant l'importance de disposer de moyens pour contrôler l'identité sur le terrain.

Par ailleurs, le contexte actuel diffère radicalement de celui de 2019. Nous sommes ainsi contraints de nous connecter en ligne pour échanger, opérer ou effectuer des transactions. Aussi critique que soit la vérification des titres physiques, nous nous trouvons désormais en plein virage numérique. Cette tendance existait déjà depuis plusieurs années, mais connaît actuellement une forte accélération à cause de la crise sanitaire. Or, personne n'avait anticipé le niveau des attentes auxquelles nous sommes confrontés.

S'agissant de notre souveraineté numérique, nous faisons face à un déséquilibre, car nous nous trouvons face à des acteurs en position dominante maîtrisant l'environnement mobile. Le smartphone est désormais devenu totalement incontournable, dans le domaine privé comme dans le public. À l'heure actuelle, ces téléphones sont maîtrisés par deux acteurs décidant de ce qu'il est possible ou non de réaliser avec eux. Ainsi, certains choix commencent déjà à se fermer pour nous. Si nous ne prêtons pas la plus grande attention à la façon dont nous souhaitons nous positionner, en tant que nation ou en tant qu'Europe, face à ces acteurs gérant

une partie de notre écosystème, nous finirons par rater le virage et il sera presque impossible de le rattraper.

Il convient donc de nous interroger sur notre façon d'utiliser les téléphones et sur les informations qui y seront disponibles. Dans le cas contraire, nous serons amenés à charger des informations liées à notre identité pivot sans savoir où celles-ci se retrouveront. Nous pourrions par exemple exiger de la part de ces acteurs un certain niveau de sécurité concernant la zone de stockage et la zone d'exécution. Il sera donc nécessaire de décomposer les étapes et les informations que nous avons besoin de partager, ainsi que de nous demander comment elles seront utilisées. Pour rappel, lors de la parution du RGPD, ces acteurs ont tenté de lutter contre les contraintes que celui-ci impliquait.

Nous nous trouvons à un point critique où un système d'identité numérique est en passe d'être lancé à l'échelle de la nation. Cette identité numérique reposera sur un certain nombre d'infrastructures. Les fournisseurs de service tels que les collectivités locales, les banques ou les opérateurs auront besoin d'accéder à l'information gouvernementale, car c'est bien l'État qui est en mesure de confirmer l'identité d'une personne. Cette information devra de toute façon être partagée sur certains supports, qu'il s'agisse d'ordinateurs ou de téléphones portables.

Nous avons donc besoin d'exprimer nos exigences et d'établir une certaine normalisation. Un premier niveau a été mis en place en ce qui concerne les données avec le RGPD. Un deuxième l'a également été avec le Règlement *eIDAS (Electronic Identification Authentication and trust Services)*, qui a permis d'atteindre un premier objectif d'harmonisation au sein de l'Europe. Nous devons désormais nous montrer plus spécifiques concernant nos attentes vis-à-vis des parties prenantes. Sur ce point, impliquer les GAFAM me paraît être une bonne façon de répondre à l'accélération face à laquelle nous nous trouvons.

M. Philippe Latombe, rapporteur. L'année dernière, les députés ont adopté une loi interdisant la simple déclaration de majorité sur Internet pour la visite de sites pornographiques. Le conseil supérieur de l'audiovisuel (CSA) est en train de mettre cette loi en pratique, en demandant à ces sites de vérifier que les personnes souhaitant y accéder sont bien majeures. Comment y parvenir, alors que l'identité numérique n'est pas encore disponible ? Des pistes existaient autour du micro-paiement bancaire mais elles ont été rejetées par le CSA, car certaines cartes bancaires peuvent être délivrées avant l'âge de 18 ans. FranceConnect représente une autre option. Un système de capture d'écran pourrait également être envisagé, la personne montrant sa carte d'identité pour accéder au site.

Au final, nous ne sommes pas en capacité de mettre en œuvre la loi adoptée. Ce retard sur l'identité numérique n'est-il pas le signe que le sujet a été pris à l'envers ?

M. Pierre Lelièvre. Nous avons participé à un certain nombre de groupes de réflexion autour de la question des usages, animés par le ministère. Cette question se pose dans de nombreux pays, en lien avec le contenu de certains sites ou à la consommation de certains produits, pour lesquels il est nécessaire de prouver son identité ou son âge. La question est donc de savoir comment partager certaines informations sans forcément transmettre l'intégralité du contenu figurant sur nos documents d'identité.

Un moyen de pallier la difficulté est de considérer l'identité comme un service pouvant être offert par l'État à sa population. L'idée est de percevoir l'identité comme un besoin fondamental, en particulier l'identité numérique. Nous pourrions alors disposer d'un service de l'État auquel il serait possible de se connecter pour accéder à certaines d'informations pertinentes aux cas d'usage. Ainsi, dans le cas où l'âge d'une personne devait être vérifié,

seule cette information serait disponible. Or il existe déjà des solutions permettant de ne contrôler qu'une partie des attributs définissant notre personne. À titre personnel, je ne souhaite pas partager mon adresse avec n'importe quel fournisseur de service ou acteur.

Quoi qu'il en soit, la technologie existe déjà et il nous reste désormais à définir la façon dont nous souhaitons la mettre en œuvre pour répondre aux différents cas d'usage.

M. Philippe Latombe, rapporteur. L'État dispose-t-il des talents nécessaires pour mener à bien ce projet ? J'ai cru comprendre que l'ANTS manquait d'experts.

M. Pierre Lelièvre. La France possède un vivier d'universités extrêmement pertinent. De notre côté en tout cas, nous ne rencontrons aucune difficulté pour recruter, tant pour les profils ingénieurs que commerciaux.

M. Philippe Latombe, rapporteur. L'État a-t-il la capacité de trouver des personnes à la fois intégrées en son sein et ouvertes sur le plan technologique, afin de pratiquer le mode projet ?

M. Pierre Lelièvre. Nous menons de nombreux projets avec le Gouvernement ainsi qu'avec l'Europe, sans pour autant rencontrer de problèmes de gestion. Dans ce cadre, nous émettons des recommandations, mais toutes ne sont pas entendues. Je suis en tout cas satisfait de nos échanges avec l'ANTS ou avec les forces de l'ordre.

L'État n'est pas seulement accompagné par des acteurs tels qu'IDEMIA ou des start-up, mais également par certains grands intégrateurs. Par exemple, l'appel d'offres sur l'identité numérique lancé en fin d'année sollicite l'aide de ces intégrateurs. Ainsi, le Gouvernement français semble bien conseillé.

M. Philippe Latombe, rapporteur. J'évoquais le mode projet car d'autres auditions ont mis en évidence que certains ministères n'étaient pas en capacité de gérer par projet.

M. Pierre Lelièvre. S'agissant de l'identité numérique, nous considérons que les moyens mis en œuvre sont insuffisants par rapport aux attentes et aux enjeux.

M. Philippe Latombe, rapporteur. Selon vous, les montants de l'appel d'offres semblent trop restreints ?

M. Pierre Lelièvre. Oui, très clairement. Je pense que nous ne sommes pas parvenus à nous maintenir dans les objectifs qui nous avaient été fixés. D'un point de vue technologique, cet appel d'offres répond vraiment à la situation actuelle, en prenant en compte différents types de documents à valider. Il permet également de se projeter vers l'avenir, avec l'utilisation de la biométrie.

M. Philippe Latombe, rapporteur. S'agit-il d'un appel d'offres alloti ou général ?

M. Pierre Lelièvre. L'appel d'offres est alloti, comme c'est souvent le cas à l'heure actuelle. Pour y répondre, un cahier des charges très précis a été formulé et a évolué en suivant certaines recommandations, notamment en provenance de l'ANSSI. Nous avons alors été amenés à travailler en consortium avec d'autres entreprises, chacune devant y trouver sa place. Nous n'avons toutefois pas été en mesure de totalement répondre aux conditions financières demandées, alors que notre réponse était cohérente sur le plan technique.

M. Philippe Latombe, rapporteur. Aucun appel d'offres n'a été lancé sur la partie relative au titre physique ?

M. Cosimo Prete. À notre connaissance, les éléments de sécurité physique de la carte n'ont fait l'objet d'aucun appel d'offres.

Je suis en grande partie d'accord avec les propos tenus par M. Philippe Lelièvre. Un élément m'interpelle cependant au sujet de l'authentification à distance. À ce propos, le CEV vient d'être présenté par l'ANTS, alors qu'un tel dispositif était encore inimaginable il y a deux ans. Les mouvements associatifs ont en effet dû batailler pour faire intégrer le CEV sur la carte. Le contraste semble ainsi saisissant avec les annonces du Président de la République. Si les associations n'avaient pas bataillé à travers des collectifs, notre CNI ne comporterait pas de CEV.

Le CEV ayant été adopté sur notre CNI en est à sa version 101 et non 105. Par conséquent, chaque fois qu'un nouveau cas d'usage n'ayant pas été prévu par le CEV actuel se présentera, il sera nécessaire de réactualiser l'ensemble du système. À l'inverse, la version 105 du CEV a été validée selon la dernière norme AFNOR pour être universelle et interopérable, avec une mise à jour des différentes fonctionnalités. Nous nous fixons ainsi nos propres limites, en adoptant la version 101 et non 105 du CEV, alors que cette dernière pourrait être lue hors de France.

Par effet ricochet, cette décision plombera d'autres projets comme le pass sanitaire (qui consistait à déployer une solution française à l'échelle européenne), à cause de l'absence d'un référencement national stratégique. Cette situation semble vraiment surprenante.

M. Philippe Latombe, rapporteur. Vous voulez dire que l'avenir n'a pas assez été anticipé ?

M. Cosimo Prete. Assurément.

Je ne suis pas favorable au « tout digital » ni au « tout physique ». Il faut plutôt combiner le meilleur des deux mondes de manière harmonieuse. À ce sujet, l'ANSSI a lancé en mars le référentiel d'exigences applicables aux prestations de vérification d'identité à distance (PVID). Si certains fournisseurs de solutions devront travailler à l'authentification à distance de ce document, il est aberrant de penser que toutes les données pourront être contenues dans un téléphone portable ou dans une carte. Il existe en revanche des technologies permettant de déterminer que le CEV placé sur le document et le document en lui-même sont tous les deux authentiques. Il ne faut donc pas chercher à opposer les deux mondes.

En l'éclairant à l'aide d'un téléphone portable, il est possible de faire changer la couleur du CEV et ainsi de prouver à la caméra l'authenticité du support et du CEV. Cette méthode sera déployée chez nos voisins alors qu'il s'agit d'une solution française. Nous ne sommes donc pas capables de préparer l'avenir. Des impératifs nous sont indiqués mais nous ne parvenons pas à nous donner les moyens intellectuels, économiques et industriels pour aller plus loin.

L'enjeu est de déterminer la part de mixité technologique entre les grands fournisseurs de solutions et le monopole de l'État pour préparer l'avenir ensemble. Nous rencontrons des difficultés sur ce point, notamment car les ressources dont nous disposons en matière de gestion de projet ne sont pas à la hauteur de nos ambitions.

M. Philippe Latombe, rapporteur. Notre identité numérique sera disponible bien plus tard que ce qui était initialement prévu. Combien de temps faudra-t-il attendre avant que celle-ci ne soit lancée ?

M. Pierre Lelièvre. Différentes étapes devront être franchies, mais il faudra un peu plus d'un an pour mettre en place la première brique de ce système d'identité numérique. Une partie est déjà disponible chez FranceConnect, qui doit généraliser certains éléments tels que l'accès à DOCVERIF. Ce système permet de valider un certain nombre d'informations auprès de l'État, par exemple pour vérifier qu'un document existe bel et bien ou qu'il est toujours en cours de validité. À l'heure actuelle, ces informations ne sont pas encore totalement généralisées dans le modèle.

Le seul fait de disposer d'une puce dans les documents permettra de débloquer un certain nombre d'usages en ligne, car ces puces demeurent des éléments extrêmement sécurisés. Elles sont par exemple utilisées dans les passeports pour passer les frontières. Elles permettent également de disposer d'une authentification de niveau élevé auprès des différents fournisseurs de services. À ce sujet, le Règlement européen considère la puce comme l'élément ultime qui permettra de procéder à l'authentification d'un document puis à l'identification d'une personne. Ce dispositif vérifiera notamment que la photo présente à l'intérieur de la puce correspond réellement à la personne en question. Plusieurs méthodes permettront d'y parvenir. L'ANSSI envisage de placer un humain de l'autre côté de la vidéo, mais il est également possible d'utiliser un système automatique. Quoi qu'il en soit, les deux approches devront être complémentaires.

M. Philippe Latombe, rapporteur. Le temps que l'identité numérique, telle qu'elle est prévue dans l'appel d'offres, soit mise en place, de nouveaux usages non prévus risquent-ils d'émerger d'ici douze à vingt-quatre mois, générant ainsi un blocage à l'arrivée ? Cette éventualité a-t-elle été intégrée dans le process ?

M. Pierre Lelièvre. Des nouveaux usages émergent en permanence. En Estonie par exemple, il est désormais possible de voter avec son document d'identité.

M. Philippe Latombe, rapporteur. Le vote figure parmi les grands sujets que nous avons évoqués hier. Le conseil scientifique a en effet affirmé que si nous avions pu vérifier l'identité numérique des citoyens, il aurait alors été possible d'organiser des élections municipales et régionales dans des conditions sanitaires convenables. La question est donc de savoir si nous disposerons d'une interopérabilité complète pour assurer ces nouveaux usages, dont l'émergence n'est pas forcément encore connue.

M. Pierre Lelièvre. Il est nécessaire de protéger la santé de nos concitoyens, en leur offrant la capacité de voter en ligne. Dans le même temps, nous avons besoin de protéger notre République, en nous assurant que les élections se déroulent dans un certain cadre. À l'heure actuelle, je ne pense pas que nous soyons en mesure d'affirmer que nous disposons d'un système permettant d'organiser des élections de façon connectée. Une telle mesure ne serait de toute façon pas en ligne avec la réglementation européenne.

En tant qu'industriel, notre rôle est de déterminer si la technologie actuellement disponible nous permet d'« adresser » ces cas d'usage. Or nous y parvenons déjà dans d'autres pays et pas seulement en Estonie. De manière générale, tous les projets dans le monde doivent faire face à une certaine flexibilité. S'il est utile de disposer d'un cahier des charges initial, certains critères évolueront en fonction de l'actualité, comme c'est en ce moment le cas.

Les informations de base dont nous aurons besoin seront présentes sur la puce de la prochaine carte d'identité. Ces informations permettront de passer à des cas d'usage nettement plus critiques, comme les élections. Il sera toutefois nécessaire de légiférer pour y recourir.

M. Philippe Latombe, rapporteur. Il semble que les individus ne voient pas trop d'inconvénients à utiliser leur empreinte digitale pour déverrouiller leur téléphone, ou à présenter leur visage pour déverrouiller leur ordinateur. À l'inverse, à partir du moment où l'État souhaite récolter des données biométriques pour sécuriser l'identité de ces citoyens, un problème finit par se poser. Quel est donc votre point de vue sur la façon dont l'opinion perçoit le recours à la biométrie ?

M. Pierre Lelièvre. La biométrie est de plus en plus utilisée. Je pense donc que le niveau de confiance s'améliore. Le grand public est en tout cas en train de se familiariser avec des systèmes d'authentification biométriques. S'agissant du téléphone, les empreintes ont d'abord fait leur apparition, avant d'être suivies par la reconnaissance faciale.

Nous avons besoin de recourir à la pédagogie, ainsi que de mieux expliquer ce que nous souhaitons faire et comment nous comptons y parvenir. Sur ce point, il est essentiel d'établir une distinction entre l'identification et l'authentification. Un dispositif d'identification de masse au sein d'une population donnée sera perçu comme un système de surveillance, alors que l'authentification consiste à prouver qu'un nom correspond bien à une personne donnée. Pour leur part, les téléphones pratiquent essentiellement l'authentification et n'ont pas vraiment intérêt à recourir à l'identification.

Il existe trois niveaux de sécurité pour s'authentifier : ce que l'on possède, ce que l'on sait et ce que l'on est. Pour augmenter le niveau de sécurité, nous cherchons à associer toutes ces notions. Vous possédez ainsi un titre sécurisé dont la puce contient un certificat doté d'éléments cryptographiques permettant d'attester de façon certaine qu'il s'agit bien d'une carte du Gouvernement français. Cette carte peut également vous distribuer un code PIN. En entrant ce code, vous démontrerez que vous êtes effectivement la bonne personne ayant reçu la carte, comme c'est le cas dans le domaine bancaire. Enfin, le dernier niveau de sécurité est incarné par la biométrie, qui consiste à démontrer que vous êtes bien une vraie personne avec un visage en trois dimensions et que ce visage correspond au nom affiché.

La biométrie paraît assez largement utilisée aujourd'hui, que ce soit dans le monde du mobile ou dans la sphère gouvernementale, dans d'autres régions du monde. Il existe ainsi une question relative au téléphone et à la confiance accordée à l'État. Sur ce point, il est vrai que la défiance s'avère plus forte lorsqu'il est question de partager plus d'informations. Je ne sais pas si cette perception concerne l'ensemble des citoyens français ou si elle résulte simplement de certains lobbies. Toujours est-il que l'État demeure le mieux placé en la matière, car il dispose de plus d'informations, que n'importe quel acteur privé.

Certaines chaînes de grande distribution demandent des informations biométriques à leurs clients afin qu'ils puissent réaliser leurs achats. À titre personnel, je ne suis pas tellement favorable à de telles pratiques, car nous ne savons pas comment sont stockées ces données, comment elles sont protégées, ni qui peut y accéder.

La confiance entre le Gouvernement et la population ne se créera pas toute seule. Pour y parvenir, il sera nécessaire d'expliquer précisément pourquoi et comment les identités numériques seront gérées. Celles-ci ne seront peut-être pas destinées à des fins d'identification mais plutôt d'authentification, afin de permettre aux individus d'effectuer des transactions de façon plus sereine sur le web, par exemple pour accéder à des services ou pour vendre des objets.

La biométrie demeure donc un vrai enjeu. La question n'est plus de savoir si elle sera utilisée, car elle l'est déjà, mais quand elle le sera dans ce contexte.

M. Philippe Latombe, rapporteur. Chacun d'entre vous dispose à présent de deux minutes pour aborder un point qui n'aurait pas été évoqué et pour conclure.

M. Pierre Lelièvre. Je ne souhaite pas que le débat se cristallise sur la biométrie, qui est un moyen d'authentification présentant trois niveaux de sécurité, la puce correspondant probablement au plus élevé.

La question du niveau de maturité de la biométrie se pose, et pas seulement à l'échelle de la France. À l'heure actuelle, l'état de l'art montre que les algorithmes de biométrie ont environ une chance sur un million de confondre une personne avec une autre. De plus, la probabilité que le système échoue à identifier une personne donnée a été estimée à moins de 1 %. Le niveau de maturité de la technologie s'avère donc très bon.

Il convient désormais de nous demander comment nous souhaitons utiliser la biométrie dans le parcours client et dans notre vie de tous les jours en tant que citoyens, plutôt que de lutter contre elle. À condition de nous en donner les moyens, nous devons absolument nous équiper car nous sommes en train de perdre notre avance au profit d'autres acteurs.

M. Olivier Charlannes. M. Philippe Lelièvre a insisté à juste titre sur l'importance de pouvoir accéder aux données dans le développement des technologies d'Intelligence artificielle.

Il semble également judicieux, au niveau européen, de mettre en place un organisme d'évaluation de la performance de ces technologies, en opposition au *NIST (National Institute of Standards and Technology)*, l'organisme américain de référence. Pour l'instant, l'évaluation des différentes technologies est réalisée à l'aune de cet organisme. Ainsi, la mise en place d'un organisme comparable, au niveau européen, offrirait la possibilité à chaque État membre de s'y référer pour évaluer les technologies qui lui seront soumises, leur niveau de performance et la manière dont elles ont été développées. Cette mesure permettrait de disposer d'un vrai référentiel de comparaison au niveau européen, auquel les État membres pourraient avoir recours.

M. Philippe Latombe, rapporteur. Je prends ce point, afin d'étudier comment nous pourrions approfondir le sujet.

M. Cosimo Prete. La proposition de M. Olivier Charlannes peut être déclinée au niveau national. Nous pourrions ainsi nous doter d'une commission mixte composée d'experts de l'industrie et d'experts publics, afin de renforcer les ressources de l'ANTS dans le pilotage des programmes régaliens. Cette mesure permettrait de prendre de la hauteur par rapport au monopole d'État et de rationaliser les choix technologiques. Pour l'heure, ce monopole se trouve encore tiraillé entre source de profit et sécurité nationale.

Nous pourrions même envisager d'aller plus loin, avec la mise en place d'un *small patriot act,* afin de nous aider à bâtir une souveraineté nationale à l'échelle de l'Europe.

Il est toujours possible de mieux faire, mais qu'avons-nous fait de plus depuis la création en 2010 de la puce implémentée dans notre nouvelle CNIe ? Le pilote ne pourrait-il pas évoluer sans pour autant perturber les contraintes calendaires d'ici le mois d'août ?

Audition, ouverte à la presse, de Mme Valérie Péneau, inspectrice générale de l'administration, directrice du programme interministériel France Identité numérique (FIN), et de Mme Anne-Gaëlle Baudouin-Clerc, préfète, directrice de l'agence nationale des titres sécurisés (ANTS) *(1er avril 2021)*

Présidence de M. Philippe Latombe, rapporteur.

M. Philippe Latombe, président et rapporteur. Je remercie Mme Valérie Péneau, inspectrice générale de l'administration et directrice du programme interministériel France Identité numérique (FIN), ainsi que Mme Anne-Gaëlle Baudouin-Clerc, préfète et directrice générale de l'agence nationale des titres sécurisés (ANTS) d'avoir accepté de participer à nos travaux.

Notre échange portera principalement sur le projet d'identité numérique régalienne développé par l'État, qui est censé garantir à chaque Français une identification sécurisée sur les services publics et privés qu'il utilise dans sa vie quotidienne. Le numérique occupe une place croissante dans la vie de chacun, ce qui rend nécessaire la proposition d'une solution publique sécurisée de confiance, pour que les garanties apportées par l'État dans le monde réel se déclinent également dans la sphère numérique.

Je me réjouis donc que nous puissions dresser ensemble un état des lieux de l'avancement de ce projet, ainsi qu'évoquer la nécessité de maximiser le recours à des technologies souveraines dans ce cadre.

Je souhaiterais vous entendre sur trois points.

J'aimerais d'abord que vous nous présentiez un état des lieux de l'avancement du projet d'identité numérique porté par l'État. Ce projet est en effet important pour l'ensemble des citoyens, au regard de leur utilisation croissante des services numériques publics et privés. Le calendrier de déploiement de cette identité numérique, qui devait intervenir à l'occasion du lancement de la carte nationale d'identité électronique (CNIe), suscite actuellement des inquiétudes. Comment cette identité numérique régalienne peut-elle participer à la construction d'une forme de souveraineté numérique nationale ou européenne ? Comment nous positionnons-nous par rapport à nos principaux voisins européens ?

Mon second point porte sur le fonctionnement de cette identité numérique. Je souhaite que vous reveniez sur ses principes et que vous indiquiez comment cette identité numérique régalienne s'articulera avec FranceConnect. J'aimerais également vous entendre sur la façon dont cette solution sera sécurisée et sur les usages qu'elle offrira aux entreprises et aux citoyens. Nous pourrons ainsi échanger sur le modèle économique de l'identité numérique et donc sur l'articulation entre la puissance publique et les acteurs privés dans ce cadre.

Enfin, j'aimerais élargir notre échange à la gestion du pilotage des projets numériques au sein de l'État. Quels sont, selon vous, les prérequis méthodologiques indispensables pour mener à bien un projet numérique de cette nature ? Nous avons eu un échange avec M. Dominique Pon, responsable de la stratégie du numérique en santé, qui nous indiquait qu'il fallait privilégier l'approche par briques, sans tenter de tout révolutionner en même temps. J'aimerais donc savoir si vous partagez cette approche, par petits pas, de la numérisation de l'État et des administrations publiques. Je souhaite également connaître les principaux

obstacles qu'un gestionnaire de projet comme vous peut être amené à affronter dans l'exercice de ses fonctions.

Mme Valérie Péneau, inspectrice générale de l'administration, directrice du programme interministériel France Identité numérique (FIN). Nous sommes deux à nous adresser à vous, illustrant l'articulation et la complexité du projet d'identité numérique régalienne. Je m'occupe pour ma part de la partie relative aux systèmes d'information du moyen d'identification électronique que nous concevons. Celui-ci a pour particularité de s'articuler avec des documents sources, que sont les titres d'identité électroniques, en premier lieu la carte nationale d'identité électronique (CNIe) mais aussi les passeports et titres de séjour, portés par Mme Anne-Gaëlle Baudouin-Clerc.

Le programme France Identité numérique s'inscrit dans la même temporalité que les autres projets liés à l'identité numérique. Il s'agit de projets complexes, sur lesquels nos voisins ont souvent pris de l'avance, certains d'entre eux ayant déjà été notifiés à la Commission européenne. Je précise qu'il ne suffit pas de notifier un schéma à la Commission européenne, l'identité numérique doit ensuite être utilisée au quotidien.

La France a souhaité accélérer un processus qui avait connu plusieurs échecs par le passé, pour des raisons assez diverses. Cette nette accélération a été permise par le nouveau Règlement européen sur les cartes d'identité électroniques, les deux projets ayant été lancés de manière concomitante. L'articulation entre les deux a ainsi pu s'établir de façon native. Dès la conception de la carte d'identité, nous avons en effet été en mesure d'y inclure une approche technologique permettant d'intégrer une application à l'origine de l'identité numérique. Cette approche a pu être définie très rapidement avec les industriels. La distribution de la carte sera donc prochainement généralisée.

Nous ne disposons toutefois pas encore du système d'information permettant d'exploiter cette dimension de l'identité numérique, puisqu'un décalage de quelques mois est attendu. Celui-ci s'explique d'abord par la complexité du processus, notamment au niveau de la mise en place de l'expertise et des compétences nécessaires. Il s'explique également par le fait que nous avons déjà fait l'objet de recommandations de la part du conseil national du numérique et de la mission parlementaire ad hoc de Mme Christine Hennion et de M. Jean-Michel Mis, qui ont déjà expertisé le projet. Une consultation publique avait également eu lieu sur le sujet. Notre cahier des charges a ainsi été complété.

Au-delà des garanties fixées par le Règlement eIDAS (Electronic IDentification Authentication and trust Services) et des référentiels de l'agence nationale des systèmes d'information (ANSSI), nous avons intégré ce cahier des charges citoyen qui a été défini l'été dernier. Celui-ci nous a amené à revoir certains parcours envisagés, pour tendre vers une plus grande inclusion, nous conduisant à reformuler un certain nombre de process.

Dans le même temps, l'ANSSI s'est penchée sur le sujet, pour aboutir à un référentiel sur la vérification d'identité à distance, publié en mars dernier. Nous avons alors dû en tenir compte lors du lancement des marchés.

Cette période de travaux complémentaires nous a par ailleurs permis de « maquetter » un certain nombre de parcours. L'objectif était de nous doter d'un premier moyen d'identification électronique. Celui-ci ne correspondra toutefois pas au niveau de sécurité le plus élevé, en raison de la longueur du temps de qualification. D'ici la fin de l'année 2021, il permettra, en revanche, à l'usager, d'utiliser sa CNIe en interface avec une application. Il s'agira par la suite d'obtenir un moyen d'identification électronique qualifié au niveau eIDAS, le délai moyen d'instruction s'élevant en moyenne à quatre mois.

Ce décalage se retrouve dans les autres pays européens, où les cartes sont en générale distribuées dans un premier temps, avant d'être accompagnées d'une offre numérique. Quoi qu'il en soit, le projet a fait l'objet d'un cadrage très précis, qui le sécurise et nous permettra, dans les prochains mois, de répondre à la demande.

Mme Anne-Gaëlle Baudouin-Clerc, directrice de l'agence nationale des titres sécurisés. Le projet relatif à l'identité numérique est piloté et mis en œuvre par le programme interministériel FIN dirigé par Mme Valérie Péneau. De son côté, l'agence a lancé l'appel d'offres précédemment évoqué à l'été 2020. Elle joue également un rôle d'ordonnateur pour les dépenses engagées autour de ce projet.

En tant que porteurs responsables pour le compte du ministère, nous sommes en charge de la gestion de quatorze titres sécurisés, pour lesquels nous sommes responsables à la fois de la conception des systèmes, de l'acheminement des titres et du support usager. En effet, le développement des téléprocédures a fait émerger un fort besoin d'accompagnement.

La priorité pour 2021 concerne le déploiement progressif de la nouvelle CNIe. Depuis le 15 mars dernier, celle-ci est déployée dans le département de l'Oise. Depuis la semaine dernière, elle a également été lancée à la Réunion et en Seine-Maritime. Sous réserve du succès de ces différents pilotes, le déploiement de la carte sera par la suite étendu par vagues successives à l'échelle des régions, entre la mi-mai et le début du mois de juillet. Dans le même temps, le Règlement européen a prescrit à chaque État de se doter d'une nouvelle carte d'identité avec puce avant le 2 août. La France est ainsi en passe de rattraper son retard sur les autres pays de l'Union européenne.

En 2020, nous avons connu une diminution importante de la demande de titres, dans une proportion inédite en ce qui concerne les passeports et de 19 % pour la carte d'identité, malgré ses usages liés à la vie quotidienne. Le déploiement de la nouvelle carte d'identité dépend donc également des évolutions de la crise sanitaire. Nous anticipons désormais une forte augmentation de la demande, qui surviendra probablement au cours de la seconde partie de l'année 2021 et en 2022. Avant la crise, cette demande de cartes d'identité se trouvait en revanche en augmentation structurelle. Cette donnée devra être prise en compte lors de la mise en service opérationnelle de l'identité numérique.

M. Philippe Latombe, rapporteur. L'identité numérique s'appuiera dans un premier temps sur la CNIe, avec l'arrivée d'une interface d'ici un an. Les deux projets sont-ils liés et embarquent-ils tous les deux des caractéristiques évolutives, ou bien d'autres projets ont-ils été menés en parallèle ?

Mme Valérie Péneau. L'identité numérique existe déjà dans le cadre de FranceConnect, mais la proposition de valeur supplémentaire que nous sommes en train de construire concerne l'obtention d'une identité numérique très sécurisée. Pour y parvenir, l'enjeu est d'aboutir à la dématérialisation de nouveaux usages, ainsi qu'à la sécurisation d'un écosystème d'échange de données. L'idée est de s'appuyer sur les titres d'identité à l'aide d'une interface cryptographique faisant le lien entre les données d'identité protégées dans la puce du titre et une application.

Les deux projets sont intimement liés. Selon la définition figurant dans la loi pour une République numérique, un moyen d'identification électronique doit servir à transmettre des données d'identité. Ces données doivent provenir de quelque part. À la différence d'autres États, la France ne dispose d'aucun registre unique de population. Ce sont en effet nos titres d'identité qui font office de source d'identité. Notre moyen d'identification électronique tirera

donc ses données de ces titres. Un ensemble logiciel passera ensuite par le smartphone de l'intéressé, pour exporter et exploiter ces données d'identité.

Avant la CNIe, nos seules sources d'identité possibles se limitaient aux passeports et aux titres de séjour. Malgré leur diffusion à environ vingt-deux millions d'exemplaires, les passeports ne sont pas très inclusifs. La perspective de déploiement de la CNIe implique donc un changement de modèle.

Mettre au point une CNIe en deux ans constitue un exploit pour un pays aussi vaste que le nôtre. Quoi qu'il en soit, puisque les deux projets ont été lancés à la même date, ils ont été conçus en partenariat. À ce propos, le programme est logé sur la même plateforme que l'ANTS et bénéficie de moyens en partie fournis par cette dernière. Nous avons également travaillé ensemble à la définition des spécificités de la puce et poursuivons notre partenariat.

Une direction de programme a été mise en place, en raison du caractère particulier de l'identité numérique, impliquant notamment des interférences interministérielles. Le projet est donc totalement articulé avec l'agence. Ensemble, nous travaillons quotidiennement à la définition des spécificités de la carte et nous nous pencherons prochainement sur les parcours ainsi que le support utilisateurs.

M. Philippe Latombe, rapporteur. Nous venons d'auditionner la société IDEMIA ainsi qu'un industriel. Selon ce dernier, la CNIe ressemblerait fortement à un copier-coller du titre de séjour ou du permis de conduire. Or d'après ce que vous évoquez, ce support aura une importance majeure, puisqu'il embarquera la partie liée à l'identité électronique. S'agit-il réellement d'une copie ? Quelles sont les évolutions apportées ? Cette carte sera-t-elle à terme en capacité d'évoluer, en fonction des besoins qui pourraient survenir ?

Mme Anne-Gaëlle Baudouin-Clerc. Le fait d'avoir pu sortir cette CNIe en deux ans constitue une franche réussite. Cette carte respecte l'état de l'art de ce que nous pouvons attendre pour un titre sécurisé.

Le ministère de l'intérieur considère qu'il n'existe pas de sécurité unique mais plutôt un ensemble de sécurités incluses dans ce nouveau titre. Ce dernier constitue une protection supplémentaire pour lutter contre l'usurpation d'identité. Des sécurités physiques y ont donc été incluses, à un niveau qui n'avait jamais été atteint en la matière. Nous sommes donc très loin de la carte actuelle, qui a été élaborée en 1995. La carte se rapproche en revanche du titre de séjour dans sa dernière version, même si le niveau d'exigence en matière de sécurité a été renforcé.

L'apport majeur se situe dans l'introduction d'une puce contenant des données biométriques. Celle-ci contient à la fois les données prévues au titre du règlement de l'organisation de l'aviation civile internationale (OACI), conformément aux prescriptions communautaires, et l'identité numérique en tant que telle. L'application pourra ainsi être déverrouillée par un code PIN associé.

Quoi qu'il en soit, cette nouvelle carte n'aura rien à voir avec une simple copie des titres existants, en particulier le permis de conduire, qui ne comporte pas de puce. Ce dernier a d'ailleurs vocation à évoluer.

M. Philippe Latombe, rapporteur. La photo d'identité qui figurera sur le titre est en noir et blanc et provient d'une technologie américaine. Certains industriels français sont en capacité de fournir des photos en couleur. De plus, le cachet électronique visible (CEV) suivra la norme 101 et non 105, qui aurait pourtant permis des évolutions à terme.

Utilisons-nous les savoir-faire de nos industriels et les privilégions-nous dans la mise en place de ce titre ? En raison du caractère régalien du sujet, il serait en effet normal de recourir à des industriels français voire européens. Il en va également du rôle de l'État de soutenir sa filière, surtout lorsqu'il s'agit d'une filière d'excellence.

En raison de sa construction rapide, ce titre est-il en capacité d'évoluer à terme en fonction des nouveaux usages dont nous pourrions avoir besoin ?

Enfin, concernant la partie relative au titre physique, aucun appel d'offres n'aurait été lancé, en raison du monopole de l'Imprimerie nationale.

Mme Anne-Gaëlle Baudouin-Clerc. La loi garantie effectivement un monopole à l'Imprimerie nationale.

M. Philippe Latombe, rapporteur. Quel rapport entretenez-vous avec l'Imprimerie nationale sur ce sujet ? Est-ce vous qui définissez les besoins et l'Imprimerie nationale qui exécute ? Celle-ci dispose-t-elle d'une force de proposition vis-à-vis de vous ?

Mme Anne-Gaëlle Baudouin-Clerc. En la matière, l'État a fait en France un choix de souveraineté qui n'est pas unique au monde, même si d'autres modèles existent.

Une convention a été conclue entre l'agence et l'Imprimerie nationale. Cette convention détermine les objectifs que nous lui fixons en matière de sécurité, ainsi que les conditions tarifaires, les objectifs de production, les conditions de déploiement et le choix des industriels.

Nous avons fixé des objectifs de sécurité à l'Imprimerie nationale, en nous basant sur notre connaissance des phénomènes de fraude et à partir d'un dialogue avec les forces de sécurité intérieures. L'une de nos préoccupations était bien de nous laisser des possibilités d'évolution dans le temps, afin de pouvoir nous adapter aux nouvelles attentes.

En revanche, l'agence ne choisit ni les prestataires, ni les sous-traitants, ni les fournisseurs de l'Imprimerie nationale, qui doit faire ses propres choix en tant qu'industriel. Nous fixons simplement des objectifs et nous assurons qu'ils sont atteints. Pour sa part, l'Imprimerie nationale recourt de plus en plus à des appels d'offres concernant le choix de ses différents fournisseurs.

Le CEV constitue une innovation par rapport à la carte nationale d'identité actuelle. S'il est vrai que la norme 105 présente l'immense avantage d'offrir l'interopérabilité, elle a en revanche l'inconvénient d'être, pour l'instant, relativement mal reconnue par les différents lecteurs. La norme 101 s'avère ainsi nettement plus accessible et inclusive. C'est pour cette raison que nous l'avons privilégiée. Nous sommes toutefois conscients que nous aurons à un moment ou l'autre de bonnes raisons de la faire évoluer, même s'il est encore trop tôt pour se prononcer sur les conditions ou le calendrier. Il ne s'agit en tout cas pas d'un choix du passé mais plutôt d'une priorité donnée à l'inclusion et à l'accessibilité, en particulier sur le territoire national, qui concentre la majorité des usages de la carte.

Certains États ont opté pour des cartes d'identité avec des photos en couleur, d'autres non. Le noir et blanc présente en tout cas des avantages en matière de lutte contre la fraude. Ce choix est donc assumé et ne traduit en aucun cas un manque de maîtrise du système.

M. Philippe Latombe, rapporteur. Je me tournerai vers l'Imprimerie nationale pour comprendre pourquoi elle a fait appel à une technologie américaine, alors qu'il aurait été possible de faire aussi bien avec des prestataires français.

S'agissant de la CNIe, je n'ai toujours pas compris pourquoi l'Imprimerie nationale n'a lancé aucun appel d'offres.

Mme Anne-Gaëlle Baudouin-Clerc. Environ 70 % des composants de la carte ont donné lieu à des appels d'offres. Je pourrai vous confirmer le chiffre exact.

Le régime juridique de l'Imprimerie nationale l'autorise à déroger à certaines règles de la commande publique. L'État actionnaire souhaite toutefois voir augmenter la part de l'activité sous monopole donnant lieu à des appels d'offres.

M. Philippe Latombe, rapporteur. C'est donc bien l'ANTS qui a délibérément choisi de produire le cachet électronique selon la norme 101 et non 105, ou encore d'opter pour la photo en noir et blanc ?

Mme Anne-Gaëlle Baudouin-Clerc. Nous prenons en compte certaines contraintes industrielles, mais ces deux aspects ont fait l'objet d'un choix assumé. J'ai toutefois conscience que, pour l'Imprimerie nationale, le passage à la norme 105 aura des conséquences industrielles, notamment de modification de sa plateforme. À titre personnel, je pense en tout cas que la situation a vocation à évoluer. Ainsi, parvenir à utiliser la norme 105 pour le pass sanitaire présentera un véritable intérêt. Enfin, la norme 105 a besoin de conforter sa gouvernance, ainsi que de clarifier ses conditions de sécurité et de souveraineté.

M. Philippe Latombe, rapporteur. L'ANTS fait face à une forme de contraction de son personnel, entraînant une perte de compétences dans ce domaine. Êtes-vous à la recherche d'un chef de projet au sujet de la CNIe ? Vous trouvez-vous réellement sous pression en matière de personnel ? Disposez-vous de la capacité à attirer des talents présentant un profil d'ingénieur, afin d'être en mesure de pratiquer des activités telles que le sourcing ?

Mme Anne-Gaëlle Baudouin-Clerc. Le plafond d'emploi de l'agence a été revalorisé cette année de six ETP, afin de répondre aux enjeux auxquels nous sommes confrontés. Nous rencontrons des difficultés de recrutement, mais pas plus que la plupart des services de l'État. À ce sujet, nous nous sommes engagés dans une démarche de type « marque employeur », afin de mieux recruter et mieux conserver nos talents, pour pallier le fort turnover que connaît l'agence. S'il est vrai que notre cheffe de projet CNIe a annoncé qu'elle souhaitait partir, ce départ ne remet pas en cause la capacité de l'agence à mener à bien ses projets.

D'aucuns ont pointé du doigt le déséquilibre existant entre l'agence, qui compte environ cent quarante collaborateurs (hors support usagers) et l'Imprimerie nationale qui demeure l'un de nos interlocuteurs majeurs. Il est de notre responsabilité de structurer le dialogue entre ces deux entités, en gardant à l'esprit que l'agence est soutenue par le ministère de l'intérieur, lui permettant de mobiliser l'expertise disponible en matière de fraude sur les titres. L'agence ne doit donc pas être réduite à ses effectifs stricto sensu.

M. Philippe Latombe, rapporteur. Il existe deux types d'attractivité, celle liée à la « marque employeur » et celle liée à la rémunération. Avez-vous la capacité d'attirer des ingénieurs ou des profils techniques figurant parmi les meilleurs dans leur domaine ?

Existe-t-il à ce jour en France, dans la sphère publique, des talents spécialisés sur l'identité numérique, ou sont-ils massivement partis chez les industriels ?

Mme Anne-Gaëlle Baudouin-Clerc. La rémunération constitue un sujet sérieux. Nous sommes engagés dans des référentiels, en termes de compétences, dans le secteur du numérique, ce qui nous permet d'être plus proches des données du marché. Sur ce point, j'accorde une grande importance à tout ce qui a trait à la cybersécurité. Au sein de l'agence, nous sommes très clairement sous-dimensionnés pour ces questions. Le référentiel se trouve ainsi en décalage avec le marché.

En quelques mois, nous avons constaté une diminution du nombre de candidatures, bien que nous recourions à un chasseur de têtes pour notre recrutement. Sur un type de poste donné, nous avons reçu trois candidatures cette année, contre une trentaine l'année dernière. Cette tendance n'est pas liée à la « marque employeur », mais à la rémunération et à l'assèchement du marché, puisque tout le monde recrute en même temps. Ce sujet nous handicape fortement.

Mme Valérie Péneau. Sur la partie relative aux systèmes d'information, nous avons lancé un appel d'offres. L'offre française s'avère de qualité sur les différents lots que nous avons publiés.

La future carte d'identité sera dotée d'une puce embarquant une application d'identité numérique. Nous avons travaillé avec les industriels français pour définir les spécificités de cette puce. L'enjeu était de déterminer collectivement la technologie pouvant se retrouver de la façon la plus interopérable possible sur le marché déjà existant. Nous devions également réfléchir aux éléments qui pourraient évoluer de la façon la plus pertinente. Pour respecter le délai de deux ans, une première cible a alors été définie. Celle-ci est actuellement mise en place dans la carte.

Dans le contrat de filière signé en janvier 2020, nous travaillons avec les industriels français à la définition de la cible de la « puce V2 » de la future CNIe. Nous projetons ainsi de définir les spécifications avant la fin de l'année, avant de passer à la mise en œuvre technique, puis à la qualification par l'ANSSI. Au final, l'objectif est de sortir la deuxième génération de la CNIe d'ici 2024.

La future application d'identité numérique intégrée pratiquera nativement la divulgation sélective d'attributs, alors que cette dernière nécessite pour l'instant d'être opérée séparément. L'application pourrait également traiter la question des pseudonymes. Tous ces sujets font l'objet d'un travail partenarial avec les industriels français. Nous souhaitons en effet que l'identité numérique régalienne repose sur des technologies françaises. Les industriels ont par ailleurs vocation à porter à l'étranger ces technologies et approches nationales.

Le recrutement s'avère effectivement compliqué, d'autant que l'identité numérique requiert des compétences extrêmement pointues, dont le marché n'abonde pas. J'ai toutefois la chance de disposer d'une équipe de grande qualité, qui s'est constituée au fur et à mesure. Celle-ci se compose à la fois de fonctionnaires et de contractuels, que l'agence nous a aidés à recruter. Les membres de mon équipe restent quant à eux en poste par passion pour le projet, car il est vrai qu'assez peu d'entre eux ont déjà eu l'occasion de travailler sur une future application grand public touchant à l'identité et au régalien. Ces personnes sont donc passionnées par le projet et ne nous restent pas fidèles pour des questions de rémunération.

Le référentiel ne semble plus du tout à la hauteur des enjeux ni de nos besoins. Ainsi, si nous souhaitons conserver une capacité de pilotage et de maîtrise des prestataires, nous devons disposer des compétences adéquates, ce qui représente un combat quotidien.

M. Philippe Latombe, rapporteur. Nous avons auditionné des membres des GAFAM (Google, Apple, Facebook, Amazon, Microsoft), qui disposent d'une assez puissante capacité de lobbying. Il leur arrive ainsi de payer le prix fort pour recruter des talents et ensuite les utiliser dans un cadre commercial. Ces personnes qui ont quitté vos équipes pour rejoindre les industriels, les retrouvez-vous sur le projet ?

Mme Valérie Péneau. S'agissant de mon projet, nous nous trouvons en phase de recrutement. Une personne risque certes de nous quitter mais elle part rejoindre une autre agence de l'État et non un GAFAM. Il peut donc parfois exister de la compétition en interne, même si nous ne pouvons pas nous opposer aux évolutions de carrière. Quoi qu'il en soit, mon équipe n'a subi aucun détournement d'expertise au profit des GAFAM, même si sa taille reste réduite.

M. Philippe Latombe, rapporteur. En évoquant les GAFAM, je pensais également à d'autres industriels spécialisés sur le sujet.

Mme Valérie Péneau. Le programme a au contraire attiré des experts en provenance d'industriels. Deux d'entre eux nous ont ainsi rejoints car le projet les passionnait.

M. Philippe Latombe, rapporteur. S'agit-il plutôt de contractuels ?

Mme Valérie Péneau. Mon équipe se compose d'une majorité de contractuels, ainsi que de deux fonctionnaires.

Mme Anne-Gaëlle Baudouin-Clerc. Nous recrutons très largement des contractuels, dont un grand nombre provient du monde industriel. Une certaine concurrence peut également exister entre les différents ministères.

M. Philippe Latombe, rapporteur. L'année dernière, les députés ont adopté une loi interdisant l'accès aux sites pornographiques aux mineurs. Le CSA demande donc que des preuves de majorité soient données pour accéder à ces sites. La même question pourrait se poser pour la vente d'alcool ou de produits interdits aux mineurs. Or pour l'heure, nous ne disposons pas d'une identité numérique. Cette dernière n'arrive-t-elle donc pas un peu tard ? Embarquera-t-elle tous les usages possibles et imaginables dont l'invention humaine pourrait à terme avoir besoin ? En d'autres termes, disposez-vous d'une capacité d'évolution rapide ? Comment pourra-t-on ainsi justifier son âge sur internet ? L'identité numérique offrira-t-elle la possibilité de voter à distance d'ici cinq ou dix ans ? Certains pays comme l'Estonie ont déjà intégré cette fonction.

Mme Valérie Péneau. L'identité numérique transmet uniquement des données, dans le but de prouver une identité. La divulgation sélective des attributs est effectivement envisageable, en particulier l'âge. En attendant, nous devrons d'abord être en capacité de délivrer une première application, avant de la faire évoluer par la suite.

Grâce à la composante logicielle, il est tout à fait envisageable de faire évoluer le projet afin de l'adapter aux différents usages, à condition de disposer d'un cadre juridique et d'un haut niveau de sécurité. Rien ne s'opposera alors à ce que l'identité numérique soit interfacée avec un système de votation. Un tel système est d'ailleurs prévu concernant les élections professionnelles ainsi que le vote des Français de l'étranger. Je pense que le Conseil constitutionnel devra toutefois se prononcer sur cette évolution.

Le sujet des mineurs présente une complexité, tant sur le plan technique que juridique. Il existe par exemple des âges de majorité différents selon les sujets. La loi pour une

République numérique a ainsi fixé à quinze ans la majorité numérique pour les services issus de la société de l'information mais pas pour les services publics. D'autres textes plus récents font état d'âges évolutifs. Sur la partie pénale également, l'âge présente un caractère variable. Il est donc difficile de construire des parcours totalement évolutifs avec l'âge.

Tant que le mineur est considéré comme tel pour une activité donnée, ce dernier doit obtenir le consentement du détenteur de l'autorité parentale. La création et l'usage de l'identité numérique d'un mineur ne pourront pas échapper à cette règle. Une telle mesure n'est pourtant pas facile à implémenter sur le plan technique, car il est nécessaire de recueillir à la fois l'identité numérique des détenteurs de l'autorité parentale et celle des mineurs. Nous finirons par y parvenir mais la première offre sera d'abord dédiée aux majeurs.

Si nous parvenons à passer le cap de la création d'identité numérique au bénéfice de mineurs, le fournisseur de service sera informé de façon sécurisée concernant l'âge de son utilisateur. Cette mesure est possible sur le principe et tout reste envisageable concernant les usages, même si certaines difficultés juridiques et techniques doivent être résolues. Les perspectives s'annoncent ainsi considérables et la cadence devra s'accélérer, afin d'articuler cette première identité sécurisée avec les titres d'identité.

Mme Anne-Gaëlle Baudouin-Clerc. Au sujet de la preuve de majorité, nous sommes en train d'étudier la possibilité d'utiliser le CEV sans attendre la mise en place de l'identité numérique. Cette solution éviterait ainsi de devoir montrer l'ensemble de sa carte. La question fait en tout cas l'objet d'un travail approfondi.

M. Philippe Latombe, rapporteur. L'ANTS se situe en dehors du ministère, ce qui ne l'empêche pas d'entretenir de forts liens avec celui-ci. Cette agence fonctionne en mode projet complet sur la question de l'identité numérique. Êtes-vous le seul organisme à fonctionner de la sorte au sein de l'État ? Ce mode de fonctionnement apparaît nouveau. Vous apporte-t-il un vrai plus pour faire avancer le projet le plus vite possible et ne pas répéter les erreurs du passé ?

Mme Valérie Péneau. Je ne sais pas si beaucoup d'autres projets sont managés de cette façon au sein de l'État, car je n'ai pas réalisé de benchmark en la matière.

Mon expérience en tant qu'inspectrice générale de l'administration m'a appris que lorsqu'un système d'information dysfonctionne, une task force est créée pour tenter de rattraper le retard. Un mode industriel classique est alors abandonné, pour concentrer des expertises et adopter un mode opératoire permettant de réactiver un projet et d'enclencher une accélération.

En l'espèce, la task force a été constituée en amont du projet, avec un rassemblement d'expertises en provenance à la fois de l'ANTS et du ministère de l'intérieur. Ces forces ont été placées sous mon autorité fonctionnelle. Ce mode de fonctionnement est particulièrement adapté à un projet numérique, rapprochant de façon très nette la maîtrise d'ouvrage et la maîtrise d'œuvre.

La difficulté du projet réside dans la complexité technique du sujet, avec tous les aléas y étant associés. Il existe également une forte interférence avec d'autres acteurs, notamment FranceConnect, qui demeure l'écosystème dans lequel nous nous insérons. Les usages sont quant à eux en cours de définition et concernent l'ensemble des sphères publique et privée. Ainsi, ce rapprochement très étroit entre maîtrise d'ouvrage et maîtrise d'œuvre permet, selon un calendrier beaucoup plus restreint, d'accélérer le projet ainsi que la traduction concrète des fonctionnalités attendues.

L'accomplissement de notre mission n'est pas simple, car elle implique des interactions continues avec l'ensemble des parties prenantes du projet, au sein de ministère de l'intérieur comme de l'écosystème interministériel. La direction de programme est ainsi chargée du bon fonctionnement du projet.

Nous disposons également d'un comité de pilotage interministériel regroupant l'ensemble des ministères concernés, ainsi que la direction générale des entreprises (DGE), la direction interministérielle de la transformation publique (DITP) et l'ANSSI. La direction de programme parvient ainsi à fédérer l'ensemble des intérêts et des parties prenantes au projet. Dans le même temps, elle essaie de limiter au maximum le risque lié à la conduite d'un projet technique, pour lequel le calendrier est très tendu et les attentes sont extrêmement fortes. Au final, tous ces éléments justifient une telle organisation, au moins pendant quelque temps.

La direction de programme n'a toutefois pas vocation à perdurer. Par conséquent, une fois que le projet aura été stabilisé, il retrouvera probablement une gestion, une gouvernance et une organisation nettement plus classiques. Le mode de fonctionnement actuel correspond en effet à un temps politique et technique très particulier.

M. Philippe Latombe, rapporteur. Selon vous, où sera logé le programme une fois que le projet sera achevé ?

Mme Valérie Péneau. Il s'agit d'une excellente question à laquelle je ne peux pas apporter de réponse. En raison des liens très forts existant avec les titres d'identité, je suis en tout cas persuadée que la relation avec le ministère et avec son opérateur perdurera.

Ce moyen d'identification étant destiné à prendre place dans un écosystème interministériel, je pense qu'une gouvernance adaptée est amenée à durer pendant un certain temps. À ce titre, cet objet ne peut demeurer uniquement l'apanage du ministère de l'intérieur, même si j'estime, à titre personnel, que nous sommes en train de construire un service public. Étant donné que nous aidons les citoyens à prouver leur identité dans le monde physique, nous devons également leur offrir un moyen de faire de même dans le monde numérique, qui est devenu le lieu où se déroulent la majorité des interactions.

Selon moi, ce service public a plutôt vocation à être placé du côté du ministère de l'intérieur. Pour les usages quotidiens, toutefois, nous devrons conserver cette gouvernance interministérielle. Quoi qu'il en soit, la question devra se poser à l'avenir.

M. Philippe Latombe, rapporteur. Je souhaite à présent que nous abordions la question du marché de l'identité numérique.

Mme Valérie Péneau. J'émets certaines réserves concernant l'expression « marché de l'identité numérique », car il convient de différencier plusieurs éléments.

En premier lieu, l'État a la responsabilité de protéger les données d'identité de ses citoyens, en lien avec ses missions régaliennes ou relatives à la souveraineté. Ce point se rapporte à ses responsabilités en matière d'état civil et ce depuis la Révolution française.

En parallèle, l'État se doit également de sécuriser l'accès à ses propres services publics, ces éléments entrant dans la sphère des prérogatives de la puissance publique. En ce qui me concerne, je pense que l'accès aux services publics et l'identité numérique permettant d'y accéder sont liés à la notion de service public.

La question de l'accès aux services privés se pose ensuite. Dans ce cadre, les informations revêtent une véritable valeur, que les banques monétisent dans le cadre des KYC (know your customer). Ces éléments relèvent sans doute de données de marché.

Pour autant, il me semble qu'il n'est pas encore possible d'affirmer qu'il existe un marché de l'identité numérique, car sa maturité est encore en construction. Nous avons à ce propos mené des études avec des cabinets de consultants, pour tenter de préciser le modèle économique de ce marché de l'identité numérique. Une étude d'Ernst and Young sur le sujet a ainsi été transmise à la mission parlementaire. Cette étude fait état d'un potentiel de développement économique mais dans des proportions encore limitées.

À partir du moment où l'identité numérique en tant que telle repose sur des titres d'identité, c'est-à-dire la constitution d'un moyen d'identification électronique, celle-ci n'apparaît pas comme une source de marché évidente.

Plusieurs dispositifs existent en France. Notre environnement correspond par exemple aux moyens d'identification électroniques dans le cas d'une identité numérique reliée à FranceConnect. En parallèle, le nouveau référentiel d'exigences applicables aux prestations de vérification d'identité à distance (PVID) de l'ANSSI définit des modalités de vérification d'identité à distance. Celui-ci s'adresse aux acteurs de confiance, sera bientôt « embarqué » par les banques et correspond au marché de la vérification d'identité. Ce dernier est amené à croître, notamment au bénéfice des banques. Quant à elles, les banques se trouvent à cheval entre, d'un côté, des acteurs tiers pour vérifier à distance l'identité de leurs usagers et, de l'autre, l'écosystème FranceConnect, auquel la plupart d'entre elles sont déjà rattachées. La mise en place d'une identité numérique sécurisée pourrait donc les intéresser.

À ma connaissance, l'écosystème FranceConnect n'a pas encore complètement été stabilisé. Le principe défini suppose en tout cas que toutes les identités numériques permettant d'accéder à des services publics soient gratuites. En revanche, l'accès aux services privés connectés à FranceConnect obéit à une forme de marché. Sur ce point, il me semble que les fournisseurs d'identité privée, qui demeurent peu nombreux, pourront librement fixer leurs tarifs. Le sujet de la gratuité du moyen d'identification électronique régalien au bénéfice des acteurs privés n'a en revanche pas encore été tranché.

Les situations varient sensiblement d'un État à l'autre. Au sein du modèle anglais, par exemple, il a été constaté que le marché était insuffisant pour permettre à des acteurs privés de vivre correctement. D'autres modèles s'orientent plutôt vers une forme de partenariat public-privé, avec des redevances ou des indemnisations croisées n'atteignant pas des sommes considérables. Le seul modèle véritablement éprouvé demeure le scandinave, selon lequel les banques produisent nativement l'identité numérique. Ce modèle diffère du nôtre.

En matière d'identité numérique, la légitimité de l'État s'avère donc plus ou moins importante en fonction des cultures. Celle-ci demeure globalement assez forte, comme c'est notamment le cas en Suisse. Cette tendance a également été mise en évidence par le rapport de la mission parlementaire, qui fait état d'une certaine confiance de la part des citoyens envers l'État pour fournir cette brique d'authentification appuyée sur les titres d'identité dans le monde numérique.

Ce sujet fait l'objet d'interrogations depuis trois ans. Peu d'acteurs privés existent dans FranceConnect, peut-être parce que le modèle économique n'est pas encore complètement défini. Toujours est-il que l'identité numérique implique de lourds investissements, alors même que, dans le modèle actuel, le retour sur investissement n'est pas complètement garanti.

M. Philippe Latombe, rapporteur. Vous avez indiqué que les citoyens considèrent que l'État est le plus à même de s'occuper des questions relatives au domaine de l'identité. Percevez-vous toutefois une réticence de la part de certains citoyens français à confier leurs éléments biométriques à l'État dans l'optique que celui-ci les intègre dans un titre d'identité, qui ferait ensuite office d'identité numérique ? Comment évolue la situation sur ce point ?

Mme Valérie Péneau. Il est vrai qu'il peut parfois exister des contradictions chez nos concitoyens. Ainsi, alors même que les sondages font état d'une plus grande confiance dans l'État que dans les acteurs privés ou commerciaux pour garantir les données d'identité, des réticences apparaissent chez une partie de la population à propos de la transmission de ses données biométriques.

Pour rappel, dans le système Alicem, les données biométriques ne servaient qu'à vérifier l'identité au moment de la création de l'identité numérique et n'étaient par la suite jamais redemandées. Ce principe a pourtant suscité certaines confusions.

À ce stade, il est possible de pratiquer l'identité numérique sans recourir à la biométrie. Des parcours permettent ainsi de créer l'identité numérique et de la faire vivre par la suite, sans pour autant recourir à la vérification d'identité à distance et donc à la biométrie. En effet, cette dernière s'apparente à la comparaison entre une vidéo ou un selfie pris par la personne et la puce se trouvant dans le titre.

La carte d'identité actuelle intègre nativement les données biométriques de l'usager. Cependant, la partie de la puce en charge de la création de l'identité numérique ne contient pas de données biométriques, seulement des données alphanumériques.

Mme Anne-Gaëlle Baudouin-Clerc. Les données biométriques sont spécifiquement protégées en tant que telles. Nous nous sommes d'ailleurs assurés de l'effectivité de cette protection à travers un audit de sécurité ayant été conduit avant le lancement de la carte. De plus, l'accès à ces données demeure par principe réservé aux autorités publiques.

M. Philippe Latombe, rapporteur. Une partie de nos concitoyens craint la mise en place conjointe d'une CNIe contenant des données biométriques et d'une identité numérique, le tout couplé à du fichage et éventuellement à de la reconnaissance faciale. Sentez-vous cette crainte monter, à l'image de l'opposition à la 5G ? Les usages pourront-ils montrer que ces craintes sont infondées et ainsi remporter l'adhésion de la population ? Comment appréhendez-vous le lancement de l'identité numérique ?

Mme Valérie Péneau. Depuis le début, nous sentons effectivement qu'un travail de conviction et de pédagogie sera nécessaire.

L'application Alicem nous a permis de monter en maturité de façon considérable. L'un de ses intérêts a notamment été de pouvoir immédiatement constater les réactions qu'elle a suscitées. Nous avons également pu nous rendre compte des limites du modèle de cette identité numérique, qui avait initialement été conçue comme un prototype. Cette approche initiale était en tout cas parfaitement justifiée par l'objectif de l'époque.

En définitive, projeter un objet nativement conçu dans un but de vérification d'identité à distance (donc autour de la reconnaissance faciale) et dont seule la sécurité est valorisée n'apparaît pas être la meilleure porte d'entrée vers l'identité numérique sécurisée.

De plus, il existe une très forte confusion concernant les usages de la technologie faciale. Cette confusion se situe entre l'usage à des fins d'identification dans l'espace public

pour des raisons sécuritaires et l'usage dans un but d'authentification, qui n'ont rien à voir entre eux. En effet, l'authentification reste à la main de l'usager et se base uniquement sur le titre plutôt que sur un fichier central. La commission nationale de l'informatique et des libertés (CNIL) a clairement affirmé cette distinction mais la subtilité demeure mal comprise.

Par conséquent, nous pensons qu'il est préférable de commencer par offrir des parcours n'obligeant pas les utilisateurs à recourir à cette technologie, qui suscite certaines inquiétudes. En parallèle, il serait intéressant de ne pas immédiatement recourir à l'authentification renforcée pour certains usages du quotidien comme la preuve de la majorité dans le monde physique, avant d'entrer dans l'identité numérique sécurisée.

L'État doit également adopter une approche un peu différente. Nous avons ainsi demandé à nos prestataires d'utiliser des briques open source, dans un souci de transparence. À l'inverse, Alicem était protégée par des licences. Nous avons donc souhaité adopter une approche plus progressive et plus itérative. Dans cette optique, nous avons recruté des UX designers afin de recueillir régulièrement les retours des utilisateurs.

À l'avenir, ce seront les usages qui porteront l'identité numérique. Ceux-ci demeurent encore relativement peu nombreux, puisque la solution n'est pour le moment pas disponible. Lors de sa sortie, j'espère qu'elle ne fera pas l'objet d'un rejet, par exemple parce que la technologie serait mal supportée ou en raison de l'existence de présupposés sur un éventuel traçage. Or un tel traçage n'est pas du tout prévu et il ne serait de toute façon pas possible. Le but est au contraire que la solution soit largement déployée dès que les usages seront prêts.

M. Philippe Latombe, rapporteur. La souveraineté technologique, française ou européenne, constitue-t-elle l'un des moteurs de votre projet ? Allez-vous totalement l'intégrer dans le projet, quitte à exclure des solutions américaines qui pourraient poser question ?

Mme Valérie Péneau. Ma réponse est très clairement positive. En effet, lors de la formulation du cahier des charges de notre système d'information, nous avons veillé à ce qu'aucune licence ne devienne la propriété d'acteurs privés français ou européens.

Dans ce cahier des charges, nous avons également intégré l'application native du Règlement général sur la protection des données (RGPD), auquel sont soumis l'ensemble des acteurs européens et français.

Avec les acteurs français, nous définissons les spécificités de la puce de demain. La souveraineté fait ainsi partie intégrante du projet. Je pense d'ailleurs que la souveraineté numérique est un sujet éminemment régalien et même national. En effet, les schémas notifiés par les États correspondent à des pratiques administratives qui leur sont propres, selon qu'ils disposent ou non de registres de population ou d'identifiants uniques. Au final, chaque schéma est d'ordre national, même s'ils se doivent d'être interopérables au niveau européen.

Lors du discours de l'Union, la présidente de la Commission européenne a soumis l'idée d'une identité européenne, qui a ainsi été intégrée aux discussions de révision du règlement eIDAS. Cette idée suscite de fortes interrogations, car nous ne disposons d'aucune définition précise de ce que représenterait cette identité européenne au-delà de l'interopérabilité de nos dispositifs. La Commission devra donc expliciter ce point, alors que la révision du règlement eIDAS a été reportée. Quoi qu'il en soit, cette question fera l'objet d'importants travaux dans les prochains mois, peut-être au moment de la présidence française. L'un des enjeux sera de définir l'articulation avec les schémas nationaux, ainsi que d'aborder le sujet de la souveraineté nationale.

M. Philippe Latombe, rapporteur. La souveraineté technologique figure-t-elle parmi les critères principaux de l'ANTS ? Plutôt que de recourir à une technologie américaine proposant une photo en noir et blanc, ne pourriez-vous pas inclure d'autres solutions au cahier des charges que vous tenez avec l'Imprimerie nationale ?

Mme Anne-Gaëlle Baudouin-Clerc. Nos projets doivent apporter les garanties en matière de sécurité informatique et être en conformité avec le cadre français et européen. J'ai conscience que nous devons encore globalement progresser dans leur conduite, ainsi que sur les questions de propriété numérique au sens large, qui ne figurent pas encore au centre de nos préoccupations. Des évolutions devront donc être intégrées.

M. Philippe Latombe, rapporteur. De manière générale, les industriels préfèrent que l'État soit leur client plutôt que de recevoir des aides de sa part.

Audition commune, ouverte à la presse, de MM. Rodolphe Belmer, directeur général d'Eutelsat, et Hervé Derrey, président-directeur général de Thales Alenia Space*)*
(6 avril 2021)

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. Je remercie M. Rodolphe Belmer, directeur général d'Eutelsat, qu'accompagne M. David Bertolotti, directeur des affaires publiques de cette société, et M. Hervé Derrey, président-directeur général de Thales Alenia Space, d'avoir accepté de participer à nos travaux.

L'espace extra-atmosphérique donne lieu à des confrontations croissantes. Deux phénomènes principaux s'y révèlent à l'œuvre.

Il s'agit d'abord d'une tendance à la privatisation. Dans ce qu'il est convenu d'appeler le *new space*, elle se traduit par l'irruption d'acteurs privés innovants, tel SpaceX. Ils remettent en cause les fondamentaux de certains marchés, comme celui du lancement de satellites, et se positionnent en matière de connectivité par satellite.

Les grandes puissances étatiques inclinent ensuite à accaparer l'espace. Face aux initiatives des États-Unis et de la Chine, l'Europe entend se doter de sa propre constellation de satellites. Le commissaire européen au marché intérieur, M. Thierry Breton, le rappelait encore récemment.

Thales Alenia Space, entreprise notamment spécialisée dans la construction de satellites, et Eutelsat, opérateur de satellites commerciaux, sont parties prenantes de l'action de l'Europe. Le satellite de télécommunications géostationnaire Eutelsat Konnect, opérationnel en orbite depuis novembre 2020, illustre cette action.

M. Philippe Latombe, rapporteur. J'évoquerai trois sujets sur lesquels nous souhaiterions vous entendre.

D'une part, nous apprécierions que vous présentiez votre secteur d'activité, en proie à de profonds bouleversements. Apparus depuis plusieurs années, ceux-ci se manifestent désormais avec prégnance. Ainsi que le rappelait M. le président, les grandes puissances investissent toujours davantage l'espace extra-atmosphérique, quand les acteurs privés y font irruption, d'une façon inédite par son ampleur. Comment la France et l'Europe peuvent-elles ici défendre leurs intérêts et leur souveraineté ? Voulez-vous nous exposer brièvement le projet de constellation européenne, que porte M. le commissaire Thierry Breton et que M. le président évoquait dans son introduction ?

D'autre part, nous aimerions approfondir les enjeux d'innovation, voire de rupture technologique, qui animent votre secteur d'activité. Comment, en particulier, jugez-vous le niveau de soutien aux entreprises spatiales en France et en Europe, tant de la part des pouvoirs publics qui en subventionnent l'effort de recherche, que du marché qui doit permettre aux entreprises innovantes de se financer ? Formulez-vous des propositions en vue de mieux appuyer le développement de ces entreprises ? Nous aimerions également savoir s'il existe d'autres segments technologiques où des ruptures majeures devraient intervenir dans les prochaines années. Le cas échéant, comment faut-il que nous nous y préparions ?

Enfin, au cœur de la réflexion de la mission d'information, nous ouvrons une séquence sur la formation. Pourriez-vous nous dire quelle est votre évaluation des formations aux métiers du spatial en France et en Europe ? Avez-vous connaissance de pratiques ou de dispositifs dont nous tirerions avantage à nous inspirer ?

M. Rodolphe Belmer, directeur général d'Eutelsat. Eutelsat est un opérateur de télécommunications par satellites. Notre métier consiste à apporter des services de télécommunications dans le monde entier, là où les opérateurs terrestres éprouvent des difficultés à offrir les leurs. Il peut s'agit de zones géographiques à très faible densité de population – zones dites de déserts numériques –, ou de zones inaccessibles par nature aux télécommunications terrestres, tels que l'espace aérien pour les avions en vol ou la pleine mer pour les navires.

Quoique peu connue du grand public, la société Eutelsat représente, avec près d'1,3 milliard d'euros de chiffre d'affaires, le troisième opérateur mondial de son secteur. Elle compte 1 200 employés. Modeste en comparaison de son chiffre d'affaires, son effectif atteste de la forte valeur ajoutée de son activité. Plus que le nombre, celle-ci requiert une ressource extrêmement qualifiée et spécialisée. J'y reviendrai au sujet de la formation que vous avez abordée dans vos questions.

En outre, l'organisation d'Eutelsat s'avère des plus ouvertes à l'internationalisation. Plus de cinquante nationalités la composent. Son siège se situe en France, à Issy-les-Moulineaux, où il vient de s'installer. Son principal téléport, ou lieu de réception des signaux produits par sa flotte de satellites, se trouve à Rambouillet, en région parisienne.

À ce jour, Eutelsat exploite une quarantaine de satellites dits géostationnaires. De taille importante, d'un poids de cinq à six tonnes en moyenne, ces satellites évoluent à 36 000 km d'altitude, en orbite autour de la Terre, selon une vitesse de rotation qui lui est identique. Ils demeurent donc à une position fixe par rapport à la surface du sol. Une telle fixité facilite les services de télécommunication.

Eutelsat est présente dans 150 pays.

Historiquement, notre cœur de métier consiste en la diffusion de chaînes de télévision. Premier acteur mondial à égalité de cette activité vectrice d'information, de culture et de divertissement, nous distribuons 7 000 chaînes de télévision. Grâce aux satellites, environ un quart de la population mondiale les reçoit.

Depuis quelques années, notre activité prend un nouvel essor. Au-delà de la télévision, elle s'adresse de plus en plus au marché de la connectivité. Dorénavant, la promesse devient celle de l'Internet accessible en tous lieux, y compris là où les opérateurs terrestres ne peuvent, pour des raisons physiques ou économiques, le proposer.

En conséquence, nous avons engagé avec nos partenaires une stratégie d'innovation et d'investissement. Il s'agit de financer les infrastructures de télécommunications spatiales à mêmes de fournir des services Internet de haute qualité à un prix acceptable aux populations des zones où les opérateurs terrestres ne parviennent pas à se rendre.

Je reprendrai un exemple que vous avez cité dans votre introduction. Nous avons récemment mis en orbite le satellite Konnect. Notre partenaire Thales Alenia Space en a assuré la fabrication, Arianespace s'est occupée de son lancement. Il permet de proposer à nos concitoyens un service Internet performant, distribué par la société Orange, d'une capacité de connexion de 100 mégabits par seconde (Mb/s). Son prix mensuel de 39,90 euros équivaut

aux offres de télécommunications terrestres. De ce point de vue, une initiative de bout en bout française contribue à réduire la fracture numérique sur notre territoire. Rassemblée dans toute sa chaîne de valeur, l'industrie française a ici produit un service assurément innovant et utile.

Je répondrai maintenant à vos questions.

Sur les aspects de souveraineté, de perturbation de notre secteur d'activité et de stratégie d'innovation, il faut à l'évidence reconnaître une profonde évolution de notre champ concurrentiel. Ainsi que je le signalais, le marché des opérateurs de télécommunications par satellites se déplace vers les enjeux de connectivité. Les dernières générations de satellites sont en mesure de connecter à l'Internet de haut débit et à des prix compétitifs, tant dans les pays émergents que dans les pays développés, de vastes segments de population qui ne l'étaient pas. Étendu, le marché qui s'ouvre répond à un besoin indéniable et d'une importance cruciale. Il suscite bien des convoitises.

De nouveaux acteurs apparaissent. Forts d'investissements puissants, ils font montre d'une ambition marquée. Ils s'efforcent de capter la demande universelle de connexion par les satellites. La situation de concurrence exacerbée favorise sans conteste l'innovation et la qualité du service proposé. Ma remarque vaut évidemment bien au-delà des seules frontières françaises.

Au regard de la souveraineté nationale et européenne, la difficulté s'avère de deux ordres.

En premier lieu, les services de connectivité proviendront toujours plus d'un nouvel outil, les constellations en orbite basse.

Pour l'heure, comme la plupart de ses concurrents, Eutelsat utilise de volumineux satellites géostationnaires, éloignés du sol et fixes par rapport à lui. Appelée à s'y substituer, la technologie des constellations en orbite basse arrive progressivement à maturité. Elle repose sur une approche toute différente. Les satellites évoluent alors beaucoup plus près de la Terre et tournent autour d'elle. Dans ce cas, apporter un service constant suppose de couvrir l'orbite d'un nombre élevé de satellites. De flottes de quelques dizaines de gros satellites, nous passons à une logique de centaines, voire de milliers ou même de dizaines de milliers d'objets en orbite basse.

En comparaison du système géostationnaire, le léger avantage de l'orbite basse tient à la latence. Recevoir un signal d'un satellite géostationnaire nécessite 0,4 seconde ; pour un satellite en orbite basse ou très basse, la communication devient quasiment instantanée, de l'ordre de 10 ou 14 millisecondes. Elle équivaut à celle de la fibre optique.

Son inconvénient majeur réside dans le fait que les constellations en orbite basse n'excéderont pas un nombre fort restreint. Le spectre des fréquences qu'elles utilisent s'avère en effet lui-même contraint par nature. Quoiqu'elle puisse être amenée à évoluer encore, l'estimation la plus communément admise aujourd'hui prévoit un maximum de cinq ou six constellations. Au-delà, l'orbite atteindra son niveau de saturation.

L'espace des constellations en orbite basse étant limité, ou « fini », il en résulte que les positions à y prendre deviennent rares, donc onéreuses. Les acteurs nord-américains, dont SpaceX d'Elon Musk, Amazon de Jeff Bezos avec Project Kuiper et la société canadienne Telesat, les Anglais avec OneWeb, ainsi que les Chinois, se préparent à occuper des positions dans l'orbite basse. La place des Européens se réduit, voire est menacée. Nous ne pouvons en

effet exclure que l'ensemble de l'espace de l'orbite basse fasse l'objet d'une captation par des puissances non européennes.

En second lieu, l'attention doit porter sur le financement des opérations que je viens de décrire. À ce stade, vous pourriez vous interroger sur la raison pour laquelle Eutelsat, un des chefs de file mondiaux d'une activité rentable, ne développe pas directement sa propre constellation en orbite basse.

La réponse renvoie au coût extrêmement élevé des objets en orbite basse. La mise au point d'une constellation en orbite basse suppose un investissement d'environ 5 milliards d'euros en moyenne. En regard de notre chiffre d'affaires, que je vous ai précédemment indiqué, la disproportion est flagrante. Un investissement de cette envergure ferait peser un poids économique et un risque commercial beaucoup trop lourds sur une société de la taille d'Eutelsat. Elle ne peut, en l'état, mener seule une telle entreprise.

En comparaison, nos concurrents y parviennent grâce au soutien massif de leurs institutions nationales, en particulier celles des États-Unis d'Amérique. Outre qu'elles portent la marque de l'incontestable dynamisme entrepreneurial de l'industrie américaine, les initiatives d'Elon Musk, Starlink pour les constellations en orbite basse et SpaceX pour les lanceurs, bénéficient du soutien déterminé et coordonné des institutions de ce pays à son industrie spatiale. Ce soutien permet ici au promoteur des initiatives de prendre une position clé dans le domaine des fréquences et de l'orbite basse.

Trois agences américaines contribuent à leur financement : celle de l'armée, la *Defense Advanced Research Projects Agency* (*DARPA*, l'agence du département de la défense), la *National Aeronautics and Space Administration* (*NASA*, l'agence fédérale en charge du programme spatial civil) et la *Federal Communications Commission* (*FCC*, commission fédérale des communications) avec son programme de réduction de la fracture numérique aux États-Unis. Elles y contribuent à hauteur de plusieurs milliards de dollars. Leur engagement témoigne de la perception, par la puissance publique, de ce pays de l'importance des nouveaux systèmes que nous évoquons et de la nécessité d'en financer puissamment la mise en œuvre.

Pour la Chine, du fait de données publiques moins accessibles, les avancées n'apparaissent pas avec la même évidence. Cependant, tant les déclarations de ses autorités que les échanges avec nos interlocuteurs et pairs Chinois montrent une volonté non moins marquée de déployer les nouveaux systèmes.

Pour sa part, Eutelsat prend activement part au consortium dont la Commission européenne a encouragé la création. Communément, ce projet spatial reçoit souvent le nom de son principal instigateur, le commissaire Thierry Breton. Il poursuit pour objectif de développer une constellation de satellites propre à l'Union européenne ou, au moins, d'identité européenne. Par rapport à ses concurrents, il introduirait une logique novatrice de systèmes complexes mêlant orbites basse, haute et moyenne.

Sans rien augurer, les réserves à formuler tiennent ici à la célérité des décisions et à la portée des projets de l'Union européenne, qui ne s'avèrent pas toujours conformes aux exigences des marchés des techniques de pointe. Ceux-ci se caractérisent par la rapidité de l'innovation et l'ampleur des moyens engagés. Il convient de ne le pas perdre de vue.

M. Hervé Derrey, président-directeur général de Thales Alenia Space. Complémentaires, mes propos s'inscriront à la suite de ceux qui viennent d'être tenus. Je partage une vision et une analyse équivalentes de la dynamique qui anime actuellement notre marché.

Je reviendrai d'abord sur certains fondamentaux de l'industrie spatiale. Ils préexistaient à l'émergence des nouvelles constellations de satellites en orbite basse.

À l'évidence, notre marché est celui d'une très haute technologie. Par essence, il revêt un double caractère institutionnel et stratégique. Les États, en particulier les États-Unis, la Chine, mais également la Russie, le financent de manière significative. Nos concurrents y jouissent de soutiens institutionnels et législatifs majeurs. Je pense par exemple au *Buy american Act* (« loi achetez américain ») de 1933 ou à la législation relative au commerce international des armes (*International Traffic in Arms Regulations*, *ITAR*) qui favorisent l'industrie nationale.

À ce jour, environ 50 États possèdent des infrastructures spatiales. Un nombre croissant d'entre eux se dotent de moyens autonomes de production. Bien que la France et l'Union européenne reconnaissent l'espace extra-atmosphérique comme un domaine important, voire stratégique, les budgets qu'elles y consacrent demeurent faibles en comparaison de ceux d'autres pays. Sous l'angle de la dépense par habitant, nos budgets dédiés à l'Espace ne nous placent qu'au quatrième rang mondial. Pour donner un ordre de grandeur, celui des États-Unis s'avère cinq fois supérieur, ceux de la Russie et du Japon respectivement trois fois et deux fois plus élevés.

Nos concurrents internationaux dépendent du marché commercial et de la compétition qui s'y livre pour environ 20 % de leur chiffre d'affaires. Ils bénéficient par ailleurs du financement de programmes institutionnels à hauteur de 80 % de ce même chiffre. En Europe, les équilibres se situent plutôt de l'ordre de 50 % en provenance du marché compétitif, l'autre moitié de celle du marché institutionnel.

Dans cet environnement, l'élément nouveau consiste, comme il a été dit, en l'apparition assez massive du secteur privé. C'est le cas de SpaceX, entité présente à la fois sur le segment des lanceurs et sur celui des satellites avec Starlink, ainsi que des GAFAM (Google, Apple, Facebook, Amazon et Microsoft) et notamment d'Amazon. Ces acteurs disposent de moyens financiers considérables qui leur permettent de ne pas appliquer les modèles économiques (*business models*) classiques. Ils procèdent ainsi à des analyses de rentabilité sur le long terme.

Dans cette conjoncture de forte compétition, Thales Alenia Space s'efforce de rester l'un des chefs de file français et européens du satellite, et de consolider sa position. Elle est une co-entreprise, ou entreprise en participation (*joint-venture*), entre les groupes Thales, pour 67 % de son capital, et Leonardo, à hauteur de 33 %. Implantée dans 17 sites, elle compte environ 7 700 salariés, dont 4 000 en France et 2 000 en Italie. Les autres se répartissent entre plusieurs États européens, en Espagne, en Allemagne, en Belgique, et plus récemment au Royaume-Uni, en Pologne, ainsi qu'en Suisse.

En 2020, en dépit d'une mobilisation et du soutien insignes des agences nationales – l'agence spatiale italienne (*agenzia spaziale italiana*, ASI), le centre national d'études spatiales (CNES) et la direction générale de l'armement (DGA) en France – de même que de l'agence spatiale européenne (*European Space Agency*, *ESA*), la crise sanitaire, les mesures qu'elle a provoquées, ont pesé lourdement sur nos programmes. Le marché de l'exportation s'est également montré quelque peu atone, notamment avec nos clients moyens-orientaux. Les conséquences en apparaissent assez significatives sur notre chiffre d'affaires et sur notre rentabilité. Ainsi, le premier tombe à 1,85 milliard d'euros en 2020, quand il s'établissait à 2,17 milliards d'euros un an plus tôt.

Dans le domaine de la connectivité, Thales Alenia Space se distingue de ses concurrents français, européens et mondiaux. Son implantation nationale se révèle marquée, particulièrement dans le champ des télécommunications et des charges utiles de télécommunication. Les trois-quarts des satellites de télécommunication qu'elle met en orbite géostationnaire sont de fabrication française. Leur production alimente ainsi un vaste tissu de petites et moyennes entreprises (PME) nationales.

Notre prééminence concerne aussi le domaine des constellations spatiales de télécommunications. Depuis la fin des années 2000, nous sommes les maîtres d'œuvre de l'ensemble des constellations commerciales actuellement opérationnelles en orbite basse : Globalstar 2, O3b, Iridium Next. Elles représentent un montant cumulé d'activité de près de 3 milliards d'euros.

Au début de 2020, Telesat, le quatrième opérateur mondial, nous a choisis pour construire sa constellation de télécommunications en orbite basse, nommée Lightspeed. Elle comprendra 300 satellites interconnectés et délivrera partout dans le monde plusieurs térabits par seconde (Tb/s) à des coûts particulièrement compétitifs, pour des services professionnels sécurisés à forte valeur ajoutée. Elle vise principalement un marché d'entreprises, tel que la mobilité à bord de navires ou d'aéronefs, la connexion des stations de base au reste du réseau en matière de communications de quatrième et cinquième génération (4G et 5G), ainsi que les communications sécurisées gouvernementales et d'entreprises.

Comme le signalait M. Rodolphe Belmer, ce marché sera un marché contraint. Du fait de la ressource rare des fréquences, cinq ou six constellations, au maximum, y prendront leur place. Dans ces conditions, les enjeux de souveraineté apparaissent déterminants. Vous ne les ignorez pas. Il importe que nous puissions offrir à nos concitoyens des communications sécurisées et intègres.

La puissance publique en a bien compris et reconnu la nécessité. À l'occasion du comité de concertation entre l'État et l'industrie spatiale (COSPACE) du 24 octobre 2017, M. Bruno Le Maire, ministre de l'économie, des finances et de la relance, s'est exprimé en ce sens. Il soulignait l'importance de privilégier les solutions françaises pour l'accès à l'Internet dans les territoires métropolitains et d'outre-mer, plutôt que de recourir à des systèmes américains, à l'époque Viasat, aujourd'hui Starlink et SpaceX, ou OneWeb, que contrôlent l'État britannique et l'opérateur indien Bharti Global. En 2018, le choix de Thales Alenia Space par Eutelsat, pour réaliser le prochain satellite Konnect VHTS, est intervenu en ce sens.

Si la dimension de souveraineté nationale apparaît essentielle au titre de la protection des communications de nos concitoyens, elle revêt également un enjeu de première importance en matière militaire. Dans ce domaine, proposer des communications parfaitement sécurisées, exemptes de tout brouillage, confine à l'autonomie stratégique. Il s'agit d'acheminer les flux de données depuis ou vers les théâtres d'opération.

À mon tour, j'insiste sur le net soutien de la puissance publique américaine à l'égard des principaux acteurs privés de son industrie spatiale. Ce soutien s'étend aux secteurs des lanceurs et des satellites. Starlink, en particulier, bénéficie de son appui afin de couvrir les zones blanches de 35 États fédérés américains. Dans ce cas précis, l'aide est évaluée à 900 millions de dollars. Outre le dessein de réduire la fracture numérique, ces subventions interviennent également en faveur de l'innovation.

J'ajouterai que SpaceX et Microsoft viennent de signer un accord. Il lie Microsoft Azure, la solution de *cloud computing*, ou informatique en nuage, de Microsoft, et le réseau de communication Starlink, en vue de permettre l'accès depuis n'importe quel point de la

planète à l'ensemble des services de la première : la conservation des données, leur analyse instantanée, l'Internet des objets, etc.

Dans le même ordre d'idée, celui d'une logique de bout en bout, Amazon entend associer sa solution de *cloud* à celles que lui ouvriront ses nouvelles possibilités de connectivité ainsi que son lanceur.

À travers l'intrication des solutions de connectivité et de *cloud*, nous percevons que l'enjeu touche à l'ensemble des services numériques proposés aux citoyens français et européens.

Nous avons déjà évoqué l'exemple du satellite Konnect VHTS, projet que Thales Alenia Space conduit en partenariat avec Eutelsat. Il illustre ce que peuvent être de bonnes pratiques en Europe.

En septembre 2017, le Gouvernement a fixé des orientations quant à la stratégie d'aménagement numérique des territoires. À cette occasion, il soulignait la nécessité de mobiliser l'ensemble des technologies adaptées, en particulier les nouvelles solutions satellitaires.

L'intérêt du satellite réside dans la possibilité de déployer un accès à haut et très haut débit dans des zones à faible densité de population ou d'accès difficile, à un coût très compétitif et dans un délai extrêmement bref. Une fois le satellite en orbite, l'accès à l'Internet devient en effet immédiatement possible en tous points du territoire national. Il apparaît ainsi comme une solution universelle de désenclavement. Au-delà, le coût de raccordement de l'utilisateur devient indépendant de la localisation de celui-ci quand, s'agissant des réseaux terrestres, il augmente de façon exponentielle à mesure que la densité de population décroît.

Thales fournit Eutelsat depuis plus de 30 ans. La première fabrication et le premier lancement d'un satellite issu de leur partenariat intervinrent en 1990. Vingt-huit autres ont suivi.

Sous l'angle des technologies disponibles, nous pouvons affirmer que les satellites géostationnaires et les constellations de satellites se révèlent complémentaires. Les premiers offrent des solutions de très haut débit pour des points spécifiques de la planète à un prix compétitif. En cours de développement, le satellite de dernière génération Konnect VHTS que nous lanceront en 2022 sera le plus puissant satellite de télécommunications jamais mis en orbite. Il pourrait contribuer à réduire fortement la fracture numérique dans quelque quarante pays que nous avons identifiés, en Afrique, en Asie, ainsi qu'en Europe de l'Ouest. Nous le voyons, les enjeux internationaux et d'exportation ne manquent pas d'importance.

Un tel projet, sa technologie de charges utiles à très haut débit, en particulier un processeur embarqué de cinquième génération développé avec STMicroelectronics, son infrastructure au sol de bout en bout des plus robustes et sécurisées, ne sont disponibles que parce qu'elles ont bénéficié d'un fort soutien à l'innovation de la part du CNES, du programme français d'investissements d'avenir (PIA) et de l'*ESA*. Il faut continuer d'en appliquer le modèle.

En définitive, la réponse à la problématique de concurrence mondiale exacerbée que nous soulevons se partage en deux volets principaux. D'un côté, le soutien à l'innovation permet le recours aux technologies indispensables à l'élaboration des nouvelles solutions, qu'elles soient celles des satellites géostationnaires ou des constellations en orbite basse. De

l'autre, nous trouvons les grands programmes, à l'instar en Europe de Galileo en matière de navigation et de Copernicus dans le domaine de l'observation de la Terre.

S'agissant de l'initiative du commissaire européen M. Thierry Breton, je rejoins l'analyse de M. Rodolphe Belmer. Une initiative de cette nature, qui tend à fédérer les forces, se révèle incontournable en ce que nos acteurs privés en France et en Europe ne possèdent pas, seuls, la capacité de financement que l'ampleur des programmes, de l'ordre de cinq voire six milliards d'euros, commande.

L'enjeu tient désormais à la vitesse d'exécution. Nos concurrents américains font montre d'une célérité redoutable. Le service Starlink connaît actuellement sa phase dite de bêta-test. Sa commercialisation complète est annoncée dès la fin de l'année 2021. Il faut que l'ensemble des acteurs européens progressent aussi rapidement que possible, tant du point de vue des financements des projets que sur un plan industriel.

Quant à la Chine, nous savons qu'une volonté forte s'y manifeste de participer à la compétition relative aux constellations. Toutefois, nous ne disposons assurément que de peu d'informations au sujet de ses programmes et de leur calendrier de mise en œuvre.

Je conclurai provisoirement en répétant combien l'innovation constitue le moteur de la compétitivité de l'industrie spatiale. Sur ce constat, il nous faut persévérer dans la direction que le CNES, la DGA, le PIA et le plan de relance ont prise. S'ajoutent la contribution de la France à l'*ESA* et les financements de la Commission européenne, tels ceux issus du programme-cadre Horizon Europe et du fonds européen de défense.

L'étendue du soutien financier que la France apportera à l'occasion de la conférence ministérielle de l'*ESA* prévue en 2022 sera décisive. Le Gouvernement et la représentation nationale doivent y assigner un objectif prioritaire, au service de programmes européens majeurs, dont celui d'une constellation européenne. Qu'il s'agisse de l'emploi, de la balance commerciale, de ses capacités industrielles stratégiques, de sa souveraineté numérique tant en matière civile que militaire, l'investissement produira indubitablement un bénéfice direct pour la France.

M. Philippe Latombe, rapporteur. Vous l'avez évoqué tous deux, les GAFAM s'impliquent désormais dans le secteur spatial. Quelles conséquences en prévoyez-vous ?

Je pense par exemple à l'initiative d'Amazon d'ouvrir une manière de concours aux jeunes entreprises innovantes, les *start-up*, de ce secteur. Celles-ci peuvent poser leur candidature jusqu'au 21 avril 2021, en vue d'être incubées, autrement dit de bénéficier d'un appui à leurs projets et développement. L'une des conditions en tient à leur utilisation du *cloud* d'Amazon Web Services (AWS). Ne s'agit-il pas pour le géant américain d'un moyen de capter certains de nos talents du domaine spatial ? Dans l'environnement, ou « écosystème », que vous connaissez, pensez-vous que de nombreuses sociétés répondront à l'appel d'Amazon ? Des méthodes de ce type induisent-elles pour nous un risque véritable de perte de compétences et de technologies d'avenir ? Au contraire, nos chercheurs sont-ils suffisamment intégrés pour ne pas céder à cet appel ?

M. Hervé Derrey. Du moins ces méthodes ne surprennent-elles nullement. Les principaux acteurs du *cloud* visent à attirer le plus d'applications possible sur celui qu'ils hébergent, d'une manière plus ou moins partenariale et ouverte. Amazon appartient plutôt à la catégorie des acteurs au système relativement fermé. L'exemple que vous décrivez s'inscrit dans la cohérence de sa stratégie et de son approche.

Certainement le risque existe-t-il qu'Amazon ou d'autres acteurs américains du *cloud* attirent de jeunes entreprises innovantes européennes. Il revient à la puissance publique d'organiser un environnement qui leur soit favorable et susceptible d'obvier à ce risque.

M. Rodolphe Belmer. Ici, le risque ne diffère pas sensiblement de celui qui prévaut dans tous les domaines d'innovation technologique. Aujourd'hui, l'idée de financer la recherche et l'innovation par les petites entreprises, les *start-up*, joue en faveur des marchés qui détiennent les capitaux les plus abondants. Elle entraîne une migration des talents, notamment de l'Europe vers les États-Unis. La situation ne concerne pas uniquement le domaine spatial. Nous la retrouvons dans bien d'autres secteurs de l'industrie.

Historiquement, la recherche spatiale en Europe bénéficiait de l'appui de grands groupes, à l'instar de Thales ou Airbus. Progressivement, la recherche se répand dans le monde des *start-up*. Moins coûteuse, reposant davantage que par le passé sur des logiciels informatiques (*softwares*), elle prend une forme nouvelle. Désormais, le poids des capitaux prime celui des groupes industriels en place. Il semblerait que l'Europe n'en ait pas pleinement pris la mesure.

M. Philippe Latombe, rapporteur. Avec le programme Ariane, l'Europe dispose d'un lanceur d'une indéniable qualité. Pour autant, nous avons manqué le marché du lanceur réutilisable. Les raisons en sont multiples. Peut-être n'y avons-nous pas suffisamment cru.

Resterons-nous maintenant en marge d'innovations majeures ? Vous-même nous l'avez indiqué : la bataille qui se joue est une bataille de place, au sens d'espace physique. L'espace autour de la Terre ouvert aux constellations de satellites s'avère limité. Y prendre une place requiert de ne pas atermoyer, car l'occasion ne se représentera plus. Or, nous constatons qu'un programme suit déjà sa phase de bêta-test. Amazon prévoit de lancer le sien. D'autres acteurs montrent une volonté identique. Ne sommes-nous pas en train de prendre un retard rédhibitoire ? Le type d'initiative qu'Amazon promeut en matière d'innovation n'aggrave-t-elle pas la situation ?

M. Rodolphe Belmer. Votre intervention appelle plusieurs niveaux de réponse.

S'agissant des constellations en orbite basse, leur nombre sera en effet nécessairement circonscrit. Nous l'avons signalé. De fait, lorsque les places seront prises, et à moins que les Européens ne parviennent à occuper l'une d'elles avant cette échéance, ils n'auront ensuite plus le moyen de rattraper leur retard.

C'est pourquoi j'estime que les constellations en orbite basse représentent une infrastructure de télécommunication critique et de souveraineté. Du moins faut-il qu'elles le deviennent en France et sur notre continent. Par suite, il appartient aux Européens d'agir de telle sorte que l'une de leurs entreprises ou institutions s'impose en la matière. La difficulté ne revêt ici nulle dimension technologique : nos industriels, comme Thales Alenia Space, savent d'ores et déjà concevoir des constellations en orbite basse ; nous savons également procéder au lancement des satellites, puis les exploiter. La difficulté ressortit d'abord à une question d'ordre financier.

Or, le secteur commercial n'est à ce jour pas structuré pour financer intégralement un investissement aussi étendu et risqué. Afin de pondérer le risque d'une infrastructure technologique de la dimension des constellations de satellites, et à l'imitation de ce qui prévaut sur d'autres continents, nous avons besoin du soutien de la puissance publique.

La décision revêt un caractère politique. Compte tenu de l'échelle de l'investissement, son niveau est vraisemblablement celui de l'Union européenne.

Un deuxième sujet porte sur l'innovation et la compétitivité de l'industrie nationale et européenne. Vous évoquiez, M. le rapporteur, l'exemple d'Ariane. Vous releviez que ce programme avait manqué l'étape du lanceur réutilisable. Sans doute sous-entendiez-vous par là que l'exemple était la marque d'un déclin, d'un déclassement, de l'industrie spatiale européenne.

Je souhaiterais nuancer l'affirmation. Je m'y emploierai en qualité de représentant d'une société cliente de l'industrie spatiale européenne et du lanceur Ariane.

Cette industrie demeure sans conteste performante. En dépit de son manque de soutien public, elle ne cède en rien à la concurrence internationale, tant du point de vue technique que sous l'angle du rapport qualité-prix. Eutelsat acquiert ainsi 90 % de ses satellites auprès des deux acteurs européens Thales Alenia Space et Airbus Defense and Space. Elle sous-traite la moitié de ses lancements à Ariane.

Toute autre considération mise à part, Eutelsat agit d'abord comme une entreprise commerciale privée. Des exigences de rentabilité la meuvent. Ses choix se fondent donc sur des critères strictement rationnels. Le satellite Konnect VHTS en cours de fabrication par Thales Alenia Space représentera une innovation de niveau mondial. Le premier de cette classe, il permettra d'offrir d'excellents débits de connexion à prix réduit à la population européenne située dans des zones rurales.

Cependant, le risque d'un déclassement existe-t-il à terme ? Nous ne pouvons l'exclure. Assurément, le secteur spatial change de paradigme. Jusqu'à présent, l'industrie repose sur une logique d'expertise et d'innovation. Chaque objet de sa production s'avère différent. Pièce unique, chaque satellite remplit des missions en propre. Elle évolue désormais vers un marché de volumes. Les constellations en orbite basse supposent la fabrication de milliers de satellites. Une logique de réplicabilité et d'industrialisation est appelée à prendre le pas.

Si notre industrie se révélait incapable d'entrer dans cette nouvelle logique, faute de commandes suffisantes en volumes, elle courrait un risque d'un déclassement. En effet, elle perdrait en productivité, ce qui jouerait défavorablement sur ses prix et sa compétitivité sur le marché.

Sans doute la co-entreprise ArianeGroup se confronte-t-elle à l'amorce d'un phénomène de ce type. Si ses ingénieurs n'ont pas opté pour la solution des lanceurs réutilisables, la raison en tient à un volume insuffisant de commandes.

Dans sa configuration actuelle, Ariane répond au besoin d'un certain nombre de lancements par an. Les institutions européennes et le marché commercial – principalement Eutelsat – les lui commandent. La faible fréquence de ces lancements ne permet pas d'envisager un bénéfice effectif à l'emploi de lanceurs réutilisables.

Au contraire, avec son projet Starlink, SpaceX s'apprête à lancer des milliers, voire des dizaines de milliers de satellites. Ils nécessiteront plusieurs centaines de lancements. Soutenue, comme nous l'avons rappelé, par le financement de la puissance publique américaine, la logique devient ici celle des gains de productivité et des volumes.

De toute évidence, une telle politique industrielle influe sur la performance économique d'acteurs comme Ariane et sur leurs choix stratégiques. Nous ne saurions néanmoins reprocher au lanceur européen ceux qu'il a adoptés en l'absence d'augmentation du volume de ses commandes. Ariane reste un excellent lanceur en considération de la mission qui lui incombe.

M. Philippe Latombe, rapporteur. Ne pouvons-nous tout de même identifier un manque d'anticipation ? Le choix de ne pas s'engager dans l'utilisation de lanceurs réutilisables en l'absence de marché au moment de la décision ne décèle-t-il pas un défaut de vision quant à l'avenir des usages et de ce marché ? Les Américains, à l'inverse, paraissent s'être projetés plus avant, avoir perçu les futures pratiques bien en amont de leur matérialisation.

M. Rodolphe Belmer. Dans ce débat, je me dois de tenir la place qui me revient. Toutefois, s'il me faut formuler un avis en tant que citoyen, je reconnaîtrai que les acteurs européens pâtissent vraisemblablement d'un problème de vision stratégique. Vous l'avez sûrement constaté dans le cours des travaux que vous menez à l'Assemblée nationale au sujet de l'Internet par satellite : jusqu'à une époque récente, la puissance publique ne croyait pas en la pertinence de ce mode de connexion. Elle en rejetait l'idée. Toute l'attention se reportait sur la fibre optique.

Or, la nécessité du recours aux nouvelles constellations de satellites, de leur lancement, naît du constat que les opérateurs terrestres ne sauront satisfaire l'ensemble des besoins de connexion des populations. En la matière, les États-Unis ont apporté la preuve de leur pragmatisme. À partir de leur constat du caractère indispensable des satellites pour couvrir les zones rurales, ils mettent en branle l'ensemble de la chaîne de valeur, de la fabrication de ces satellites à leurs lanceurs. Par leurs institutions, par le programme *Rural Digital Opportunity Fund* (*RDOF*), ils y apportent les financements adéquats.

M. Philippe Latombe, rapporteur. Nous manque-t-il l'équivalent de la *DARPA* américaine ?

M. Hervé Derrey. Je reconnais également que, dans le domaine spatial, l'industrie européenne se révèle très performante. Elle remporte des marchés partout dans le monde. Plus tôt au cours de nos échanges, je citais l'exemple de la constellation de TeleSat. Cet opérateur a choisi les services de Thales Alenia Space.

Nous sommes manifestement en capacité de répondre aux attentes, à condition que se maintienne ou se renforce le financement de l'innovation. Politique, la décision d'appuyer les grands programmes permettra d'offrir des solutions autres que celles des entreprises et de l'industrie américaines.

Le programme de constellation européenne nécessite le soutien massif des États membres de l'Union européenne. Son financement, ainsi que son déploiement rapide, en dépendent. Pour l'heure, nous accusons certainement quelque retard par rapport aux initiatives américaines. Paradoxalement, il nous laisse la possibilité de nous montrer plus innovants encore et d'apporter une vraie valeur ajoutée. Ce résultat suppose une volonté politique forte. Sa concrétisation laisse désormais peu de champ à d'autres retards.

M. Philippe Latombe, rapporteur. Mais pensez-vous que nous ayons besoin d'un organisme stratégique de vision à long terme ? Dans l'affirmative, doit-il se placer à l'échelle française ou européenne ? Subsidiairement, le personnel politique, les décideurs, vous

paraissent-ils suffisamment au fait des technologies à l'œuvre de nos jours ? Ne percevez-vous pas un déficit d'acculturation de leur part dans le domaine des techniques de pointe ?

M. Hervé Derrey. Pour ce qui a trait aux organes, je ne crois pas qu'il nous en faille de supplémentaires. Je n'en perçois pas véritablement l'intérêt. Nous disposons déjà des agences spatiales nationales et de l'agence européenne, l'*ESA*. En France, le CNES se révèle éminemment compétent.

Quant à la conscience politique, nous constatons qu'elle émerge. À mon sens, M. le commissaire Thierry Breton et ses équipes énoncent une vision parfaitement claire dans le domaine dont nous traitons. Ils en comprennent les sujets et enjeux. Il faut désormais qu'ils trouvent un relais dans le soutien indéfectible des États membres de l'Union.

M. Rodolphe Belmer. Pour ma part, j'estime que le long terme prime dans les domaines d'innovation technologique. Il incombe à l'État de remplir son double rôle de stratège et de stimulateur d'investissements qui s'inscrivent dans la durée. La logique en échappe parfois au marché commercial qui, par définition, s'attache prioritairement à des considérations de rentabilité de moyen terme.

Concernant la culture de l'innovation, du progrès, celle de la technologie, je procède au même constat que M. Hervé Derrey. J'en tire cependant une conclusion différente.

Certes, avec l'arrivée de M. Thierry Breton, l'Union européenne prend en charge la nouvelle problématique des constellations en orbite basse et des télécommunications par satellites, essentielle à notre souveraineté numérique. Elle y donne une impulsion forte. Devons-nous uniquement nous en féliciter ? Rien n'est moins sûr.

Nous pouvons en effet nous interroger sur ce qu'il serait advenu si une autre personnalité politique avait pris la responsabilité du portefeuille du marché intérieur. Doté de qualités de meneur hors du commun, l'actuel commissaire européen vient lui-même du secteur industriel, il y a acquis une compétence considérable. Sa présence, son action, constituent une chance précieuse et décisive. Nous ne saurions cependant laisser les institutions européennes reposer sur le talent d'un seul homme.

M. Philippe Latombe, rapporteur. Souhaitez-vous aborder d'autres aspects du sujet qui nous réunit ou insister sur certains de ceux dont nous avons traité ?

M. Rodolphe Belmer. Vous nous avez demandé s'il existe dans notre domaine des segments d'innovation qui méritent notre attention parce qu'ils représentent des services d'avenir. Je répondrai par l'affirmative.

Nous nous distinguons avantageusement en France dans ce que nous appelons le segment spatial. Par le moyen des lanceurs, il consiste à amener des satellites dans l'espace extra-atmosphérique. Bientôt, les systèmes de télécommunication spatiaux reposeront sur des systèmes espace et sol. Autrement dit, les systèmes sols prendront davantage d'importance dans la création de valeur ajoutée. Or, nous ne disposons que de fort peu de segments sols de qualité en Europe. Nous n'innovons pas suffisamment en la matière. Il nous semble que la puissance publique devrait y réfléchir et l'industrie s'organiser pour développer les technologies qui s'imposent.

M. Hervé Derrey. Je souhaite pareillement intervenir sur la question des nouveaux segments. Outre le segment sol, pour lequel je souscris aux propos de M. Rodolphe Belmer, je mettrai en avant le sujet de la maîtrise de l'espace. Il induit en particulier l'enjeu de la

supervision des objets spatiaux. Lui-même a trait au problème des collisions et recouvre par ailleurs une dimension de défense. J'évoquerai ensuite les services en orbite. Ils sont appelés à se développer significativement. Enfin, l'attention demeure de rigueur en matière d'observation spatiale vers la Terre ou l'espace, qu'elle soit optique, radar ou hyperspectrale. Elle progresse également selon une cadence soutenue et apparaît comme un domaine stratégique d'avenir.

M. Philippe Latombe, rapporteur. Je prends bonne note de vos dernières remarques.

Audition commune, ouverte à la presse, de représentants - du groupe Atos : Mme Coralie Héritier, responsable des identités numériques, dirigeante d'IDnomic, et d'IN Groupe : MM. Romain Galesne-Fontaine, directeur des relations institutionnelles, et Yann Haguet, vice-président exécutif identité numérique, copilote du groupe de travail identité numérique au sein du comité stratégique de filière des industries de sécurité

(6 avril 2021)

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. Nous accueillons Mme Coralie Héritier, dirigeante d'IDnomic et responsable des identités numériques chez Atos, M. Yann Haguet, vice-président exécutif identité au sein d'IN Group, copilote du groupe de travail identité numérique au sein du comité stratégique de filière (CSF) des industries de sécurité, ainsi que M. Romain Galesne-Fontaine, directeur des relations institutionnelles d'IN Group.

Notre échange s'inscrit dans une réflexion sur l'identité numérique. La semaine dernière, nous avons auditionné les représentants de l'agence nationale des titres sécurisés (ANTS), du programme interministériel France Identité numérique, ainsi que le responsable d'une entreprise concernée par ce sujet.

Aujourd'hui, notre objectif consiste à mieux comprendre les choix technologiques qui s'opèrent à l'occasion du projet d'identité numérique régalienne. Nous souhaitons également mieux cerner la façon dont les acteurs de ce projet interagissent au service de la meilleure performance possible et de la prise en compte des enjeux de souveraineté qui occupent nos travaux.

M. Philippe Latombe, rapporteur. J'évoquerai trois sujets sur lesquels nous aimerions vous entendre.

Le premier a trait aux enjeux de l'identité numérique et à la manière dont le déploiement de solutions publiques ou privées est susceptible de contribuer au renforcement de la souveraineté numérique de la France et de l'Europe. Quels choix technologiques ont été retenus et la position de l'Imprimerie nationale vis-à-vis de l'ANTS.

Pour parler sans détour, nous cherchons à savoir comment vous vous organisez pour définir ensemble des solutions techniques qui, dans le domaine de la sécurité, répondent à l'état de l'art. J'entends des solutions qui intègrent les dernières innovations. La question s'étend également à votre capacité à privilégier des solutions souveraines.

Le deuxième point intéresse le déploiement de la carte nationale d'identité électronique (CNIe), dont il était prévu qu'il s'effectue en lien avec une identité numérique. Vous ne l'ignorez nullement, cette perspective nourrit de fortes inquiétudes. Des parlementaires s'en sont récemment fait l'écho dans un courrier qu'ils ont adressé au Gouvernement.

Selon vous, comment s'explique le retard de déploiement que nous enregistrons, alors que la France s'avère déjà en décalage avec les autres pays européens ? Des marges de manœuvres, des moyens existent-ils afin d'accélérer le mouvement qui permettra d'apporter à nos concitoyens les nouvelles solutions disponibles ?

Enfin, nous reviendrons sur les usages de l'identité numérique. Je m'interroge, d'une part, sur les besoins et attentes des utilisateurs, d'autre part, sur les possibilités que ces solutions offrent ou offriront à terme.

J'apprécierais tout particulièrement de vous entendre sur le modèle économique de l'identité numérique. Il a fait l'objet de nombreux débats. À votre avis, quelle place les acteurs privés doivent-ils y prendre ? Comment convient-il de le financer ? En dernier lieu, de quelle manière rassurerons-nous les citoyens quant à la protection de leurs données personnelles, alors que la presse révèle régulièrement des affaires de fuites de ces données ?

M. Romain Galesne-Fontaine, directeur des relations institutionnelles, IN Groupe. Mon propos liminaire concernera IN Groupe. Structure publique, IN Groupe est l'imprimerie de l'État. Celui-ci en détient intégralement le capital. Spécialiste de l'identité et des services numériques sécurisés, IN Groupe opère au service de la mission régalienne de réalisation des documents et des systèmes d'identité sécurisés. Il s'agit des passeports biométriques, des cartes nationales d'identité électroniques, des permis de conduire, des titres de séjour.

IN Groupe conçoit également les documents et systèmes qui permettent l'exercice d'un droit professionnel reconnu par l'État, telles que les cartes des agents publics, celles des conducteurs de poids lourds en France, ou la plateforme d'identité des professionnels de santé.

IN Groupe mène sa mission conformément au cadre légal applicable aux prérogatives de l'Imprimerie nationale exercées pour le compte de l'État.

Comme la plupart des membres de l'Union européenne, la France a choisi de s'appuyer, en matière d'identité, sur un opérateur industriel public capable d'intégrer de manière agnostique les meilleures technologies du marché. Ce choix permet à l'État de préserver sa souveraineté et son indépendance technologique, tout en garantissant la protection et la confidentialité de l'identité de ses ressortissants. De fait, l'Imprimerie nationale est amenée à connaître de l'identité de l'ensemble des Français.

Ses prérogatives trouvent leur contrepartie dans les engagements qu'elle prend vis-à-vis de l'État. Qu'il s'agisse des composants, des moyens de sécurité, des systèmes et des innovations, elle assure tout d'abord une veille technologique permanente dans le domaine de l'identité. Par cette action, elle apporte à l'État une maîtrise technologique à l'état de l'art. Elle lui garantit ensuite la sécurité de l'approvisionnement de ses titres d'identité, de leurs composants et des techniques qui concourent à leur fabrication. Enfin, dans sa démarche de sécurisation des titres, elle sélectionne les solutions techniques pour lesquelles elle sait compter sur au moins deux fournisseurs qualifiés ou qualifiables.

L'exigence en est devenue centrale depuis les crises de 2017 et de 2018. Les liquidations judiciaires inopinées et soudaines de fournisseurs risquèrent alors de compromettre la production des passeports français. Seules la mobilisation des réserves de sécurité de l'Imprimerie nationale et l'identification d'autres fournisseurs permirent de maintenir la production. Ces situations ont conduit le ministère de l'intérieur, l'ANTS et l'Imprimerie nationale à entériner, en matière d'identité, une obligation de travailler simultanément avec plusieurs fournisseurs et de diversifier les sources d'approvisionnement.

Les fournisseurs retenus dans le respect des règles de la commande publique se soumettent de plus à une qualification industrielle stricte. Elle permet de vérifier leur capacité à fournir leur prestation à l'Imprimerie nationale pendant toute la durée de vie du titre. La

qualification intègre ensemble des aspects techniques, économiques, de durabilité, de conformité aux normes et de sécurité d'approvisionnement.

À titre d'exemple, pour chaque approvisionnement stratégique, le choix des fournisseurs de l'Imprimerie nationale en vue de la production de la nouvelle CNIe a fait l'objet d'une sélection rigoureuse. De façon non exhaustive, je citerai le polycarbonate, les encres, le dispositif holographique, les composants électroniques, la plateforme de personnalisation ou les équipements de fabrication. Il est à noter que la plupart des entreprises partenaires du programme de CNIe sont françaises ou européennes.

L'enjeu consiste évidemment à assurer le déploiement généralisé de la CNIe, engagé le 15 mars 2021. La montée en puissance repose sur un outil industriel que nous avons dimensionné en conséquence. Nous aurons la capacité d'atteindre un volume de production et de personnalisation de 10 millions de CNIe par an. Pour la partie identité numérique de la carte, nous sommes aussi en mesure de poursuivre les travaux relatifs aux conditions de fourniture aux usagers d'un code confidentiel, ou numéro d'identification personnel (PIN, *personal identification number*).

Par ailleurs, pour le compte de l'agence du numérique en santé, nous développons le projet e-CPS. Il consiste en une version dématérialisée, sur *smartphone*, de la carte des professionnels de santé. Avec elle, nous évoquons une identité numérique que ces professionnels utilisent notamment pour se connecter au système informatique de l'assurance maladie.

IN Groupe mène aussi des activités à l'exportation. Elles contribuent à maintenir sa maîtrise de l'état de l'art. Le gouvernement monégasque nous a par exemple sélectionnés pour mettre en œuvre sa nouvelle plateforme d'identité légale, physique et numérique. IN Group lui fournira une carte d'identité électronique puis, à partir d'elle, une identité numérique dérivable sur *smartphone*, ainsi qu'une plateforme de services numériques.

Je compléterai mon propos en revenant sur une audition que votre mission d'information a conduite ce jeudi 1er avril 2021. Il me semble que l'une des personnes que vous avez entendues a fait montre d'approximation, voire vous a volontairement communiqué des données erronées.

En aucun cas la nouvelle CNIe n'équivaudra-t-elle à une simple copie du permis de conduire de 2013 ou du titre de séjour des étrangers.

Certes, comme ces titres, la CNIe doit respecter la réglementation européenne. Elle partage avec eux un cadre commun. Elle en partage encore quelques propriétés : le polycarbonate, le format d'une carte bancaire. Cependant, pour tout expert de l'identité, la ressemblance s'arrête là.

La CNIe inclut des sécurités de toute nouvelle génération. Elles n'avaient pas encore été employées. Son dispositif holographique utilise ainsi des nanomatériaux. Il autorise un contrôle variable optique. Inédit, le bord transparent de la carte prolonge le fonds sécurisé. Sa puce comprend un conteneur identité numérique développé avec l'industrie française. Un cachet électronique visible associe une signature numérique. La liste est longue des innovations visibles ou invisibles du nouveau titre. Des raisons évidentes de confidentialité m'interdisent de décrire les secondes.

La CNIe correspond à un titre dont les innovations côtoient des sécurités expérimentées et robustes. Les unes et les autres se conforment au cahier des charges de l'ANTS et des forces de police.

Une remarque avait porté sur un possible déséquilibre de la relation entre l'ANTS et l'Imprimerie nationale. Je rappelle qu'il s'agit d'une relation de confiance entre un donneur d'ordre public et un expert industriel public. L'ANTS, ainsi que les forces de police, établissent le cahier des charges sécuritaire d'un titre. Nous parlons alors de « cibles de sécurité ». En réponse, l'Imprimerie nationale propose une architecture qui combine un ensemble de sécurités physiques, électroniques et numériques. L'ANTS et les forces de l'ordre valident ensuite cette architecture : elles conservent donc le dernier mot sur la conception (*design*) et les aspects de sécurité du titre que l'Imprimerie nationale leur soumet.

Au cours de votre audition, des questions portaient sur la photographie du nouveau titre d'identité.

Avant toute chose, je préciserai qu'il ne s'agit pas d'une photographie en noir et blanc, mais d'une photographie en tons de gris. La directrice de l'ANTS a expliqué que la demande en provient des forces de l'ordre. Les raisons en tiennent au contrôle visuel, physique, du titre.

Ensuite, on a pu se demander si le procédé en était américain et ce qui avait justifié le choix de recourir à une technique étrangère.

Je déments ici un quelconque défaut de maîtrise technique : l'Imprimerie nationale peut parfaitement produire des titres en polycarbonate qui contiennent de la couleur. Elle le démontre à l'occasion de son partenariat avec le gouvernement monégasque. Il s'avère que 90 % de la centaine de pays qui, dans le monde, émettent des titres d'identité en polycarbonate, utilisent le système de gravure laser en tons de gris au cœur de la carte, choisi pour la CNIe française.

La technique en comprend deux blocs principaux : le matériau et les équipements de gravure laser. Une société européenne développe et fournit le premier. Les seconds se révèlent d'origine française. Une société située à Orléans, qui emploie 50 collaborateurs, produit et utilise ces équipements. Il se trouve qu'elle a fait l'objet d'un rachat, voici quelques années, par une entreprise américaine. La technologie que nous sollicitons n'en demeure pas moins française. Conclure que nous aurions opté pour un procédé américain au détriment de techniques d'une origine géographiquement plus proche de nous, paraît pour le moins contestable.

Enfin, s'agissant du cachet électronique visible de la CNIe, et ainsi que la directrice de l'ANTS l'a indiqué au cours de son audition, le projet n'a pas pu intégrer dans les premières phases de son développement la norme 105 car la publication de celle-ci ne remonte qu'au mois d'octobre 2020. En revanche, il reste loisible d'envisager une évolution conforme aux spécifications de cette norme dans les prochaines phases du projet. La décision en reviendra à l'ANTS.

Nous nous confrontons souvent à des sollicitations de sociétés qui surenchérissent sur les aspects de sécurité en vue de promouvoir leurs solutions. Je rappelle qu'un titre d'identité se compose d'un ensemble d'éléments de sécurité qui répondent précisément aux cibles que le ministère de l'intérieur et l'ANTS ont déterminées. La surenchère que nous constatons ne nous apporte rien, à plus forte raison quand la technique dont elle vante le mérite n'a obtenu aucune reconnaissance en dix ans d'existence et qu'elle fait peser un risque certain en matière d'approvisionnement stratégique.

Je terminerai ma présentation en ramenant le débat sur un sujet central, celui de l'identité numérique. De véritables enjeux s'y décèlent sous l'angle de la souveraineté nationale.

En elle-même, l'identité ressortit à la souveraineté. Pour IN Groupe, elle constitue non un service, mais un droit fondamental. Il nous semblerait inconcevable que l'État ne prenne aucune part à la mise en place de l'identité numérique. Au contraire, par le moyen de la CNIe, l'État introduit un support qui autorise un large déploiement dans la population française, à l'attention de ceux qui le souhaitent, d'une ou plusieurs identités numériques sécurisées.

À notre niveau, nous nous réjouissons de contribuer à ce vaste projet. Nous saluons l'ambition et la qualité des travaux de son promoteur, le programme France Identité numérique.

Prête à fournir l'identité numérique des Français, l'Imprimerie nationale jouera son rôle au service de la stratégie de l'État, à l'instar d'autres acteurs publics ou parapublics, telle La Poste. Moyennant la délivrance du code confidentiel PIN de la CNIe, nous pouvons dès 2021 déployer la solution d'identité numérique que nous avons développée.

Ici, souveraineté nationale et souveraineté européenne se combinent. Par sa puissance normative, face à d'autres modèles qui émergent à travers le monde, l'Europe doit incarner une troisième voie dans la société numérique : celle de la protection des données personnelles et de l'identité. Elle se distinguera alors d'un modèle de monétisation de la donnée personnelle, ainsi que d'un autre modèle où données et identité numériques serviraient au contrôle social.

Mme Coralie Héritier, dirigeante d'IDnomic, responsable des identités numériques du groupe Atos. Je comprends que j'interviens devant vous principalement en ma qualité de copilote d'IN Groupe auprès du comité stratégique de filière (CSF) sur le projet identité numérique et en tant qu'experte de l'identité numérique.

Je vous présenterai le groupe Atos puis, en son sein, l'activité relative à l'identité numérique qui retient aujourd'hui notre attention.

Le groupe Atos est issu de la réunion de plusieurs acteurs du conseil et des services du numérique, ou technologie de l'information (*information technology*, IT) : Sligos et Sema Group, puis Siemens IT Solutions and Services et Bull. Son histoire a conféré au groupe Atos une dualité d'activités complémentaires, entre les services numériques et des produits intéressant des domaines comme la cybersécurité ou les supercalculateurs. S'ajoute une activité de recherche et d'innovation en matière d'informatique quantique.

D'une manière générale, le groupe Atos soutient le développement numérique de ses clients. À ce titre, il s'attache aux questions de cybersécurité. L'identité numérique figure au nombre de ces questions. Elle forme en effet l'un des piliers qui assurent la confiance indispensable au déploiement des activités numériques.

Anciennement Keynectis SA, spécialisée en cybersécurité, l'entreprise IDnomic a rejoint le groupe Atos en octobre 2019. À cette date, elle assurait déjà le copilotage du groupe de travail consacré au projet identité numérique du CSF des industries de sécurité.

IDnomic conçoit des certificats électroniques, selon une technologie d'infrastructure à gestion de clés. Celle-ci apporte des éléments de sécurité, comme le chiffrement de communications ou de fichiers, de l'authentification forte, la signature électronique. Nous l'avons tôt mise en service, en sous-traitance de l'Imprimerie nationale, désormais IN Groupe,

et en partenariat avec l'ANTS. Son utilisation a d'abord concerné les passeports électroniques, devenus biométriques, français. Nous l'avons ensuite exportée. Elle a servi au déploiement des passeports d'environ trente autres pays.

Dans le processus d'émission des passeports biométriques, nous avons fourni avec cette technologie une chaîne de sécurité et de confiance.

M. Philippe Latombe, rapporteur. Sur l'identité numérique et, en particulier, la CNIe, pourquoi avons-nous pris autant de retard en France ? Pourquoi avons-nous dû, dans l'urgence, nous diriger vers une solution dont l'Union européenne nous avait d'assez longue date montré la voie ?

Mme Coralie Héritier. La réaction française n'est cependant pas si récente. Avec IN Groupe, nous appartenons aux acteurs qui nous trouvons au cœur de la question depuis des années. Nous avons œuvré dans différentes commissions, à des projets tels qu'IdéNum. Le Parlement s'est également saisi du sujet. Le frein qui y fut mis eut une origine essentiellement politique. Il ne m'appartient pas d'insister sur cet aspect. Sans doute, la société ni le monde politique français n'étaient-ils suffisamment prêts.

Désormais, la réponse que nous apportons se conforme parfaitement au Règlement européen. J'évoquais les passeports biométriques précisément parce que ce Règlement tend à généraliser les exigences qui, à l'instigation de l'organisation de l'aviation civile internationale (OACI, ICAO en anglais), prévalent en matière de transport aérien.

M. Philippe Latombe, rapporteur. S'agissant de la carte nationale d'identité, nous avons le sentiment que des pays européens ont été nettement en avance sur la France. Je pense en particulier au Portugal. Il semble qu'il en aille de même en matière d'identité numérique. La France paraît très en retard. Ce constat a incité, voici quelques jours, plusieurs de mes collègues parlementaires qui ont conduit la mission identité numérique à écrire au Premier ministre. Ils lui demandent d'intervenir pour hâter les réalisations françaises dans ce domaine.

La base réglementaire existe. Que se passe-t-il donc pour que nous accusions un tel retard ? La question reste ouverte.

M. Yann Haguet, vice-président exécutif identité numérique d'IN Groupe, copilote du groupe de travail identité numérique au sein du comité stratégique de filière des industries de sécurité. Je n'entrerai pas non plus dans des considérations d'ordre politique. Je puis néanmoins apporter certaines précisions. Par les retours d'expérience qui s'y échangent, le groupe de travail consacré aux enjeux d'identité numérique auprès du CSF des industries de sécurité offre un observatoire privilégié sur ces questions.

La genèse du programme s'avère plutôt ancienne. Elle remonte aux années 2000. Mme Coralie Héritier évoquait la multiplicité des commissions ou groupes de travail qui sont intervenus. Je puis citer le projet d'identité nationale électronique sécurisée (INES). La préoccupation a tôt existé. Les industriels se sont pareillement vite intéressés au sujet.

Le projet de protection des identités est apparu à partir de 2005. Il comportait deux volets. La France a d'abord choisi de concentrer ses efforts sur le problème du passeport, parce qu'il s'agit d'un document de voyage. Ils ont abouti en 2006 à la création du passeport électronique, en 2009 au passeport biométrique.

Au début des années 2010, la France s'est penchée sur la question de la CNIe. Par sa décision n° 2012-652 DC du 22 mars 2012, le Conseil constitutionnel a porté un coup d'arrêt

à son élaboration. La décision de la Haute instance remettait en cause le principe de la mise en place d'une base centralisée des données biométriques de la population française, que la Commission nationale de l'informatique et des libertés (CNIL) jugeait par ailleurs irrecevable.

Il a fallu en conséquence retenir une approche non seulement différente, mais qui tînt compte de la pratique des autres États membres de l'Union européenne. Des événements sont ensuite intervenus.

Je pense d'abord à l'adoption le 23 juillet 2014 du Règlement européen n° 910/2014, relatif à l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (*Electronic Identification, Authentification and trust Services*, eIDAS). Il a significativement contribué à façonner la solution française de CNIe.

Il y a introduit la notion d'interopérabilité entre les identités numériques des différents pays, la nécessité d'utiliser un langage commun. Le Règlement eIDAS a eu le mérite de clairement caractériser les niveaux d'identité numérique : faible, substantiel ou élevé, et d'en définir les critères d'appréciation.

En 2014 toujours, l'apparition de FranceConnect a posé un autre jalon de la création d'une identité numérique à la française. FranceConnect correspond au souhait de l'État d'ouvrir à l'ensemble de ses ressortissants la possibilité de s'identifier sur un serveur unique, afin d'accéder à des services publics en ligne. Ce serveur fédère les identités numériques, il favorise lui aussi l'interopérabilité entre elles, standardise les critères d'identification des citoyens. À terme, conformément à la réglementation eIDAS, il jouera le rôle de nœud de connexion également pour des identités européennes qui, si elles y sont autorisées, pourront ainsi accéder à des services publics français.

Certes, la France a attendu le début de l'année 2019 avant d'entreprendre de définir précisément son modèle de CNIe et la manière dont elle y intégrerait la dimension d'identité numérique. La carte émise depuis le 15 mars 2021 applique les diverses spécifications, les choix et arbitrages qui sont intervenus depuis lors.

En obligeant les États membres à renforcer la fiabilité de leurs titres d'identité, l'Union européenne et sa réglementation ont joué un rôle de catalyseur. Le choix d'un mode électronique garantit le respect de ces contraintes de sécurité. Il permet de plus de transformer la carte nationale d'identité en vecteur de diffusion de l'identité numérique.

M. Romain Galesne-Fontaine. Soyons clairs, la situation actuelle ne résulte nullement d'un défaut de maîtrise technique. Avec de nombreux acteurs français, l'Imprimerie nationale possède celle de l'identité numérique. Dès 2012, à l'occasion de l'adoption de la loi relative à la protection de l'identité, qui prévoyait la mise en place d'une CNIe, nous étions prêts. La censure du Conseil constitutionnel en a retardé la réalisation.

Toutefois, depuis 2019 et l'essor de FranceConnect, nous comprenons que le succès d'une identité numérique ne repose pas uniquement sur un support ou la fourniture d'une telle identité. Pour qu'elle atteigne ses buts, les exemples européens nous montrent que l'identité numérique suppose de fournir avec elle tout un ensemble, ou « écosystème », de services qui répondent à des usages. FranceConnect nous a justement permis de réfléchir plus avant à cet aspect décisif, que nous avions auparavant qu'insuffisamment considéré.

Désormais, notre démarche embrasse toutes les dimensions nécessaires à la réussite du projet. Ce projet d'identité et de services numériques sécurisés s'avère d'autant plus ambitieux

qu'il concerne à terme une population de 67 millions de Français et un nombre proportionnellement élevé de connexions quotidiennes.

Mme Coralie Héritier. J'ajoute que dorénavant, à côté de la CNIe, l'identité, et même les identités numériques dérivées, gagnent en importance. Elles requièrent que nous nous projetions et poursuivions, notamment au sein du CSF, notre travail en commun avec les industriels de la sécurité.

Démocratisée, une identité numérique citoyenne et régalienne doit permettre d'accéder à un autre niveau de services, pour des usages courants. Je pense notamment à la possibilité de l'employer depuis un *smartphone*. Je suis d'accord pour dire que son utilisation dépendra de l'étendue des services auxquels elle donnera accès. Il nous faut faire en sorte que l'identité numérique interagisse avec son environnement. Isolée de lui, elle ne sert à rien. Au contraire, l'interopérabilité et une large connectivité avec des services numériques lui confèreront toute sa valeur.

M. Philippe Latombe, rapporteur. Force est de constater que dans l'administration même, le réflexe perdure qui consiste à demander systématiquement des photocopies de la carte d'identité. À ce jour, il reste impossible d'engager une action en justice, d'immatriculer une société au greffe du tribunal de commerce, d'ouvrir un compte bancaire, voire simplement d'actualiser le dossier client qui s'y rapporte, enfin d'engager nombre de démarches, par exemple auprès de la caisse d'allocations familiales ou des organismes de sécurité sociale, sans produire une copie papier recto-verso de la carte nationale d'identité. Selon les cas de figure, il s'y ajoutera la demande d'une copie de la fiche d'imposition, ainsi que d'un justificatif de domicile, autrement dit une facture d'eau, de gaz ou d'électricité.

L'utilité de l'identité numérique ne laisse aucun doute. Prouver sa majorité sur Internet en donne un autre exemple.

Mme Coralie Héritier. Les progrès que la CNIe amène avec elle font présager une évolution rapide dans le sens que nous souhaitons. L'autorité nationale de la sécurité des systèmes d'information (ANSSI) vient de publier un référentiel d'exigences applicables aux prestataires de vérification d'identité à distance (PVID).

Lorsque nous parlons d'écosystème, nous nous interrogeons sur la manière d'adopter, grâce aux technologies disponibles, des solutions qui répondent aux usages que vous décrivez. Des prescriptions réglementaires, des référentiels adaptés nous le permettent dans des conditions de sécurité et de confiance qui garantissent l'intégrité ainsi que la fiabilité des données, et empêchent l'usurpation d'identité. Tel est bien l'un des objectifs que la CNIe poursuit.

M. Romain Galesne-Fontaine. Vos exemples, M. le rapporteur, ne manquent pas d'intérêt. Ils montrent combien la fourniture d'une identité numérique, outre qu'elle constitue un enjeu sur le plan de la sécurité, représente, ou peu s'en faut, un chantier de transformation culturelle. Elle emporte la modification d'un certain nombre de processus administratifs. Au préalable, il nous appartient de nous figurer comment ces services peuvent évoluer à l'aune du numérique.

Nous voyons qu'il s'agit à présent de travailler concomitamment à la conception d'une identité sécurisée et de penser la relation à l'usager à l'ère du numérique. Ainsi dédoublé, l'effort requiert davantage de temps. Néanmoins, nous le pouvons considérer comme suffisamment avancé sur ces deux aspects pour affirmer que la CNIe, qui ouvre la possibilité

de lui associer une identité numérique, offre désormais un outil efficace en vue d'une amélioration à brève échéance des services mis à la disposition des usagers.

M. Philippe Latombe, rapporteur. Bien que la CNIe soit prête, les usages ne suivront pas immédiatement son entrée en vigueur. Il suffit que nous songions à la carte vitale en matière de sécurité sociale. Le réflexe n'est manifestement pas encore celui d'une identité numérique à part entière. Dans les prochaines années, nous aurons toujours besoin d'un titre d'identité physique. La fracture numérique existe dans notre pays. Quand même elles en disposeront, des personnes n'utiliseront pas l'identité numérique et lui préféreront l'élément strictement physique de la carte pour justifier de leur identité.

La remarque me conduit à revenir, après vous M. Galesne-Fontaine, sur les auditions que nous avons tenues la semaine passée. Quoique vous affirmiez le contraire, il me paraît en ressortir que l'ANTS ne dispose plus, faute d'un effectif suffisant d'experts, de la maîtrise totale du projet. Vous semblez avoir pris une forme d'ascendant sur l'agence.

Je l'illustrerai par un exemple : actuellement, l'ANTS recherche un chef de projet CNIe.

C'est pourquoi je vous pose sans détour la question de savoir si la CNIe se situe réellement à l'état de l'art du point de vue de la sécurité. Nombreux sont ceux qui prétendent le contraire et estiment qu'elle accuse un retard dans ce domaine. À leur avis, d'autres pays en proposent le même format depuis plusieurs années ; certains ont indiqué depuis une grosse dizaine d'années.

Je prolongerai ma question par celle-ci : que coûte à l'État la production de la nouvelle CNIe ?

M. Romain Galesne-Fontaine. Sur votre première question, je rappellerai que l'Imprimerie nationale aurait été en mesure de produire une carte en polycarbonate dès 2012. Tel en était le projet. Des cartes de ce type existent donc depuis longtemps.

Pour autant, le fait que la nouvelle carte d'identité utilise le même matériau que des titres sortis dix ou quinze ans plus tôt revient-il à dire qu'elle présente des sécurités en tous points identiques aux leurs ? Je le répète : la réponse est négative. Je vous la donne en ma qualité d'expert industriel de l'identité. À l'Imprimerie nationale, nous travaillons pour plus d'une trentaine d'États à travers le monde, nous produisons régulièrement des titres d'identité modernes qui s'appuient sur les dernières innovations.

La CNIe française ne s'écarte pas de cette exigence. Elle comprend par exemple un dispositif holographique tout à fait original qui, composé de nanomatériaux, se distingue de l'habituel hologramme.

Au surplus, je n'affirme pas seul que la CNIe correspond à l'état de l'art en matière de sécurité. Pensez-vous que les forces de l'ordre françaises et l'ANTS, qui en ont supervisé le projet, en auraient validé la réalisation s'il en allait autrement et si elles avaient constaté que la carte ne répondait ni à leurs besoins ni à leurs prescriptions ? Je répète ici que l'Imprimerie nationale leur a soumis une architecture de sécurité destinée soit à prévenir les tentatives de fraude, soit à atteindre des objectifs de contrôle de sécurité sur le titre. La décision finale de valider cette architecture ne lui revenait pas.

M. Philippe Latombe, rapporteur. Sous l'angle des spécificités techniques, le format de CNIe, tel qu'il existe aujourd'hui, applique-t-il l'ensemble des préconisations que les spécialistes de la police aux frontières et de la gendarmerie nationale ont formulées ?

M. Romain Galesne-Fontaine. L'Imprimerie nationale s'est vu prescrire ce que nous appelons des cibles de sécurité. Elle devait y ajuster la nouvelle carte d'identité qu'elle mettait au point. Pour les atteindre, notre expertise tant nationale qu'internationale, notre veille technologique permanente, nous ont permis de combiner des éléments innovants de sécurité avec des solutions aussi robustes qu'éprouvées.

Nous ne saurions condamner des techniques qui ont apporté la preuve de leur efficacité en matière de sécurité au seul motif de leur ancienneté. À ce jour, nous n'avons connaissance d'aucun phénomène de fraude massive réussie sur nos titres français en polycarbonate. Jouant leur rôle, les sécurités en place ont permis de détecter immédiatement, à l'occasion d'un contrôle, les rares tentatives de fraude.

Mme Coralie Héritier. J'ajoute que l'ensemble des acteurs qui interviennent dans l'élaboration de la carte française ont exporté les technologies qu'ils mettent en œuvre. Ailleurs qu'en France, des titres d'identité les utilisent. Elles se conforment aux exigences en vigueur, notamment aux normes européennes. En aucune façon une moindre rigueur ne s'y attache dans le projet français.

M. Romain Galesne-Fontaine. Une partie des sécurités des titres que l'Imprimerie nationale produit, qu'il s'agisse des permis de conduire, des titres de séjour ou de la nouvelle carte d'identité, correspondent à des sécurités réglementaires. L'Union européenne les impose.

M. Philippe Latombe, rapporteur. Nous pourrions aussi nous interroger sur le point de savoir si la France trouve systématiquement un intérêt à reprendre à son compte les technologies que d'autres États utilisent.

Pour ce qui a trait au refus de recourir à la photographie couleur, je vous avoue n'avoir toujours pas saisi la raison qui le motive. J'entends l'explication relative au rachat d'une entreprise française par une entreprise américaine. Néanmoins, quand j'interroge des experts, y compris parmi les forces de l'ordre, on m'explique que la photographie en noir et blanc pose un problème opérationnel aux agents sur le terrain et que la couleur lui serait préférable.

Or, nous nous retrouvons avec une CNIe qui contient une photographie en noir et blanc. Pourtant, nous possédons la technique de la couleur, que nous ne manquons pas d'exporter. Le représentant d'IDEMIA, que nous auditionnions le 1er avril dernier, nous a indiqué que son entreprise l'employait. Pour leur part, grâce à leur partenariat avec leur entreprise nationale Veridos, les autorités allemandes, comme celles d'autres pays, utilisent une photographie en couleur sur leur CNIe.

Vous nous signaliez qu'en France, la demande d'une photographie en noir et blanc, ou en tons de gris, émanait de l'ANTS. Du moins ne vient-elle pas des forces de l'ordre.

Je réitère par ailleurs ma question sur le coût de revient, pour l'État, de la CNIe. À quel montant ce coût s'élève-t-il, à l'unité et tout compris ?

M. Romain Galesne-Fontaine. Nous pourrons partager avec vous, M. le rapporteur, les informations relatives au coût de la CNIe à la condition indispensable que l'ANTS y donne préalablement son accord exprès. Dans l'immédiat, au cours d'une audition publique, je ne puis vous les communiquer pour d'évidentes raisons de confidentialité.

Mme Coralie Héritier. Sans me prononcer quant à l'intérêt d'une photographie en couleur sur un titre d'identité, je signalerai que la nouvelle CNIe donne aux forces de police des possibilités de contrôle supplémentaires. C'est par exemple le cas du cachet électronique visible. Il facilitera leur travail sur le terrain.

M. Yann Haguet. La carte d'identité française fait appel à trois types de sécurité.

Nous venons de discuter en détail des sécurités physiques. Comme M. Romain Galesne-Fontaine l'a indiqué, elles correspondent à celles en vigueur dans la majorité des pays. Ici, notre devoir consiste à observer les pratiques qui prévalent, tout en nous assurant de la maturité des solutions que nous intégrons à notre projet.

À l'autre bout de la chaîne, la puce apporte elle-même un certain nombre de sécurités. Entre les deux extrémités, le cachet électronique visible (CEV) offre un premier niveau de lecture et de contrôle automatisé.

Au total, la duplication des éléments de sécurité confronte les éventuels fraudeurs à autant de barrages contre leurs intentions malveillantes.

Revenons à la question de la photographie en couleur. Dans l'élaboration de la CNIe, pour chacun de ses composants, pour tout élément de sécurité, l'un des points essentiels tenait à l'exigence de diversifier nos fournisseurs. Comme nous l'avons précédemment expliqué, nous devions nous assurer de la disponibilité d'au moins deux sources d'approvisionnement.

Or, les techniques de gravure de photographies en couleur disponibles sur le marché présentent la particularité d'être toutes différentes entre elles. De plus, aucune n'a complètement démontré sa capacité à traiter des volumes de l'ordre de ceux qui intéressent la France. Jusqu'à présent, les projets qui y ont recouru trahissent ce que j'appellerai, courtoisement, une marge de progrès.

Sans remettre en cause vos témoignages de l'appréciation des forces de l'ordre, sachez que, parmi elles, des acteurs considèrent aussi que les dégradés de gris de la gravure laser donnent d'intéressants résultats en matière de contrôle et de détection des fraudes, là où les techniques en couleur peuvent pêcher en raison de caractéristiques différentes de sensibilité et de granularité de leur impression. Pour les forces de l'ordre, l'aspect essentiel du métier de contrôle consiste d'abord à se forger, à partir de l'image, une appréciation globale de points remarquables du visage, qu'elles comparent à la personne à qui elles font face. Elles n'analysent pas nécessairement le détail de la couleur. Assurément, il s'agit ici d'un débat d'experts et des avis divergents s'y feront toujours entendre.

En tout état de cause, la CNIe française ne saurait nourrir nul sentiment de malaise. Bien au contraire, il convient de reconnaître qu'elle intègre les meilleures techniques du moment, tant sous l'angle de sa sécurisation physique que du contenu de sa puce électronique. Peut-être y reviendrons-nous au cours de notre échange, c'est précisément dans cette puce que nous trouvons la base indispensable à la construction d'une identité numérique.

M. Philippe Latombe, rapporteur. Pour en terminer sur le problème de la couleur, je signale que les Allemands connaissent une problématique de volumes au moins comparables aux nôtres, voire supérieurs. Ils n'en utilisent pas moins une photographie en couleur.

À présent, évoquons en effet la puce de la CNIe, en particulier du point de vue de son évolution. La validité de la nouvelle carte court pendant dix ans. Une deuxième version en est-

elle prévue ? Dans l'affirmative, à quel horizon ? À l'inverse, le même titre est-il appelé à se maintenir en l'état pendant la décennie qui s'ouvre ?

Au sujet de la norme 105, vous avez, M. Galesne-Fontaine, fait valoir un manque de recul pour une intégration immédiate à la CNIe. Cependant, des usages de l'identité numérique nécessiteront vraisemblablement que cette norme, ou un équivalent, soit tôt ou tard mise en application. Ce constat suppose une évolution du titre d'identité. Comment alors procéderons-nous ?

M. Yann Haguet. M. Galesne-Fontaine l'a souligné, la CNIe est d'ores et déjà configurée et prête pour l'identité numérique. Son système d'exploitation (*operating system*) et sa puce comprennent deux compartiments.

L'un, le compartiment ICAO, équivaut à celui d'un passeport. Il contient l'identité régalienne. À la manière d'un passeport, il remplit la fonction que la réglementation européenne définit, celle qui permet à un citoyen de franchir les frontières internes à l'Europe. Son contrôle peut être automatisé.

L'autre, le compartiment d'identité numérique, respecte un standard français issu, entre 2019 et 2020, de l'intervention conjointe de l'ANTS, de France Identité numérique et des industriels, dont l'Imprimerie nationale, Thales et IDEMIA. Son déploiement ne suppose plus que son activation et, par un canal séparé et sécurisé, la transmission d'un code PIN à chaque citoyen français. Une fois activé, ce conteneur n'autorisera en effet son accès en lecture qu'à la condition que le possesseur du titre renseigne son code confidentiel.

Dès à présent, la CNIe contient donc un volet identité numérique. Il ne reste qu'à mettre en œuvre l'infrastructure d'un fournisseur d'identité. Ce fournisseur pourra être public ou, si la réglementation le prévoit, privé. Son rôle consistera à administrer l'identité numérique associée à la CNIe. Il interviendra par exemple si le titulaire de l'identité victime d'un vol souhaite révoquer sa carte.

Ainsi que le mentionnait Mme Coralie Héritier, il sera également possible d'étendre, ou « dériver », l'identité numérique associée à la CNIe à son utilisation à partir d'un *smartphone*. Une telle extension permettra deux types d'authentification pour des services publics ou privés.

La première, une identification de niveau élevé, au sens que lui donne la définition du Règlement européen eIDAS, se destine aux transactions les plus importantes, telles que l'ouverture d'un compte bancaire, la souscription à un emprunt bancaire ou la délivrance d'une procuration de vote. Elle impliquera que l'usager approche la carte de son téléphone et saisisse son code confidentiel.

La seconde servira à des transactions d'un niveau de sécurité substantiel. On estime qu'elles recouvrent 80 ou 85 % des cas de figure. Elles ne nécessitent pas de recourir à la carte, l'identité numérique dérivée contenue dans le téléphone étant alors jugée suffisante.

Vis-à-vis d'un fournisseur d'identité, ces possibilités techniques impliquent que la réglementation lui permette d'utiliser le conteneur, ou compartiment, siège de l'identité numérique. Le fait qu'une décision rapide d'activation de ce conteneur puisse intervenir dès la délivrance de la CNIe requiert encore que son possesseur dispose de la faculté de s'enregistrer sans délai auprès d'un fournisseur d'identité. L'activation de l'identité numérique s'effectuera soit à partir d'un ordinateur personnel, après renseignement du code confidentiel,

soit auprès d'un guichet public. Par l'intermédiaire de FranceConnect, elle rendra possible la connexion aux portails publics ou privés qui auront autorisé son utilisation.

Le fait que le service FranceConnect fonctionne déjà, qu'il ait récemment obtenu de l'ANSSI la reconnaissance d'un niveau élevé d'authentification au sens du Règlement eIDAS, qu'il définisse le format dit « pivot » des données à transmettre par chacun des fournisseurs d'identité, permettra à l'avenir un recours des plus étendus à l'identité numérique issue de la CNIe.

M. Philippe Latombe, rapporteur. Si je vous entends bien, la CNIe laissera à son détenteur le choix de son fournisseur d'identité, un fournisseur public ou privé ?

M. Yann Haguet. Techniquement, rien du moins ne s'y oppose. Il reviendra à la réglementation de préciser le dispositif, les conditions d'utilisation du conteneur et celles de l'agrément donné aux fournisseurs d'identité.

M. Philippe Latombe, rapporteur. La semaine dernière, Mme Valérie Péneau, inspectrice générale de l'administration, directrice du programme interministériel France Identité numérique, nous expliquait que, de son point de vue, aucun marché ne se dessinait pour une identité numérique privée. L'identité numérique lui paraissait ressortir exclusivement à la mission régalienne de l'État.

Votre analyse contredit apparemment la sienne. Pensez-vous qu'il y ait place pour un marché privé de l'identité numérique ?

M. Yann Haguet. Je m'appuierai sur l'expérience d'IN Groupe à l'exportation. M. Romain Galesne-Fontaine le signalait, nous déployons l'identité numérique ailleurs qu'en France, notamment à Monaco. Notre pratique montre qu'une place existe tant pour un fournisseur d'identité régalien, autrement dit public, que pour des fournisseurs privés ou semi-privés.

Un fournisseur d'identité public garantit le niveau de sécurité le plus élevé. Il s'accorde avec le principe de gratuité qui, souvent, concerne la fourniture de l'identité ainsi que l'accès aux services publics.

Il n'en reste pas moins envisageable d'autoriser un système de fournisseurs privés ou semi-privés. Il existe dans certains pays. En France, La Poste, voire IN Groupe, pourraient revêtir cette qualité. Un tel système implique que les fournisseurs d'identité s'engagent à donner l'accès à des portails de services publics, au moins à un niveau de sécurité substantiel, par exemple, pour le paiement des impôts. Ils se rémunèrent alors auprès des fournisseurs de services en ligne qui recourent à l'identité numérique.

M. Romain Galesne-Fontaine. Pour compléter ce propos, j'estime qu'il serait opportun de reprendre les différentes études économiques qui ont concerné le sujet, à la lumière de la survenue de la crise sanitaire et des conséquences qu'elle entraîne. Sans doute ne mesurons-nous pas pleinement combien la situation que nous vivons depuis plus d'un an provoque une accélération de la mutation numérique de nos modes de vie, qu'il s'agisse des usages privés ou des pratiques professionnelles.

Nous pensions déjà nécessaire de fournir une identité numérique dans un cadre à la fois public et privé. Désormais, il nous apparaît que le bouleversement que nous connaissons rend d'autant plus attractif un marché pour des fournisseurs d'identité privés. La décision en

revient à l'État. L'agrément qu'il donnera aux fournisseurs d'identité veillera à leur respect des règles de sécurité et de confidentialité des données personnelles.

Au sein de l'Imprimerie nationale, nous reconnaissons à ces données un caractère unique. Elles nous paraissent requérir l'emploi des plus hauts niveaux de protection. En dernière analyse, du strict respect de cette exigence dépend l'adhésion des usagers aux systèmes d'identité numérique. Les usagers doivent recevoir la double assurance que leur fournisseur d'identité n'utilisera pas leurs données personnelles à leur insu et qu'il se révélera en mesure de protéger ces données contre toute atteinte extérieure.

M. Philippe Latombe, rapporteur. La fourniture de l'identité numérique correspond-elle à un segment d'activité sur lequel IN Groupe entend se positionner ?

M. Romain Galesne-Fontaine. En effet, avec la perspective d'accélérer la mise en place de l'identité numérique en France, nous nourrissons l'ambition d'en devenir un fournisseur. Nous interviendrions en complément de solutions d'identité régaliennes. Les technologies dont nous disposons nous permettraient d'assurer, en application du Règlement eIDAS, le niveau substantiel de sécurité.

M. Philippe Latombe, rapporteur. Vos propres ressources internes vous suffiraient-elles ? Pourriez-vous vous passer de partenariats ?

M. Romain Galesne-Fontaine. Je vous le confirme. Nos moyens nous autorisent à prétendre à un statut de fournisseur agréé d'identité numérique, pour autant que l'État crée ce statut.

Mme Coralie Héritier. Comprenons que tous les acteurs auront une place à prendre. En tant que telle, l'identité citoyenne ne peut exister seule.

Sur un plan numérique, l'identité est susceptible de revêtir différentes formes. Il s'agira par exemple d'un certificat électronique. Cependant, dans les divers services et applications auxquels elle donnera accès, il lui faudra être associée à d'autres facteurs d'identification.

L'idée de multiplier ces facteurs gagne en importance. Le code confidentiel en est un. Il importera qu'ils se complètent entre eux, afin d'atteindre le plus haut niveau possible de confiance.

Ne concevons pas la CNIe comme le sésame unique qui répondrait à l'ensemble des besoins. Un véritable écosystème de l'identité numérique existe déjà. Il tend à s'étoffer, il se développe avec l'évolution des techniques. Pour leur part, les usages connaissent une croissance considérable. Ils requièrent l'emploi des facteurs multiples d'authentification que j'évoquais.

De ce point de vue, la gestion des identités numériques, celle de leur cycle de vie, s'avérera fondamentale. Une réglementation devra l'étayer. Le rôle d'en contrôler le respect incombera vraisemblablement à l'ANSSI.

M. Philippe Latombe, rapporteur. Nous accusons un tel retard sur le sujet de l'identité numérique qu'il est à craindre qu'il ouvre une porte, comme dans d'autres domaines avec les Google, Apple, Facebook, Amazon et Microsoft (GAFAM), à des entreprises privées qui imposent leurs propres standards. Non sans raison, des collègues parlementaires ont adressé un courrier au Premier ministre dans lequel ils mettent en exergue l'ampleur de notre retard. En comparaison d'autres États européens, celui-ci est indéniable.

M. Yann Haguet. Je souhaite apporter un complément de réponse sur la question de la maintenance du titre d'identité. Vous nous interrogiez sur le devenir de la CNIe pendant les dix années de sa validité et sur ses éventuelles versions successives.

N'importe quel titre d'identité représente un état des techniques de sécurité disponibles à un instant précis. Il s'ensuit une forme de course-poursuite, aux échéances plus ou moins rapprochées dans le temps, avec les fraudeurs. L'apport de sécurités supplémentaires peut devenir nécessaire à tout moment.

Par le passé, avec les titres à sécurités purement physiques, la fréquence de nos interventions s'espaçait dans le temps. Dorénavant, l'emploi de l'électronique, de systèmes d'exploitation, d'algorithmes cryptographiques, conduit à la resserrer. En quelque sorte, le temps s'accélère.

Pour les cartes prochainement émises, IN Groupe a proposé à l'ANTS le recours à un gestionnaire du cycle de vie du titre et des versions de son système d'exploitation. Il lui reviendrait de procéder, en cas de besoin, à des opérations de maintenance de sécurité, de modifier ou d'activer des algorithmes de cryptographie, voire d'intégrer de nouvelles applications informatiques.

Un titre d'identité qui comprend une dimension électronique doit évoluer avec son environnement. Garantir que la CNIe assure sa fonction, y compris pour sa partie identité numérique, impose au minimum de respecter les contraintes du référentiel général de sécurité (RGS). Ces dernières prévoient le changement régulier des clés utilisées pour cryptographier les données et le processus qui permet d'y accéder.

Par ailleurs, en accord avec l'ANTS et sous sa direction, des phases de décision de nouvelles versions du titre interviendront. Elles correspondront à l'émergence de besoins ou usages, ainsi que vous le mentionniez M. le rapporteur, ou tiendront compte de celle d'autres règles ou contraintes européennes. La situation s'en est présentée avec l'actuel titre de séjour français. L'ancienneté de sa version dite V1 remonte à moins de dix ans. Voilà six mois, il a fallu redéfinir une nouvelle version, afin d'intégrer les évolutions que l'Union européenne imposait.

Un titre d'identité vit. Le principe de départ veut que son possesseur le détienne pendant dix années. Sauf cas exceptionnel, durant toute cette période, sa version initiale ni son apparence globale ne font l'objet d'une remise en cause radicale. En revanche, de réguliers changements de clés et, si nécessaire, des adaptations et mises à jour de sécurité en accompagnent l'existence.

Les versions des titres évoluent donc. Il est ainsi permis d'imaginer, d'ici à quelque temps, une version V2 de la CNIe.

M. Philippe Latombe, rapporteur. Quelle entité assurera-t-elle le suivi ? IN Groupe jouera-t-il ce rôle ?

M. Yann Haguet. Tout changement dans le système d'exploitation, toute introduction d'un élément de sécurité destiné à y combler une faille, suppose des échanges et l'activation de mécanismes dans un réseau plutôt fermé d'acteurs.

La décision d'opérer des changements relève du ressort de l'ANTS, en coordination avec l'ANSSI.

Selon les circonstances, nous pouvons envisager, soit une modification qui ne concerne que les futurs titres, soit à l'inverse une modification qui affecte l'ensemble de ceux déjà distribués, soit, dans les situations les plus graves, un remplacement pur et simple de la carte.

Certains cas de figure justifieront un retour de l'usager devant les services de sa mairie. Moyennant des authentifications et des contrôles, des changements de clés mineurs pourront s'effectuer depuis un ordinateur personnel ou un *smartphone*.

M. Philippe Latombe, rapporteur. Soumettez-vous la CNIe à des tests de vulnérabilité, aussi bien physiquement qu'électroniquement, afin de la protéger contre les atteintes des faussaires ou des pirates informatiques ?

M. Yann Haguet. Nous réalisons évidemment de tels contrôles de sécurité. Chacun des industriels parties prenantes à la conception de la carte, en particulier de sa puce électronique et de son système d'exploitation, participe sous le contrôle de l'ANSSI et de laboratoires indépendants à un processus de qualification et de certification. Ce processus doit démontrer que la carte remplit les critères de sécurité attendus, que ses mécanismes de défense atteignent le niveau de complétude et de sécurité souhaités.

J'ajoute que nos fournisseurs ont l'obligation de répéter régulièrement leurs cycles de certification et de prouver que leurs solutions demeurent valides au cours du temps. À cette occasion, l'identification d'un risque peut conduire à l'ajout d'un correctif.

Le fait que le titre inclut de l'électronique et des systèmes d'exploitation emporte qu'un nombre accru de mécanismes entrent en ligne de compte dans sa maintenance.

M. Philippe Latombe, rapporteur. Je vous poserai une question en rapport avec la commande publique. Comment IN Groupe favorise-t-il l'émergence ou la consolidation d'acteurs, ainsi que leur excellence sur la scène internationale, sur les aspects de sécurité des titres d'identité ?

Certes, IN Groupe assure directement, en interne avec ses compétences, un certain nombre de réalisations, mais il en sous-traite également d'autres. Comment vous y prenez-vous ? Privilégiez-vous d'abord vos propres compétences avant que de vous adresser à l'extérieur ? Passez-vous systématiquement des appels d'offres ou procédez-vous de gré à gré ?

M. Romain Galesne-Fontaine. Je l'ai dit, le rôle de l'Imprimerie nationale est celui d'un intégrateur agnostique des meilleures technologies du marché. Même s'il possède certaines d'elles en propre, IN Groupe ne travaille pas isolément. Dans le cas de la CNIe, il compte plus d'une quinzaine de partenaires privés, dont le groupe Atos, associés à la fourniture des différents composants du titre.

Il nous tient à cœur d'animer ce que je qualifie d'écosystème. Chaque année, notamment pour l'élaboration des titres d'identité sécurisés, l'Imprimerie nationale recourt aux services de plus de 400 sociétés réparties sur l'ensemble du territoire français. Les retombées économiques en représentent plusieurs dizaines de millions d'euros.

Quant aux titres sécurisés, nous respectons systématiquement le cadre légal et réglementaire de la commande publique auquel nous sommes soumis. La sélection de l'intégralité des composants stratégiques de la CNIe n'a pas échappé au principe. Ici, la procédure de la commande publique nous permet d'appliquer scrupuleusement notre obligation de diversification de nos sources d'approvisionnement par le choix d'au moins deux

fournisseurs pour chacun des composants. Nous garantissons ainsi à l'État sa capacité à délivrer sans interruption ses titres d'identité pendant toute la durée de leur validité.

M. Philippe Latombe, rapporteur. S'agissant de la CNIe, il nous intéresserait que vous nous précisiez les valeurs de la répartition entre ce qu'IN Groupe réalise directement et ce qu'il sous-traite par la commande publique.

Dans l'immédiat, je n'attends pas de réponse chiffrée, vous nous l'apporterez plus tard. Vous nous signaliez précédemment que, sur les aspects de coûts, il vous fallait obtenir l'accord préalable de l'ANTS. En revanche, peut-être pouvez-vous déjà nous communiquer un ordre d'idée de la répartition ?

M. Romain Galesne-Fontaine. Pour des raisons de sécurité, je ne puis non plus indiquer le nombre exact des composants stratégiques qui entrent dans la fabrication de la CNIe. Je vous disais qu'il avoisinait une quinzaine. L'Imprimerie nationale n'en fournit que deux. Vous obtenez là un aperçu assez clair du ratio qui vous intéresse.

M. Philippe Latombe, rapporteur. À ceci près que l'étendue des prestations respectives et de leurs montants, qu'en l'état nous ignorons, est susceptible de relativiser considérablement la pertinence d'une conclusion hâtive.

Sous l'angle de la souveraineté, prêtez-vous une attention particulière à la nationalité de vos fournisseurs potentiels ? Au contraire, ce critère n'entre-t-il pas en ligne de compte ?

M. Romain Galesne-Fontaine. L'ensemble de nos achats respectent les principes de la commande publique. Nous agissons dans la stricte limite que ces principes nous fixent.

Parmi les fournisseurs des composants de la CNIe, nombreux sont ceux d'origine française ou européenne.

M. Philippe Latombe, rapporteur. Voulez-vous aborder un sujet que nous n'aurions pas encore évoqué ?

M. Yann Haguet. Il convient de souligner combien la réussite du déploiement de l'identité numérique renvoie aux usages, à leurs approches, aux conditions de création d'un écosystème. Sans doute l'expérience de Mme Coralie Héritier au sein du groupe Atos et du CSF des industries de sécurité lui permet-elle de se forger une opinion sur la probabilité du succès de l'entreprise ?

Mme Coralie Héritier. Je vous avouerai ma perplexité quant à la raison pour laquelle la mission d'information m'a invitée à intervenir devant elle. Je note que la plupart des questions ont concerné l'Imprimerie nationale. J'aurais souhaité un débat à l'objet moins resserré. Cependant, je vous ai exprimé mon point de vue sur ce que l'identité numérique citoyenne devrait recouvrir.

Chez Atos, nous retenons une acception large des questions numériques ; nous considérons la transformation numérique en général. À notre sens, l'identité numérique en forme certes un pilier, mais non le seul. Il faut lui ajouter toutes les infrastructures, le *cloud* de confiance à qui il revient de supporter le volume des données, les outils, concevoir au surplus des socles mutualisés à destination de l'administration publique. À la vérité, bien des sujets nous permettraient d'étendre la discussion au-delà de la seule CNIe.

M. Philippe Latombe, rapporteur. La semaine dernière, lors de notre audition de Mme Valérie Péneau, nos questions relatives aux usages des identités numériques ont trouvé peu d'écho. En toute franchise, notre interlocutrice fut assez évasive. Il semblerait que nous ignorions encore ce que seront ces usages.

Pour l'heure, l'utilisation de l'identité reste plus physique que numérique. Sans doute appartient-il à cet égard à l'administration française de changer de paradigme et de mode de fonctionnement. L'identité s'inscrit au cœur de la transformation numérique de l'État. Nous nous en ouvrirons à Mme Amélie de Montchalin, ministre de la transformation et de la fonction publique.

Madame Coralie Héritier, vous semblez établir un lien entre *cloud* et identité numérique. Voici qui nous surprend. Pouvez-vous nous en préciser la nature ? Le premier conserverait-il les données de la seconde ?

Mme Coralie Héritier. Afin de traiter des volumes importants de données relatives à l'identité numérique, la chaîne de confiance utilise des technologies, notamment des certificats électroniques. Privé, le *cloud* que j'évoque ne correspond pas à la définition que l'on donne ordinairement de ce terme. Pour ma part, j'entends par lui des infrastructures fiables, dont des opérateurs de services de confiance, dûment habilités, se chargent de la gestion. Elles permettent d'industrialiser tous les éléments de sécurité nécessaires à la création des identités numériques. En définitive, elles ne diffèrent pas significativement des techniques d'industrialisation du *cloud* au sens strict.

Pour une société comme Atos, partie au projet européen d'infrastructure de données GAIA-X, développer des capacités de calcul importantes, anticiper les évolutions post-quantiques à venir, lui sont indispensables pour se maintenir à l'état de l'art.

M. Philippe Latombe, rapporteur. Quel usage de l'identité numérique voyez-vous pour la France ? Quand y deviendra-t-elle la norme ?

Mme Coralie Héritier. Tout dépend d'abord du type d'identité dont nous parlons. De nombreuses identités numériques circulent déjà, qui ne sont pas d'un niveau de sécurité élevé et qui servent à accéder à un système d'information ou à une application en ligne. Certains en utilisent quotidiennement plusieurs. Elles sont entrées dans les mœurs.

À présent, il importe de mener une action de pédagogie sur l'usage d'une identité numérique d'un niveau de sécurité d'abord substantiel, puis élevé. Cette démarche favorisera la confiance des citoyens, elle-même primordiale pour le développement des usages numériques du quotidien.

L'évolution de l'identité numérique, sa démocratisation, reposent ensuite sur la facilitation de son usage.

L'authentification multifactorielle existe déjà. La directive européenne sur les services de paiement (DSP2) du 13 janvier 2018 l'a imposée pour toute transaction de plus de 30 euros. Chacun possède de même un code confidentiel attaché à sa carte bancaire. L'accès à des services en ligne sensibles ou à des données personnelles pourra encore tirer profit de l'authentification faciale, couplée à d'autres facteurs.

À mon sens, la banalisation de l'usage d'identités de niveaux de sécurité substantiel et élevé devrait devenir la règle assez rapidement.

M. Romain Galesne-Fontaine. Il nous faut réfléchir à des solutions d'identité qui soient inclusives. Personne ne saurait rester en marge de l'évolution en cours. Nous pensons que l'identité constitue un droit, non un service. L'universalité, l'effectivité, de ce droit supposent un langage compréhensible par tous, accessible y compris à ceux qui se tiennent fort éloignées de l'univers du numérique.

C'est pourquoi, nous nous attachons à mettre en place des systèmes qui s'appuient sur des procédures connues, tel que le code PIN. Nous travaillons de plus à l'élaboration de parcours d'usages aussi simples que possible, par exemple avec la dérivation de l'identité de la CNIe vers le téléphone portable.

Nous contenter de numériser des procédures fondées sur les documents du centre d'enregistrement et de révision des formulaires administratifs (Cerfa) équivaudrait à un échec. Aujourd'hui, l'occasion s'ouvre d'œuvrer à la simplification des parcours administratifs. La perspective en anime l'intention de nombreux experts engagés dans les programmes de transformation numérique de l'État.

M. Philippe Latombe, rapporteur. Je soulèverai une réserve. Nous ne contournerons pas l'obligation, sinon de conserver des guichets physiques, du moins de prévoir un substitut à la partie strictement numérique.

La situation actuelle en matière de délivrance et modification des cartes grises est éloquente. Pour la moindre demande, la numérisation intégrale de la procédure, l'impossibilité de se présenter devant les services de la préfecture, transforme un incident mineur en d'inextricables complications. Il en résulte une forte insatisfaction, notamment chez des personnes peu coutumières du numérique. En parallèle, nous assistons à l'émergence d'une économie de l'immatriculation des véhicules : partout en France, des officines apparaissent aux alentours des services préfectoraux, qui proposent aux administrés d'effectuer à leur place les démarches officielles d'immatriculation.

M. Romain Galesne-Fontaine. Je vous rejoins. Nous ne nous représentons pas un monde à 100 % numérique.

M. Philippe Latombe, rapporteur. Précisément, comment jugez-vous les expériences d'États qui ont opté pour un modèle intégralement ou presqu'intégralement numérique ? Il s'agit certes d'États plus petits que la France : l'Estonie, ou Israël qui a dans une large mesure numérisé les aspects d'identité et de santé. Néanmoins, gagnerions-nous à nous en inspirer ?

M. Romain Galesne-Fontaine. Les critères de réussite que nous avons identifiés dans ces pratiques de pays étrangers tiennent d'abord au rapprochement et à la coordination des divers acteurs et de leurs environnements spécifiques. En France, dans son essence même, le CSF des industries de sécurité participe d'une logique équivalente, avec l'objectif de fournir une identité, ou des identités, numériques sécurisées et de services.

En second lieu, un travail de pédagogie vis-à-vis de la population intervient. Il faut décrire les services que l'identité apporte. Il faut aussi expliquer que l'identité numérique a pour fonction de protéger, non de contrôler. Sans ce travail préalable, nous nous confronterons de nouveau en France aux débats que nous avons connus en 2012 sur les projets de CNIe et d'identité numérique, autour de la préservation des libertés fondamentales.

Non seulement nous devons insister sur ce que nos dispositifs respectent la législation et la réglementation en matière de données personnelles, mais sur ce qu'en outre ils contribuent à leur protection et offrent de nouveaux services.

Inclusion, pédagogie, travail avec un écosystème sur des services immédiatement utiles à la vie de nos concitoyens, nous engagerons, me semble-t-il, dans la bonne direction.

Mme Coralie Héritier. Dans les pays qui ont choisi, ou peu s'en faut, le « tout numérique », la politique a pris appui sur quatre piliers : les infrastructures nationales, la diffusion des outils numériques dans tous les milieux et âges de la population, les financements dédiés à l'innovation et au développement des technologies tournées vers les usages, enfin l'identité numérique.

Nous pouvons nous en inspirer, même si chaque pays possède son histoire et son organisation administrative propres. En France, afin de réussir notre transformation numérique, je pense que nous aurions intérêt à promouvoir une forme de transversalité des actions que nos différents ministères mènent dans ce domaine. Nous poserions opportunément des socles communs, en particulier sur les aspects de cybersécurité et d'identité numérique. Le partage d'applications informatiques, la coordination à tous les niveaux de l'État et de l'administration me paraissent essentiels. Pour leur part, les solutions techniques existent.

La coordination des services de l'État en matière numérique contribuerait de plus significativement à l'effort de pédagogie auprès du public.

Le CSF des industries de sécurité a exprimé son souhait de poursuivre sans relâche le dialogue entre les industriels et l'État. Dans l'élaboration des solutions numériques, particulièrement à l'occasion du plan de relance, nous apportons, en tant qu'industriels, notre contribution et notre vision. En retour, nous nous nourrissons des enjeux et ambitions de l'État.

M. Yann Haguet. Je partage cet avis sur l'importance de la coordination et de l'inclusion. J'ajouterai celle, clé à mes yeux, de la mixité entre les acteurs publics et privés.

À l'étranger, souvent les réussites sont apparues dès lors que l'État a favorisé l'implication du secteur privé et de la société civile dans la promotion de l'identité numérique, quand même celle-ci demeurait attachée à une identité régalienne. Je pense par exemple à la Pologne. L'intervention du monde bancaire y a joué un rôle majeur. Pareillement, en Belgique, l'essor des usages de l'identité numérique a suivi l'initiative d'un consortium d'utilisateurs.

Le CSF des industries de sécurité a pour vocation d'encourager les échanges et la coordination entre les acteurs publics, les fournisseurs de services et les industriels. Cette coordination s'avère décisive quand, vous l'avez compris, la CNIe nous ouvre dès à présent le champ à une identité numérique.

M. Philippe Latombe, rapporteur. En somme, nous disposons avec elle du réceptacle de l'identité numérique.

Audition, ouverte à la presse, de M. Jérôme Notin, directeur général du groupement d'intérêt public Action contre la Cybermalveillance (GIP ACYMA)
(8 avril 2021)

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. M. Jérôme Notin, la structure dont vous êtes le directeur général, plus connue sous le nom de cybermalveillance.gouv.fr, correspond au dispositif national d'assistance aux victimes de cybermalveillance, et de sensibilisation des publics au risque numérique. Dans nos travaux sur les enjeux de cybersécurité, votre audition s'inscrit à la suite de celles de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et de la fédération française de la cybersécurité.

Nous souhaitons échanger avec vous sur l'état de la menace cyber, les modalités d'accompagnement des victimes, déployées par votre dispositif, et la nécessité de promouvoir une véritable culture de l'hygiène numérique auprès des acteurs publics et privés.

M. Philippe Latombe, rapporteur. Je commencerai par vous poser une question rituelle : comment définiriez-vous la souveraineté numérique ? J'aimerais que vous nous présentiez ensuite le groupement Action contre la Cybermalveillance (ACYMA), son actualité et son fonctionnement. Comment soutenez-vous les victimes de cyberattaques ? Comment collaborez-vous avec les acteurs publics également chargés de la question en France, mais aussi en Europe ? Des pratiques de coopération ou d'échanges ont-elles cours avec vos homologues dans d'autres États membres de l'Union européenne ?

Je souhaiterais en outre établir un bilan de la menace en revenant sur les principaux types d'attaques répertoriés, leurs évolutions durant la crise sanitaire et le profil des victimes qui se tournent vers vous.

J'aimerais dans un second temps que nous prenions du champ par rapport à la cybersécurité. Le gouvernement vient d'annoncer qu'il lui consacrera des moyens renforcés dans sa stratégie nationale cyber. Comment percevez-vous cette initiative ? J'aimerais que vous évoquiez votre tout nouveau label ExpertCyber, attestant l'expertise numérique de prestataires cyber.

Enfin, je voudrais aborder la diffusion d'une culture cyber au sein de la société. Quel regard portez-vous sur le degré de sensibilisation à la cybersécurité, aussi bien des entreprises et des administrations publiques, dont les collectivités territoriales, que des citoyens ?

Je voudrais pour conclure évoquer la formation en compétences cyber, puisqu'un campus cyber devrait bientôt voir le jour avec l'appui, entre autres, de l'ANSSI. Comment se positionne la France sur ces enjeux par rapport à d'autres pays ? Devrions-nous compléter notre offre de formation dans certains segments en particulier ou combler des lacunes que vous auriez identifiées ?

M. Jérôme Notin, directeur général du groupement d'intérêt public Action contre la Cybermalveillance (GIP ACYMA). La souveraineté implique selon moi de disposer de produits inspirant à juste titre la confiance. La création de votre mission prouve en soi qu'il reste de véritables besoins à couvrir dans ce domaine. On trouve bien quelques acteurs français et européens de cybersécurité, mais il subsiste de nombreux « trous dans la raquette ». Ni les

particuliers, ni les entreprises, ni les collectivités territoriales ne disposent pour l'heure d'une offre à cent pour cent souveraine. Un travail considérable reste à mener.

La France a la chance de disposer de compétences entrepreneuriales et d'expertise technique en cybersécurité, mais qui ne se rencontrent pas forcément. Je ne peux qu'engager à poursuivre vos travaux pour que, dans les années à venir, la France jouisse enfin d'une souveraineté nationale en ce domaine.

Notre groupement d'intérêt public s'est donné pour objectif de faire savoir à nos concitoyens (collectivités territoriales, entreprises ou particuliers) qu'en cas de problème de cybersécurité, notre plateforme « .gouv.fr » est en mesure de les aider.

Trois missions nous ont été confiées suite à la présentation de la stratégie nationale pour la sécurité du numérique en 2015 :

– L'assistance aux victimes passe essentiellement par la plateforme cybermalveillance.gouv.fr. Toute victime qui s'y connecte suit un parcours défini : elle renseigne son profil, puis répond à quatre ou cinq questions permettant d'établir un diagnostic, après quoi, soit nous lui fournissons des conseils, si elle est en mesure de les appliquer de manière autonome, soit nous la dirigeons vers internet-signalement.gouv.fr ou la plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS), puisque nous avons vocation à constituer un fichier unique. Surtout, quand une assistance technique s'avère nécessaire, nous proposons une mise en relation avec des prestataires de proximité. Notre plateforme en référence aujourd'hui un millier, en mesure d'aider aussi bien des particuliers que des entreprises ou des collectivités territoriales, victimes de l'une des 45 formes de cybermalveillance répertoriées. Nous avons réussi à glisser dans le dossier de presse complétant les annonces du président de la République la création du label ExpertCyber, dont bénéficient aujourd'hui 55 prestataires aux compétences vérifiées.

– Dès la création de notre dispositif en 2017, nous avons produit beaucoup de contenus de sensibilisation, sous licence ouverte, dès que leur format le permettait. Une partie de nos publics, notamment les collectivités territoriales, nécessite encore de prendre conscience du risque cyber. Certains élus se croient à l'abri d'une attaque, du fait qu'ils ne détiennent pas de propriété intellectuelle ou de fichier clients, donc de données susceptibles *a priori* d'intéresser des pirates. Ils se trompent. Pendant le premier confinement, en avril et mai 2020, nous avons, grâce à France Télévisions, à TF1 et au groupe Canal+, diffusé de brefs messages de sensibilisation.

– Notre troisième mission est la mise en place d'un observatoire de la menace, afin d'analyser celle-ci aussi exhaustivement que possible, et va s'accélérer en 2021. Le ministère de la justice a d'ores et déjà mis à notre disposition un agent dans cette optique. Personne ne sait aujourd'hui qui visent les attaques, ni ce qu'elles coûtent à l'économie française, à l'État ou à l'Europe.

M. Philippe Latombe, rapporteur. Que les confinements nous ont-ils appris en matière de sensibilisation ? Avez-vous noté une amélioration de la prise de conscience au fil du temps ? Les entreprises, et je pense plus à celles de petite taille qu'aux grands groupes sans doute mieux avertis, utilisent-elles plus volontiers des réseaux privés virtuels (VPN) ? Ont-elles compris qu'il ne fallait pas se servir d'un ordinateur personnel à des fins professionnelles ?

Les collectivités territoriales qui lancent en ce moment même de nombreux projets de villes intelligentes (ou *smart cities*) y intègrent-elles la cybersécurité dès le départ ? Ou n'y

songent-elles qu'à la fin, après avoir pris conscience qu'elles ont oublié de se doter d'une « porte blindée » ?

Que s'est-il passé mardi dernier sur les espaces numériques de travail et les plateformes d'école à la maison ? Il était peut-être maladroit de rejeter la faute de l'incident sur OVH. Les attaques russes contre le centre national d'enseignement à distance (CNED) semblent brandies comme excuse, peut-être en partie à juste titre. N'y recourt-on pas toutefois par facilité, pour masquer les défaillances de l'architecture du site ?

M. Jérôme Notin. Je garderai pour moi ce que m'inspire cet incident et me contenterai de rappeler les faits : une recrudescence de connexions légitimes à la plateforme du CNED et à ses sites satellites a fait peser sur les serveurs une forte charge. Le ministre a évoqué des cyberattaques de l'étranger. La chaîne sécurité des systèmes d'information (SSI) du ministère m'a confirmé la réalité d'une attaque par déni de service (DDoS). Le ministère a déposé plainte auprès du parquet chargé de la cybercriminalité.

Je me permettrai une digression : s'il existe en France un axe d'amélioration de la cybersécurité, et donc, de la souveraineté qui en découle, il réside auprès du parquet. Par chance, celui-ci a pris conscience de la nécessité de disposer de magistrats spécialisés. D'une remarquable compétence, ils accomplissent un travail extraordinaire. Malheureusement, ils ne sont que trois. Il en faudrait bien plus.

M. Philippe Latombe, rapporteur. Combien selon vous ?

M. Jérôme Notin. La question s'adresse peut-être plus aux magistrats eux-mêmes. J'estime qu'une dizaine d'entre eux auraient encore fort à faire pour que la justice se saisisse des affaires comme il se doit, identifie les auteurs des infractions et y mette un terme. Un parquet renforcé serait en mesure de traiter aussi bien la petite cybercriminalité (les arnaques visant les particuliers) que les attaques étatiques contre les infrastructures régaliennes de la France, sans oublier celles dont le CNED a fait les frais.

M. Philippe Latombe, rapporteur. Ces magistrats disposent-ils d'outils judiciaires adaptés ? Au-delà de la question des effectifs, sont-ils capables de réagir rapidement ou, à l'inverse, de s'accorder du temps quand une investigation le requiert, et de mobiliser les experts indispensables aux enquêtes ?

M. Jérôme Notin. Je les crois en mesure, par le biais de l'ANSSI, de saisir les experts les mieux à même de les seconder. Ils disposent en outre du meilleur policier de France en matière de rançongiciel, en sa qualité d'assistant technique du parquet.

En revanche, les outils juridiques pourraient être améliorés. Nous cherchons à créer un groupe de travail réunissant des représentants des ministères de la Justice et de l'Intérieur, des opérateurs, des associations de victimes et des fédérations professionnelles, pour traiter de l'hameçonnage. Nous estimons les tentatives d'hameçonnage insuffisamment prises en compte, sans doute faute d'un outil législatif adapté, alors que cette forme de cyberdélinquance sert de point de départ à nombre d'autres attaques.

De faux sites de vente de gel et de masques ont proliféré en pleine pénurie, pendant le premier confinement. On connaît l'extraordinaire capacité d'adaptation des cybercriminels. Dès le soir du 16 mars, notre plateforme a constaté une multiplication par cinq des tentatives d'hameçonnage, dénoncées par des victimes cherchant auprès de nous de l'aide. Nous avons formé à leur répression la direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF), qui ne pouvait hélas que couper l'accès à ces plateformes

frauduleuses. Dix nouvelles autres les remplaçaient aussitôt. La justice ne s'est pas saisie de ces affaires, faute d'un outil législatif permettant d'identifier les coupables. La loi a évolué depuis. Mais cette absence d'une législation adaptée pose un réel problème aux collectivités territoriales et aux entreprises victimes de tentatives de récupération des mots de passe en vue d'installer un rançongiciel qui bloquera leur activité. Empêcher les cybercriminels de récupérer des données, personnelles, professionnelles ou institutionnelles marquerait un formidable bond en avant, en limitant considérablement leurs capacités de nuisance.

M. Philippe Latombe, rapporteur. Les collectivités territoriales réservent-elles toujours un budget à la protection contre la menace cyber ou n'y songent-elles qu'après coup ? Les intégrateurs, souvent sélectionnés par appel d'offres, jouent-ils bien leur rôle ? Angers, par exemple, souffre encore des conséquences d'une attaque, au point qu'elle ne parvient plus à gérer ses horodateurs sur la voie publique.

M. Jérôme Notin. Je me permettrai de remarquer qu'il ne suffit pas à une collectivité territoriale de prendre d'entrée de jeu en compte la cybercriminalité pour y échapper.

Il en va des collectivités territoriales comme des entreprises : leur maturité sur le sujet apparaît corrélée à leur taille. Les plus grandes ont bien conscience du risque, notamment grâce à l'ANSSI. Ce n'est toutefois pas le cas des petites ou moyennes collectivités territoriales, qui ne songent parfois même pas à protéger les données de leurs administrés, n'imaginant pas que celles-ci puissent intéresser les cybercriminels.

Le premier confinement a contribué à une prise de conscience liée à la quantité de collectivités territoriales visées par des rançongiciels. Leurs victimes sont passées de la sixième place sur notre liste de demandes d'assistance en 2019 à la première aujourd'hui. Ces demandes d'assistance ont augmenté de plus de moitié de la part des collectivités territoriales, contre une hausse d'un quart seulement de la part des entreprises et un recul de 85 % de la part des particuliers. Nous assistons donc à un déplacement de la cybercriminalité.

L'été dernier, lors d'une visioconférence, un employé d'une collectivité territoriale m'a remercié, car notre campagne de sensibilisation sur France Télévisions avait enfin convaincu les élus, auxquels il réclamait des fonds depuis des années, de lui allouer un budget cybersécurité.

Une première prise de conscience a donc eu lieu, qu'on ne doit peut-être pas tant à nos actions qu'à la quantité de victimes de cyberattaques. Il nous reste encore du travail et nous nous y attelons. Le plan de relance va permettre d'élever le niveau de sécurité des collectivités territoriales. On ne peut que s'en réjouir.

M. Philippe Latombe, rapporteur. Estimez-vous suffisantes les mesures du plan de relance en matière de cybersécurité ?

M. Jérôme Notin. Les intégrateurs ne jouent pas le jeu : ils n'assurent qu'un service minimum au moindre coût, afin d'obtenir le marché. Ils ne prennent pas assez d'initiatives, alors que les collectivités territoriales sont en droit de les consulter avant la rédaction d'un dossier technique. Ils devraient inciter celles-ci à prendre dès le départ en compte la cybersécurité, plutôt que de l'ajouter au projet fini à la manière d'une rustine. Je les estime moralement tenus d'alerter les élus sur ce sujet. Il en coûtera à ceux-ci ce que vaut une assurance prémunissant contre les catastrophes.

Le plan de relance prévoit d'allouer 136 millions d'euros à l'ANSSI, dont une partie bénéficiera aux collectivités territoriales, dans la mesure où cette somme nous permettra, entre

autres, de mieux sensibiliser à la cybersécurité celles de petite taille. Nous nous efforcerons en 2021 de répondre au plus près à leurs besoins en adaptant à leur intention nos contenus. Nous avons d'ailleurs déjà participé l'an dernier, avec la banque des territoires, à une campagne de sensibilisation des élus au moyen d'un guide. Nous y avons ajouté quatre vidéos illustrant la cybercriminalité par des exemples concrets, comme l'inondation d'un stade de foot suite à une intrusion sur un réseau, ou le dérèglement de feux de circulation obligeant à poster des gendarmes à chaque carrefour.

M. Philippe Latombe, rapporteur. La somme que vous évoquez servira-t-elle directement à protéger les collectivités territoriales ou à dresser une liste de leurs besoins, qui les obligera ensuite à investir ? Beaucoup de collectivités territoriales s'attendent à recevoir de quoi financer leur cybersécurité sans pour autant savoir comment s'attaquer au problème.

M. Jérôme Notin. Nous allons leur indiquer leurs failles et les moyens d'y remédier, sous le pilotage de l'ANSSI. Notre groupement d'intérêt public (GIP) a la chance d'être présidé par M. Guillaume Poupard, le directeur général de l'ANSSI, qui a mis sur pied notre dispositif avec le ministère de l'Intérieur. Nous collaborons au quotidien avec l'ANSSI, à un niveau à la fois stratégique et opérationnel.

M. Philippe Latombe, rapporteur. Les petites et moyennes entreprises (PME) et les très petites entreprises (TPE) se soucient-elles aujourd'hui suffisamment de cybersécurité ?

M. Jérôme Notin. Les grandes entreprises s'en préoccupent assez, grâce à l'ANSSI et à la loi de programmation militaire, par exemple, mais pas les PME. Leurs patrons, à l'instar des élus que j'évoquais tout à l'heure, pensent ne présenter aucun intérêt pour les cybercriminels, puisqu'ils ne possèdent ni fichier clients ni propriété intellectuelle. Les événements de 2020 ont pourtant démontré que la menace cyber touchait tout le monde. Bloquer le réseau d'une PME prend quelques heures à un cybercriminel, qui en retire plusieurs milliers d'euros. Même si peu d'entreprises « passent à la caisse », et tant mieux, une telle opération reste rentable.

Nous œuvrons main dans la main avec des syndicats et des fédérations professionnelles, la confédération des petites et moyennes entreprises (CPME) et le mouvement des entreprises de France (MEDEF). Cette menace réelle n'est toutefois pas encore suffisamment prise en compte. Reconnaissons que notre message manque d'attrait : nous suscitons des craintes et incitons à la dépense. Ceci dit, une telle dépense prépare l'avenir. Nous devons songer que, si la France s'améliore en matière de cybersécurité par rapport à ses voisins, alors les criminels cibleront d'autres pays.

M. Philippe Latombe, rapporteur. Le rôle de sous-traitant de grands groupes assumé par certaines TPE facilite-t-il la diffusion par le haut d'une culture de la cybersécurité ? Je songe à Airbus adressant par exemple à une TPE de Vendée, chargée de fabriquer un morceau d'aile, des plans protégés, amenant ainsi l'entreprise à se moderniser et, du même coup, à se prémunir des cyberattaques.

Pourriez-vous nous communiquer un ordre de grandeur des entreprises victimes de cyberattaques qui, indépendamment de leur taille, paient les rançons ?

M. Jérôme Notin. Quelques grandes entreprises ont bel et bien pris des initiatives hélas encore limitées. La filiale aéronautique et spatiale a lancé l'initiative vertueuse d'Aerospace Valley, à l'impact réel, pour aider les PME critiques de la chaîne d'approvisionnement à mieux se sécuriser.

Cette filière a par ailleurs créé une communauté de confiance : dès lors qu'un des grands donneurs d'ordre a validé le niveau de sécurité d'un prestataire, les autres n'ont plus à s'en préoccuper.

J'ai discuté récemment avec un ami responsable de la sécurité des systèmes d'information (RSSI) chez un intégrateur. Depuis un an, ses tâches se limitent à remplir des dossiers de conformité cyber pour les commerciaux. Chaque donneur d'ordre souhaite en effet désormais qu'un tel dossier accompagne la moindre proposition, comme aux États-Unis. Mon ami RSSI en a perdu de vue son métier.

Songeons aussi au ministère des armées, membre de notre dispositif depuis quelques mois. Il a bien compris que la base industrielle de la technologie de défense constitue la clé de la sécurité et qu'il doit accompagner les entreprises concernées via la direction du renseignement et de la sécurité de la défense (DRSD). Même les PME détentrices d'un savoir-faire spécifique n'ont pas toujours conscience des risques contre lesquels elles doivent se protéger.

M. Philippe Latombe, rapporteur. Le grand public est-il aujourd'hui conscient de ce que représente la menace cyber ? Une culture s'est-elle développée à tous les échelons de la société ?

M. Jérôme Notin. L'ANSSI et les ministères de l'intérieur, des finances, de la justice et des armées, à l'origine de notre dispositif, nous ont confié la mission de lancer une grande campagne de sensibilisation, sur le modèle de celle de la sécurité routière. Je ne doute pas qu'un jour, nous la mènerons à bien. Il ne nous manque que des moyens financiers, mais il suffit d'une volonté politique pour les débloquer.

Il est impératif de se rendre compte que, si le numérique apporte de nombreux bénéfices, son usage requiert par ailleurs une grande vigilance.

Depuis plusieurs mois, des « cybercrapules » appellent des particuliers, soi-disant pour les accompagner dans la création de leur compte professionnel de formation. Leur objectif est en réalité de récupérer le mot de passe associé au profil de la victime pour vider ce compte à l'aide de complices. Pour gagner la bataille, il suffirait que les Français comprennent qu'aucun organisme public ne les contactera jamais en leur demandant leur mot de passe. Le remboursement des victimes a coûté douze millions d'euros à l'État *via* la Caisse des dépôts et consignations (CDC). La justice s'est saisie de l'affaire, cependant il suffirait d'investir un peu pour éviter d'entrer dans des frais de cet ordre.

Dans le même esprit, depuis des années, la fraude à la réparation informatique coûte des millions d'euros tous les mois aux Français qui croient leur ordinateur infecté par un virus, parce que s'ouvre à l'écran une fenêtre les orientant en réalité vers un centre d'appels vendant de faux antivirus. Je suis convaincu que chaque euro investi dans des actions de sensibilisation en rapporterait à terme plusieurs dizaines.

M. Philippe Latombe, rapporteur. Nous avons auditionné la semaine dernière l'Imprimerie nationale et ATOS au sujet de l'identité numérique, à laquelle pourrait servir de réceptacle la carte d'identité électronique équipée d'une puce. Un code secret lui sera associé, comme à une carte bancaire. Selon vous, nos concitoyens sont-ils suffisamment bien informés des cybermenaces pour éviter tout vol de leur identité ?

M. Jérôme Notin. La CDC a réagi à l'incident relatif au compte professionnel de formation en imposant, en préalable à toute commande de formation, une activation du compte

Franceconnect, c'est-à-dire une authentification numérique par un organisme public. Cette excellente réponse technique, opérationnelle, devrait permettre de résoudre les problèmes d'hameçonnage. Reste encore à la généraliser rapidement.

Les cybercriminels, redoutablement imaginatifs, innovent en permanence. En ce moment circule sur les réseaux sociaux une chaîne de messages incitant à leur diffusion auprès d'autres utilisateurs. Leurs auteurs laissent espérer à leurs destinataires que ceux-ci remporteront des entrées gratuites dans un parc d'attractions fêtant son anniversaire, alors qu'ils ne cherchent en réalité qu'à collecter des données personnelles. Beaucoup de jeunes mordent à l'hameçon dans l'espoir de remporter ces invitations et de les offrir à leurs proches. Quelques mois plus tard leur parvient un e-mail émanant en apparence, mettons de la Fnac, de fait très active dans la lutte contre ce type d'arnaques. Ce message, récapitulant les données qu'eux-mêmes ont préalablement communiquées, leur signale la livraison d'une commande qu'ils n'ont bien sûr jamais passée. La possibilité leur est laissée d'en obtenir le remboursement par un simple clic conduisant à une page aux couleurs de la Fnac où leur est alors demandé leur numéro de carte bancaire. Voilà comment les cybercriminels enrichissent progressivement leurs fichiers.

Le recours à l'identité numérique résoudra certains problèmes mais pas celui-là, par exemple.

M. Philippe Latombe, rapporteur. Une anecdote me revient à l'esprit : une chaîne de livraison de repas à domicile, en guise de poisson d'avril, a envoyé des « factures » de livraison de pizzas d'un montant de près de 450 euros. Les clients ayant cru à un piratage vous l'ont-ils signalé ?

M. Jérôme Notin. Non, je n'étais pas au courant.

M. Philippe Latombe, rapporteur. Je m'interrogeais sur l'existence d'un réflexe qui amènerait à vous déclarer systématiquement les situations anormales.

M. Jérôme Notin. En tant que dispositif d'assistance, nous avons pour vocation de fournir de l'aide. Beaucoup déclarent auprès de nous les arnaques dont ils sont victimes. J'y vois l'une des forces de notre dispositif. Ceci étant, comme nous n'employons en tout et pour tout que treize personnes, nous ne communiquons pas trop sur cet aspect de notre rôle. Nous formons une équipe trop réduite pour échanger en direct avec les 1,2 million d'utilisateurs qui se sont connectés à notre plateforme en 2020. Ce chiffre correspond d'ailleurs à une véritable explosion de la fréquentation de notre site pendant le confinement. Quand la forme de cybermalveillance à laquelle nos usagers ont été confrontés n'a pas encore été répertoriée par nos services, ils peuvent la signaler par un message « JNPT » (je n'ai pas trouvé). C'est ainsi que nous avons eu vent des arnaques au compte professionnel de formation. Nous nous sommes rapidement saisis du problème avec la CDC, qui opère la plateforme de gestion de ces comptes. Cependant, les grands sites privés de commerce ne prennent pas toujours aussi rapidement les devants. Certains ne traitent pas correctement la fraude.

La Française des jeux nous a indiqué que, depuis une dizaine d'années, des particuliers reçoivent un courrier les informant d'un gain à une loterie à laquelle ils n'ont jamais joué. La recrudescence récente du phénomène nous a incités à communiquer sur le sujet prochainement. Jusqu'à une personne sur cinq se laisse prendre en versant parfois des centaines de milliers d'euros à des « avocats » dans l'espoir de récupérer leur gain pourtant fictif.

Expliquer à l'ensemble de nos concitoyens qu'il n'est pas logique qu'ils donnent de l'argent pour percevoir une somme qu'ils auraient gagnée à un jeu auquel ils n'ont pas participé relève d'une action de sensibilisation restant encore à mener.

M. Philippe Latombe, rapporteur. Avez-vous des homologues dans d'autres pays d'Europe ? Si oui, coopérez-vous ? Disposent-ils d'outils qui vous manqueraient ?

M. Jérôme Notin. Nous n'avons pas d'homologues. Tous les États disposent d'une agence nationale équivalente de l'ANSSI et tous mènent des actions de sensibilisation auprès de l'ensemble des publics. En revanche, notre capacité à mettre en relation quasi immédiate des victimes avec des prestataires de proximité en mesure de les aider est unique au monde.

Nous sommes ainsi en mesure d'aiguiller presque tout de suite une collectivité territoriale, mettons en Vendée, vers une entreprise qui se chargera de réinstaller son système d'exploitation après avoir identifié la façon dont s'y sont introduits les attaquants. Je rappelle à ce propos qu'il importe de conserver des preuves des méfaits des cybercriminels avant d'y remédier.

Nous échangeons avec nombre de pays, francophones ou non, proches ou lointains, dans l'idée de leur fournir gratuitement notre outil sous licence libre, pour qu'ils reproduisent notre action sur leur territoire. Derrière notre plateforme œuvre tout un *back-office* qui, à l'aide d'un arbre de décisions, pose des diagnostics et fournit des conseils adaptés aux 45 formes de cybermalveillance que j'évoquais tout à l'heure. Nous proposons aujourd'hui plus de 400 conseils personnalisés. Nous menons presque au quotidien un travail d'adaptation et de reformulation en fonction de ce que nous rapportent les victimes *via* les messages « je n'ai pas trouvé ». Nous complétons régulièrement nos questionnaires et ajoutons de nouvelles formes de cybermalveillance à notre liste.

Les chiffres que nous mettons en avant, les retours de nos utilisateurs et les signalements auprès du parquet d'attaques que n'avaient même pas détectées les services du ministère de l'intérieur, parce que toutes les victimes ne portent pas plainte et qu'il faut de toute façon du temps, après un dépôt de plainte, pour analyser celle-ci et se rendre compte si tel phénomène est isolé ou non, prouvent l'intérêt de notre action. L'adoption d'une taxonomie commune et d'une même définition des incidents de sécurité nous apparaît comme une démarche tout à fait sensée.

Rendre disponible un outil sous forme de logiciel libre requiert un considérable travail, de documentation notamment. J'espère que nous aurons l'occasion de le mener à bien au cours des mois ou des années à venir.

M. Philippe Latombe, rapporteur. Auriez-vous une idée du nombre d'entreprises victimes de rançongiciels qui acceptent de payer ?

M. Jérôme Notin. On cite souvent des proportions allant de 20 à 30 %. Il doit être possible d'améliorer la situation en agissant sur les prestataires qui facilitent le paiement des rançons. Des réflexions sont menées par le Trésor public, le parquet et le ministère de l'intérieur pour leur compliquer la tâche.

J'ai conscience de former là un vœu utopique, mais il faudrait faire passer le message que, si plus personne ne paie de rançon, ce type d'attaque cessera, quitte à ce que les criminels recourent ensuite à d'autres formes de malveillance. En attendant, l'impact de leurs méfaits aura quand même été réduit.

M. Philippe Latombe, rapporteur. Pourriez-vous revenir sur le label que vous avez créé en précisant sa place dans l'écosystème de la cybersécurité ? Que garantit-il exactement ? En quoi se distingue-t-il des autres labels ? Apporte-t-il des assurances complémentaires ? Recoupe-t-il certaines certifications existantes ?

M. Jérôme Notin. Notre label a été créé pour garantir à la victime d'une cyberattaque que l'entreprise vers laquelle elle se tournera possède un niveau d'expertise technique en cybersécurité vérifié. Notre plateforme référence 1 000 prestataires de proximité, allant de petits commerces en régions, en mesure de réinstaller le système d'exploitation d'un particulier exposé à un incident de sécurité, à des Prestataires d'audit de la sécurité des systèmes d'information (PASSI) ou des Prestataires de détection d'incidents de sécurité (PDIS) qualifiés par l'ANSSI.

Quand nous avons créé ce label avec les représentants des prestataires de proximité, notre objectif consistait à garantir leurs compétences en cybersécurité aux PME qui auraient recours à eux. Nous avons établi un référentiel avec l'Association française de normalisation (AFNOR) en vue de réaliser un audit des prestataires. Cet audit se base sur une documentation, d'une part, de leurs réponses aux incidents de sécurité et, d'autre part, de leurs actions de sécurisation auprès de leurs clients. Un examen technique d'une vingtaine de minutes comportant 30 à 40 questions le complète. L'obtention du label dépend de la note obtenue.

Les représentants de la profession nous ont signalé la nécessité d'évaluer leur capacité à sécuriser des systèmes, au-delà de leur aptitude à gérer les incidents. Nous avons ainsi identifié sur l'ensemble du territoire 55 entreprises en mesure d'éviter aux PME et aux collectivités territoriales de tomber dans le piège d'une cyberattaque. Nous ambitionnons de faire passer leur nombre à 200 voire à 400. Nos entreprises et nos collectivités territoriales doivent pouvoir s'appuyer sur un réseau de prestataires de confiance capables de leur fournir une solution rapide aux incidents, mais aussi d'élever globalement le niveau de sécurité cyber.

M. Philippe Latombe, rapporteur. Les entreprises se prémunissent-elles suffisamment contre les risques de cyberattaques ? Que proposent en ce domaine les compagnies d'assurance et qu'en coûte-t-il ? Utilisent-elles les protections contre la cybercriminalité de la même manière qu'elles se sont servies des portes blindées, c'est-à-dire comme d'un levier de diffusion, en l'occurrence d'une culture de la cybersécurité ? Autrement dit : les compagnies d'assurance refusent-elles de couvrir les entreprises et collectivités territoriales mal protégées ? Leur imposent-elles des tarifs supérieurs ?

M. Jérôme Notin. Les compagnies d'assurance disposent là d'un formidable levier. Nous nous réjouissons d'ailleurs de compter la fédération française de l'assurance parmi les membres fondateurs de notre GIP. Trois assureurs nous ont rejoints depuis. Nous travaillons avec eux sur la partie « observatoire » du dispositif. Il leur faut des chiffres précis pour concevoir des polices d'assurance efficaces.

Des progrès restent à réaliser, tant de l'offre elle-même que de l'adhésion des victimes potentielles. Nous avons besoin, d'un côté, d'une offre cyber adaptée au marché et, de l'autre, de clients conscients que les assureurs ne couvriront que les risques résiduels. Notre label intéresse de ce fait aussi les assureurs, désireux de s'appuyer sur des prestataires capables d'évaluer le niveau de cybersécurité de leurs clients. Une assurance cyber bien conçue ne coûte que quelques centaines d'euros à une PME.

Nous demandons en somme aux assureurs de nous aider à les aider. Nous ignorons quels chiffres au juste ils souhaitent connaître. Nous œuvrons en outre avec eux à déterminer comment communiquer de manière anonyme sur le coût des cyberattaques et le temps

d'immobilisation potentiel des systèmes pour qu'une offre adaptée voie le jour et que les entreprises se prémunissent de leur côté contre les risques les plus courants.

M. Philippe Latombe, rapporteur. Les assurances tentent-elles, non sans opportunisme, de conquérir un nouveau marché ou se rendent-elles compte qu'elles risquent de perdre des clients si elles s'avèrent incapables de protéger les entreprises de leur portefeuille, à présent numérisées et, partant, plus vulnérables, car exposées à des risques jusque-là inexistants ?

M. Jérôme Notin. Leur démarche participe sans doute des deux approches que vous évoquez, et peut-être plus de la première mais, en un sens, peu importe, d'autant que la distinction n'apparaît pas nette.

Le marché des polices cyber représente 40 millions d'euros, soit une part infime du marché des assurances. L'apparition, dans les prochaines années, de véhicules autonomes entraînera une diminution du chiffre d'affaires des assureurs, ces véhicules présentant des risques d'accident moindres, sauf, évidemment, si des pirates prennent le contrôle de l'ensemble du système de pilotage. Il semble donc logique que les assureurs compensent le manque à gagner sur les polices d'assurance automobile en proposant de couvrir les risques cyber. Tant qu'on observe une adéquation entre la nouvelle offre et les besoins, on peut considérer cette évolution comme vertueuse.

Il faut en tout cas que des assureurs couvrent le risque cyber, quelle que soit leur motivation. J'espère que notre observatoire nous permettra sous peu de fournir le nombre exact des PME en France incapables de se relever d'attaques cyber. Le maire d'Angers a eu l'intelligence de communiquer sur la situation de sa ville, mais il n'est pas le seul confronté à ce type de problème.

Un directeur général dans une commune importante me confiait récemment que, depuis une attaque en novembre, son service ne fonctionnait plus qu'au cinquième de sa capacité nominale, l'empêchant de servir les administrés. La création de polices d'assurance adaptées pourrait remédier à de telles difficultés en imposant par exemple de réaliser des sauvegardes déconnectées.

M. Philippe Latombe, rapporteur. L'incendie d'OVH a montré que bien peu d'entreprises et de collectivités hébergées sur leur *cloud* disposaient d'un plan de reprise d'activité (PRA) ou d'un plan de continuité d'activité (PCA), pourtant à la base de toute protection d'un système informatique. Cet incident a contraint certains hôpitaux incapables de se passer de l'informatique à fonctionner en mode dégradé.

Les organisations professionnelles, dont certaines font partie de votre GIP (la CPME et le MEDEF), relaient-elles aujourd'hui l'information auprès de leurs adhérents ? La fonction publique, dans son versant hospitalier décentralisé notamment, est-elle suffisamment avertie du risque cyber ? A-t-elle assez conscience de sa vulnérabilité pour vous solliciter afin de prendre les mesures adéquates ?

M. Jérôme Notin. L'actualité a montré l'absence totale de scrupules des cybercriminels, n'hésitant pas à entraver le fonctionnement d'un établissement de santé, quitte à empêcher le personnel soignant d'assurer sa mission, à la seule fin de récupérer de l'argent. Cela, les hôpitaux l'ont compris.

Le problème qui se pose est celui de la dette technique des collectivités territoriales, à présent tenues de compenser leur manque d'investissement en cybersécurité. Tant qu'elles n'y

seront pas parvenues, elles resteront vulnérables. Par chance, la France dispose d'une agence nationale de la santé, et l'ANSSI réalise un travail fabuleux d'accompagnement après les incidents. Je garde confiance en notre capacité à rattraper rapidement notre retard, grâce au plan de relance qui s'est concentré sur le domaine hospitalier.

Dès le début du premier confinement, les fédérations professionnelles et le MEDEF nous ont contactés, parce que leurs adhérents ne savaient pas comment mettre en place le télétravail de manière sécurisée. Nous leur avons très vite fourni des conseils dans un article largement relayé sur la mise en place du télétravail en situation de crise.

En tant que plateforme « .gouv.fr », nous nous sommes octroyé le droit, par souci de pragmatisme, de rappeler, en cas d'utilisation d'un ordinateur personnel à des fins professionnelles, quelques principes de base, tels que la mise à jour d'un antivirus, l'installation de pare-feu locaux ou d'un VPN.

Le MEDEF, la CPME, la fédération Syntec et la fédération des entreprises du bureau et du numérique (EBEN) se sont empressés de relayer cet article, destiné à l'origine aux patrons de PME, preuve d'une véritable demande de leur part. La CPME, qui vient d'engager quelqu'un d'extrêmement volontaire en matière de cybersécurité, se montre depuis longtemps très active dans notre dispositif.

Les fédérations assument donc leur rôle. Reste à savoir si leurs adhérents saisissent bien le message.

Mon contact à la CPME m'a confié que, lorsque, deux ou trois ans plus tôt, il proposait aux adhérents locaux des formations à la cybersécurité, celles-ci ne suscitaient aucun intérêt. Aujourd'hui, à l'inverse, la cybersécurité apparaît bien comme le premier sujet de préoccupation des patrons de PME.

La prise de conscience du risque s'améliore, or elle marque une première étape indispensable avant d'entreprendre le nécessaire pour s'en prémunir.

M. Philippe Latombe, rapporteur. La formation des experts en cybersécurité et des RSSI vous semble-t-elle aujourd'hui d'un niveau satisfaisant ?

M. Jérôme Notin. Les formations actuellement dispensées en France, en informatique en général et en cybersécurité en particulier, sont d'un très bon niveau. Les écoles produisent des diplômés aux profils parfaitement adaptés aux besoins. Ceci dit, ils sont loin d'être assez nombreux.

Le manque ne porte pas seulement sur les ingénieurs aux compétences pointues mais aussi sur les techniciens. L'idée reste prégnante en France qu'un métier technique est « sale ». Il nous faudrait plus de personnel intermédiaire de niveau bac +2 qui mette les mains sur le clavier pour opérer directement les infrastructures.

Les écoles d'ingénieurs, qui préparent leurs étudiants à devenir chefs de projet après deux ou trois ans de carrière, leur annoncent qu'ils oublieront dès lors l'aspect technique de leur métier, ce que je trouve scandaleux. Chacun doit pouvoir continuer à s'occuper de questions techniques, quel que soit son âge. Prétendre qu'il faudrait renoncer à la technique pour devenir RSSI n'a pas de sens et relève selon moi d'une déformation française, dégradante, qui plus est, pour l'image de la technique. D'autant que celle-ci correspond quand même à un besoin fondamental de l'entreprise, au même titre que sa stratégie ou son

organisation. Il est nécessaire que des personnes compétentes administrent les réseaux au quotidien et vérifient les règles des pare-feu.

M. Philippe Latombe, rapporteur. Selon vous, qui devrait former des techniciens ? Des instituts universitaires de technologie (IUT) ?

M. Jérôme Notin. On pourrait valoriser les brevets de technicien supérieur (BTS). Ayant moi-même quitté l'université depuis un certain temps, j'ai quelque peu perdu de vue l'organisation des études supérieures. Je songeais à des formations de niveau bac+2 ou bac+3. En France perdure une culture de l'élitisme, qui explique ce défaut de personnel qualifié de niveau intermédiaire.

Il faut aussi se dire qu'un ingénieur peut encore « s'amuser » à 45 ans en s'occupant de technique. L'état d'esprit qui prévaut, et que je ne suis malheureusement pas en mesure de changer, me paraît dommageable. Des étudiants frais émoulus d'une école d'ingénieurs m'expliquaient, voici quelques années, qu'un emploi de consultant leur semblait plus noble qu'un poste d'administrateur de réseaux. Je ne partage pas ce point de vue.

M. Philippe Latombe, rapporteur. Que pensez-vous du futur campus cyber ? Comment concevez-vous son rôle et son futur impact ? Le voyez-vous comme une belle vitrine à même d'attirer des talents, comme un dispositif efficace qu'il conviendra de généraliser ? Le jugez-vous trop centralisé, même s'il est prévu qu'il essaime en région ? Faudrait-il le dupliquer au niveau européen ?

M. Jérôme Notin. J'y vois avant tout une opportunité extraordinaire. Sur le papier au moins, il m'apparaît comme un dispositif fabuleux. Réunir en un même lieu les acteurs industriels, universitaires, étatiques, les *start-up* et les investisseurs, permettrait à la France de réaliser, en matière de cybersécurité, les formidables progrès dont elle a besoin.

Cela étant, il faut, pour que ce campus réussisse, que tout le monde joue le jeu, ce qui ne s'annonce pas simple. Michel Van Den Berghe, qui porte le projet, parvient aujourd'hui, ce dont je me réjouis d'ailleurs, à faire passer à de grands groupes industriels concurrents le message qu'ils travailleront ensemble à des projets communs.

De grands groupes industriels du secteur de la défense mettent pour l'heure au point, indépendamment les uns des autres, des dispositifs de sécurité spécifiques destinés à renforcer un système d'exploitation commun. S'ils mutualisaient leurs ressources en personnel, en s'adjoignant le concours d'un universitaire, autrement dit s'ils œuvraient de concert, ils gagneraient en efficacité. Or tel est l'objectif du campus.

Notre GIP aura la chance de rejoindre ce campus. Notre observatoire de la menace se construira en son sein. Si j'ai pleine confiance en ce projet, je doute quand même un peu de la capacité des industriels à travailler ensemble. L'ANSSI sera heureusement très présente. Il faudra peut-être plus de temps qu'on ne l'imagine aujourd'hui à ce cyber campus pour porter ses fruits.

Je vous livrerai mon avis personnel sur ses déclinaisons régionales. Il existe déjà de remarquables initiatives à Saint-Quentin-en-Yvelines, dans le Nord et la région Provence-Alpes-Côte d'Azur (PACA). Des déclinaisons régionales du campus réalisant un maillage du territoire permettraient de franchir une étape cruciale.

Nous répétons depuis tout à l'heure que les principales victimes de la cybermalveillance ne sont autres que les PME et les collectivités territoriales, par nature

ancrées dans les territoires. Disposer dans le tissu économique local de structures en mesure de déployer des technologies cyber adaptées nous donnera les moyens de réaliser en cinq ans des progrès tels que 2021 nous apparaîtra, avec le recul, comme une période moyenâgeuse en matière de cybersécurité.

M. Philippe Latombe, rapporteur. Souhaiteriez-vous aborder d'autres sujets que nous aurions omis ?

M. Jérôme Notin. Nous avons consacré beaucoup d'énergie à la rédaction de notre rapport d'activité, que nous allons publier dans quelques jours. Fruit d'un travail collectif, il récapitule des chiffres relatifs à la cybermenace, son analyse et ses tendances les plus récentes. N'hésitez pas à consacrer un peu de temps à sa lecture. J'invite enfin ceux qui assistent à cette audition à nous suivre sur les réseaux sociaux et à s'inscrire à notre lettre d'information.

M. Philippe Latombe, rapporteur. Pourriez-vous nous faire parvenir ce rapport ? Nous l'ajouterons en annexe et disposerons ainsi de plus amples éléments pour nourrir notre réflexion.

M. Jérôme Notin. Je n'osais pas vous le proposer, mais je vous le transmettrai avec plaisir.

M. Philippe Latombe, rapporteur. Je vous souhaite bon courage pour la création de l'observatoire, qui devrait en effet permettre de mieux suivre l'évolution de la cybermenace d'un point de vue aussi bien qualitatif que quantitatif.

Audition, ouverte à la presse, de M. Guillaume Vassault-Houlière, président-directeur général et cofondateur, et Mme Rayna Stamboliyska, vice-présidente en charge des affaires publiques et institutionnelles, de Yes We Hack
(8 avril 2021)

Présidence de M. Philippe Latombe, rapporteur.

M. Philippe Latombe, président et rapporteur. Nous auditionnons aujourd'hui M. Guillaume Vassault-Houlière, président-directeur général et cofondateur, et Mme Rayna Stamboliyska, vice-présidente de la gouvernance et des affaires publiques, de Yes We Hack.

Yes We Hack est une plateforme de mise en relation d'entreprises avec des hackers éthiques, créée en 2013. Spécialiste de la prime aux bogues (ou *bug bounty*), c'est-à-dire la chasse aux vulnérabilités, elle regroupe la première communauté européenne d'experts en cybersécurité.

Le gouvernement a récemment fait appel à Yes We Hack préalablement au lancement de l'application TousAntiCovid, qui portait à l'origine le nom de StopCovid.

J'aimerais que vous nous présentiez Yes We Hack, son actualité, son mode de fonctionnement, son processus de sélection de *hackers* et ses relations avec sa clientèle d'entreprises. Entretenez-vous des relations commerciales régulières avec des acteurs publics tels que l'État, les collectivités territoriales ou les hôpitaux ? Comment appréhendent-ils les enjeux de sécurité numérique et leurs solutions ? Manifestent-ils de l'intérêt pour le type d'offres que vous proposez ?

Je souhaiterais ensuite prendre du champ par rapport à la cybersécurité proprement dite. Le gouvernement prévoit d'y consacrer des moyens renforcés dans sa stratégie nationale « cyber ». Comment percevez-vous l'action des pouvoirs publics dans ce domaine ? Que pensez-vous des initiatives européennes, et notamment de la stratégie « cyber » présentée par la Commission européenne, ou encore de la révision envisagée de la directive *Network and Information System Security (NIS)* ?

À l'approche de la présidence française de l'Union européenne, à compter du 1er janvier 2022, il me semble important d'avoir les idées claires sur les priorités à défendre en la matière.

Quant à la diffusion d'une culture cyber au sein de la société, quel regard portez-vous sur le niveau de sensibilisation, aussi bien des entreprises et des administrations publiques, dont les collectivités territoriales, que des citoyens ? J'aimerais en outre aborder la formation aux compétences cyber, alors même qu'un campus cyber s'apprête à voir le jour avec l'appui, entre autres, de l'agence nationale de la sécurité des systèmes d'information (ANSSI). Comment la France se positionne-t-elle par rapport à ces enjeux, comparée à d'autres pays ? Devrions-nous compléter notre offre de formation dans certains segments en particulier ? Nous resterait-il d'éventuelles lacunes à combler ?

M. Guillaume Vassault-Houlière, président-directeur général et cofondateur de Yes We Hack. Je reviendrai sur l'identité de Yes We Hack, sa coopération avec les ministères et institutions publiques, son vécu de la crise sanitaire et les moyens par lesquels nous incitons à la mise en place d'une cybersécurité efficace à l'échelle nationale, en démystifiant les pirates

ou *hackers*, en réalité des passionnés d'informatique d'une grande compétence ne demandant qu'à contribuer à l'amélioration de la cybersécurité.

Yes We Hack se présente aujourd'hui comme la première plateforme de *bug bounty* d'Europe. Nous fédérons 22 000 hackers présents dans 168 pays, ce qui nous permet de traiter les demandes de clients de tous types dans une trentaine de pays. Parmi notre clientèle figurent des entreprises connues comme BlaBlaCar ou Deezer et d'importantes banques asiatiques. Je ne suis bien sûr pas autorisé à toutes vous les citer. Nous disposons de bureaux en Suisse, à Munich et à Singapour.

Surtout présents en Europe et en Asie, nous employons près de cinquante personnes dans le monde entier, dont 40 % de femmes : une proportion dont nous sommes très fiers. Forte de sa croissance à trois chiffres et de sa capacité à exporter ses activités, notre *start-up*, qui ne mérite de fait peut-être plus cette dénomination, dispose d'une excellente résilience opérationnelle grâce à la diversité de notre communauté, en mesure de communiquer dans une multiplicité de langues et de se confronter aux technologies les plus diverses.

Nos clients font d'abord appel à nous pour tester des applications web ou mobiles du quotidien, quoique les demandes relatives aux objets connectés et aux voitures autonomes aient explosé. La mise en évidence de failles de sécurité à l'intérieur des périmètres soumis à nos tests donne lieu au versement de primes s'échelonnant de 50 à 15 000 euros, selon la criticité du bogue, une fois celui-ci validé par nos propres services ou par nos clients, selon la prestation pour laquelle ils optent.

Notre stratégie à l'international se consolide peu à peu. Il convient de le souligner. Nos effectifs devraient atteindre une centaine de personnes d'ici la fin de l'année, conformément à notre volonté d'accélérer notre développement. Cinq plateformes, essentiellement américaines, dominent aujourd'hui le marché de la chasse aux bogues. Nous avons la chance qu'existe en Europe une plateforme comme Yes We Hack. Nous ambitionnons de nous hisser, pas à pas, parmi le peloton de tête.

Nous avons travaillé sur StopCovid mais aussi sur la messagerie interministérielle Tchap pour améliorer sa transparence et sa fiabilité. Notre modèle, d'une grande agilité et d'une remarquable efficacité, apparaît parfaitement adapté au monde actuel. On dénombre environ quatre millions de postes en cybersécurité non pourvus à l'échelle de la planète. Nous sommes en mesure de mettre à pied d'œuvre jusqu'à des milliers de chercheurs pour qu'ils procèdent à des tests sur des applications en continu.

Chacun sait que les systèmes d'information actuels ne sont plus figés. Il arrive que les mises en production suivent une cadence horaire plutôt qu'annuelle comme jadis. Nous travaillons aussi bien avec des banques ou des assureurs que des acteurs numériques impliqués dans la défense ou encore des concepteurs d'objets connectés.

Un besoin de transparence et de confiance se fait jour chez les citoyens et les entreprises, et pas seulement en France. La cybersécurité constitue un outil de marketing. Il ne faudrait pas que son coût rebute, vu qu'elle assure une formidable impulsion aux affaires. En tant que Français, en tant qu'Européens, nous défendons des valeurs démocratiques, en matière de souveraineté et de données notamment, qui s'exportent à merveille. Le succès de notre plateforme en apporte la preuve. L'expertise et la qualité opérationnelle de Yes We Hack bénéficient aujourd'hui d'une reconnaissance mondiale. Nous poussons d'ailleurs nos clients à relayer notre promotion.

Parrot nous a récemment accordé sa confiance pour que nous assurions la sécurité de ses données et la transparence de son code. De plus en plus de gouvernements comprennent que notre communauté de *hackers*, autrement dit de passionnés, se définit, selon le *manifeste du hacker* publié en 1986, par l'envie d'apprendre et de se remettre en cause, soi et son environnement, afin d'améliorer celui-ci par souci du bien commun.

Nous avons transposé ces valeurs à l'échelle industrielle partout dans le monde et en tirons une immense fierté. Un nombre croissant d'États s'efforce de protéger notre communauté, comme le montrent bien certains rapports de l'organisation de coopération et de développement économiques (OCDE). Nous souhaitons qu'on lui donne les moyens de s'exprimer et d'étendre sa philosophie de vie à tous les domaines du quotidien pour améliorer celui-ci en lui apportant plus de transparence.

La traçabilité de l'argent joue un rôle notable dans notre sélection des *hackers*. Les primes leur sont versées par un prestataire bancaire, dans le respect des normes de lutte contre le terrorisme et le blanchiment d'argent, ce qui nous différencie d'ailleurs de nos homologues américains, au même titre que le Règlement général sur la protection des données (RGPD). Yes We Hack utilise aujourd'hui dans ses infrastructures des technologies européennes. Nous prônons notre savoir-être européen avec succès jusqu'aux États-Unis.

La prise de conscience de l'importance de la cybersécurité en France assure notre développement à l'échelle nationale. Nous améliorons la sécurité des outils numériques du quotidien qui gèrent des quantités de données, à la demande de nos clients, quels qu'ils soient. Nous répondons d'ailleurs à leurs demandes avec un égal sérieux, indépendamment de leur taille. Au final, tout le monde y gagne, les entreprises autant que les citoyens. Yes We Hack allie aujourd'hui une excellente qualité de service à une redoutable rapidité d'exécution.

Mme Rayna Stamboliyska, vice-présidente en charge des affaires publiques et institutionnelles de Yes We Hack. Les enjeux éminemment complexes et passionnants que vous avez esquissés dans votre introduction, M. le rapporteur, évoluent très rapidement. Ces derniers mois, de nombreux sujets sont revenus sur le devant de la scène, sous un éclairage différent d'il y a quelques années.

J'aimerais mettre en correspondance la vaste question de la définition de la souveraineté numérique avec la notion d'autonomie stratégique. Je me permettrai un trait d'esprit en vous annonçant que : « je suis venue vous parler d'Europe », à l'instar du président de la République en ouverture de son discours de la Sorbonne, voici quelques années. La souveraineté numérique française se joue aujourd'hui à l'échelle européenne et s'inscrit pleinement, selon notre point de vue, dans une démarche et une volonté d'autonomie stratégique européenne. Bien sûr, cette dernière notion évolue extrêmement vite.

Je me rappelle que les débats sur la souveraineté numérique tournaient, voici une dizaine d'années, autour de la gouvernance d'Internet. Une fracture se dessinait alors entre les approches technicistes occidentales et des conceptions plus centrées sur l'accès à l'information à l'Est. L'accès à la connaissance et à la liberté d'expression permises par le numérique sont ensuite revenues sur le devant de la scène, avant de céder la place aux préoccupations de surveillance liées aux révélations d'Edward Snowden en 2013 et 2014. Depuis, nous avons vécu, ou plutôt, survécu à la présidence de Donald Trump, durant laquelle se sont cristallisées des tensions géopolitiques d'une importance cruciale autour de questions d'économie stratégique, notamment sous son versant technologique. Le mandat de Donald Trump a donné un coup d'arrêt à un multilatéralisme que l'on croyait acquis, encore que la situation semble se débloquer dernièrement, depuis le changement d'équipe au pouvoir aux États-Unis.

Pendant que nous parlions de gouvernance du net et d'accès à la connaissance, cet objet à la fois diffus et précis que représentent les données a silencieusement transformé et refaçonné nos vies. Ces données, dans leurs multiples dimensions (personnelles ou ouvertes par exemple), sont d'abord apparues comme un nouvel or noir (« *data is the new oil* »), puis un nouveau terreau (« *data is the new soil* »), avant qu'on ne les qualifie de radioactives (« *data is the new uranium* »). Des acteurs sont en effet apparus, dont le modèle économique n'est autre que la prédation de données, notamment personnelles. Ils ont connu une croissance tellement gargantuesque qu'ils posent dorénavant un défi à la gouvernance au quotidien. Il nous semble primordial de garder en tête, quand on traite de souveraineté numérique, ce rapport de forces asymétrique, qui place en situation de vulnérabilité les individus mais aussi, de plus en plus, les administrations publiques et les entreprises.

Au vu de la complexité des enjeux interdépendants qu'elle implique, la question de la souveraineté numérique dépasse aujourd'hui le champ numérique traditionnel, des infrastructures et du web, pour toucher à la cybersécurité, à la neutralité du net, à la protection des données, à la lutte contre la désinformation, aux discours de haine, au multilatéralisme, à la fiscalité du numérique, aux technologies de rupture et à la transparence des algorithmes. Une telle conception de la souveraineté numérique correspond en tout cas à l'ambition que nous portons, à notre manière et à notre échelle, par la promotion d'une meilleure maîtrise du risque numérique, *via* la gestion des vulnérabilités.

La souveraineté numérique est partie intégrante de l'autonomie stratégique, qui dépasse quant à elle le modèle gaullien historiquement daté. Nous nourrissons une ambition claire : celle que la souveraineté française ne s'entende qu'en harmonie avec une souveraineté européenne. L'approche de la présidence française de l'Union européenne donne lieu à un alignement de planètes. J'en profiterai pour insister sur trois piliers constitutifs de la souveraineté numérique.

Le premier, politique, est aussi démocratique. Nos processus démocratiques apparaissent aujourd'hui des plus fragiles. Différentes mesures sont à l'étude pour protéger notre démocratie. Au-delà de cette approche conservatoire, il convient d'insuffler les valeurs démocratiques européennes aux initiatives technologiques et géopolitiques à venir. L'importance qu'attache Yes We Hack à la traçabilité des flux financiers relève de ce principe. Nous tenons au respect de la réglementation en matière de lutte contre le terrorisme et le blanchiment d'argent, en dépit de sa pesanteur souvent dénoncée. Elle traduit en effet nos valeurs, quitte à ce que d'aucuns voient parfois en elle un léger frein à la construction de notre offre de services. Nos valeurs d'éthique, de transparence et d'intégrité nous semblent un garde-fou nécessaire pour éviter que la construction d'un modèle européen ne tourne à la caricature d'une gestion d'entreprise à l'ancienne.

Le deuxième pilier de la souveraineté numérique, économique celui-là, touche à la prospérité commune. J'entends par là le fait de favoriser ou du moins de rendre possible une politique industrielle forte, qui capitalise sur la recherche scientifique. Le budget prévu par le fonds de relance européen complète dans cette optique d'autres instruments tels que le programme Horizon Europe ou DigitalEurope. La Commission présidée par Mme Ursula von der Leyen a fait du marché unique une priorité. Différentes initiatives plus ou moins avancées participent déjà à sa construction. En matière de cybersécurité, citons la démarche, soutenue par le *Cyber Act*, de certification européenne, en vue d'harmoniser le niveau de cybersécurité exigé dans l'Union européenne.

Le troisième et dernier pilier de la souveraineté numérique, pour le coup technologique, n'implique pas une autarcie technique mais vise à réduire notre dépendance, voire notre servilité actuelle vis-à-vis d'acteurs extra-européens, notamment américains. Différentes

approches existent, qu'elles passent par la législation ou par la commande publique, sur les insuffisances de laquelle, tant au niveau national qu'européen, il faudra d'ailleurs absolument se pencher. La tâche ne s'annonçant pas simple, je souhaite bien du courage à la personne qui tentera de relever le défi. Sans doute avez-vous déjà, dans cette mission d'information, abordé la commande publique française. De plus en plus d'initiatives européennes, certes discrètes, s'attaquent heureusement au problème, autrement dit, cherchent un moyen d'implémenter un marché unique du numérique européen.

Le modèle européen d'une souveraineté numérique fondée sur ces principes doit apporter la preuve de sa fonctionnalité et de sa capacité à s'exporter, seule à même de garantir sa place dans le monde. Yes We Hack l'a démontré par son exemple.

C'est dans ce cadre à la fois civil et militaire qu'en tant qu'acteur français et européen de la cybersécurité, nous inscrivons notre exigence de maîtrise et de gestion du risque numérique. Celle-ci se décline en un versant relatif aux données et aux infrastructures, auquel s'ajoute une composante stratégique de préservation et de maîtrise des fournisseurs. La question transversale de la gestion des vulnérabilités constitue notre cœur de métier. Son importance s'est encore accrue depuis les récents travaux de l'OCDE auxquels nous nous sommes activement associés, mais aussi grâce à d'autres initiatives telles que l'Appel de Paris, auquel nous avons également pris part, dont M. l'ambassadeur Henri Verdier vous a déjà parlé.

Un grand nombre d'initiatives s'attellent à la question de la cybersécurité de manière à la fois constructive, défensive et innovante, en questionnant ce qu'il est possible de mettre en œuvre pour dépasser une vision protectrice de ce concept, dans une volonté d'innovation, comme cela a d'ailleurs été fait pour les données, voici dix ans.

M. Philippe Latombe, rapporteur. Comment estimez-vous aujourd'hui le niveau de cybersécurité en France et en Europe ? Une culture de la cybersécurité s'est-elle selon vous suffisamment développée dans les entreprises, les collectivités territoriales et les États ?

Mme Rayna Stamboliyska. Je m'efforcerai de rester polie. Plaisanterie à part, on constate bel et bien un sursaut, même s'il est dommage qu'il survienne dans certains cas en réaction à un incident qui oblige à se demander comment reconstruire un système d'information, comment protéger des données d'utilisateurs ou de patients. La conscience, inégale, du rôle clé de la cybersécurité, apparaît largement plus développée dans certaines administrations ou pays que dans d'autres.

Ceci nous ramène à la notion de pouvoir ou plutôt de volonté. Un besoin évident se fait jour d'un État stratège, d'une ligne de conduite globale à suivre. Beaucoup se découragent quand ils comprennent que la sécurité d'une installation n'est jamais acquise une fois pour toutes, mais qu'il faut au contraire l'améliorer constamment. La nécessité de soutenir, consolider et nourrir cette amélioration continue implique la poursuite d'objectifs liés à une stratégie globale, qui s'appuie sur des outils dont on ne pourra disposer qu'en recourant à la commande publique, aujourd'hui insuffisante.

Je ne songe pas ici aux difficultés que pose un référencement à l'Union des groupements d'achats publics (UGAP), par exemple, mais aux exigences de sécurité bien trop faibles, voire inexistantes, imposées aux fournisseurs de services et d'outils numériques susceptibles d'être sollicités pour des commandes publiques. L'absence, en 2021, d'exigence d'un niveau minimal de sécurité ou d'un maintien aux conditions opérationnelles et de sécurité de ce qui est acheté dans le cadre de la commande publique a de quoi désagréablement surprendre.

Certes, des initiatives voient le jour, comme celle du sénateur M. Laurent Lafon. Le texte de sa proposition de création d'un CyberScore devrait parvenir sous peu à l'Assemblée nationale. L'ANSSI, en France, est forte de sa capacité à décerner des certifications et des qualifications. Nous ne comprenons toutefois pas pourquoi cette cohésion ne se renforce pas plus pour fournir aux administrations des outils performants, ergonomiques et surtout fiables. Je constate peu de discussions ou de travail concret effectif sur cette pierre d'achoppement, sans doute en raison d'une absence de stratégie globale.

Le gouvernement français s'est déjà doté d'un administrateur général des données. Pourquoi ne pas imaginer une harmonisation des exigences en matière de cybersécurité sous l'égide d'un fonctionnaire général de la sécurité des systèmes d'information (FSSI) ? Il fixerait à tous des objectifs clairs, et communiquerait une vision tout aussi claire de l'adoption, par tous, des instruments existants. La seule mention du référentiel général de sécurité (RGS) fait aujourd'hui grincer des dents. Ses préconisations sont pour l'heure appliquées de manière pour le moins inégale et parfois insuffisante, pour ne pas dire « au lance-pierres ».

M. Guillaume Vassault-Houlière. Le besoin se manifeste aujourd'hui d'une sécurité opérationnelle. Une grande diversité de cultures cyber coexistent dans le monde. Les Anglo-saxons n'optent pas pour la même approche que les Latins, sans parler de ceux qui pratiquent la politique de l'autruche. Les solutions de cybersécurité ont été pour l'heure empilées en couches successives. La loi du net oblige ses acteurs à rester en permanence opérationnels. Chaque jour en apporte la preuve. La crise sanitaire a incité à la rationalisation des coûts mais aussi à l'équipement en outils opérationnels.

Certains pays européens semblent mieux à même de gérer les risques, du fait de leur culture. Je songe aux pays nordiques ayant historiquement intégré le concept de développement agile. L'activité de notre plateforme enregistre d'ailleurs une forte croissance dans ces pays. D'autres nations semblent plus figées dans leur attitude et plus lentes à évoluer. En 2021, tout le monde a compris qu'il fallait démystifier la cybersécurité et prôner dans ce domaine une cohésion nécessaire, qui passera forcément par une multiplicité d'acteurs. Les relations entre secteurs public et privé jouent un rôle majeur en générant de l'innovation et en permettant de former du personnel qualifié. Il en résulte un cercle vertueux. Par ailleurs, certains pays accélèrent leur développement en matière de cybersécurité plus que d'autres, malgré leur retard initial. Tout dépend aussi des acteurs sur lesquels chaque pays peut s'appuyer sur son territoire.

Aujourd'hui, la géopolitique, loin de se limiter aux acteurs traditionnels du champ, implique plus que jamais les entreprises, qui en transposent les tendances. Plus il existe de sociétés innovantes, plus celles-ci jouent un rôle moteur d'innovation globale, en matière notamment d'utilisation des outils cyber à l'échelle mondiale. Nous pouvons aujourd'hui nous appuyer en Europe sur les pays nordiques et sur des acteurs compétents et passionnés.

La diversité des acteurs publics et privés impliqués dans le projet de campus cyber assurera sa force. Cette diversité a déjà démontré son efficacité dans d'autres pays. Certes, la prise de conscience en matière de cybersécurité s'accélère, pour autant, il ne faut pas emprisonner la commande publique dans des outils dépassés constituant un frein technologique pour les États tenus de se numériser rapidement. La tendance est aujourd'hui à l'ouverture croissante des systèmes d'information et des données dans un souci de transparence et de confiance. Il faut, pour y parvenir, des outils adaptés, des entreprises adéquates, une stratégie globale cohérente avec les valeurs européennes et une volonté de transformer un monde où le commerce se développe parfois en dépit du bon sens.

Chacun de nous est un client de ces grandes entreprises du numérique. En tant que tels, nous avons le pouvoir de les amener à fléchir, du moins celles qui n'appliquent pas les valeurs qui nous tiennent à cœur ou ne créent pas un cercle vertueux pour l'évolution de la société.

M. Philippe Latombe, rapporteur. Impliquez-vous que l'État et les collectivités territoriales se sont numérisés à toute vitesse sans intégrer d'entrée de jeu la cybersécurité, dont ils se sont occupés en ajoutant des couches successives à leurs projets ? Estimez-vous que, pire encore, ils n'en tiennent peut-être même pas compte dans leur vision à court et moyen terme ?

M. Guillaume Vassault-Houlière. Il faut bien comprendre qu'on ne trouvera jamais deux entités, qu'elles soient publiques ou privées, disposant exactement du même système d'information. Ces systèmes conçus par des personnes différentes, et à chaque fois transposés, ne sont pas partout maintenus selon les mêmes principes. Leurs composants, en particulier dans la commande publique, devraient inclure leur maintien aux conditions de sécurité. De plus en plus de pays dressent des catalogues pour faciliter la commande publique, en tenant compte de ces exigences.

Aujourd'hui, le plan de relance cyber, piloté notamment par l'ANSSI, place les collectivités territoriales dans une situation dont je ne doute pas, pour avoir discuté avec nombre d'entre elles, qu'elles la jugent inconfortable : elles doivent se plier à des normes édictées au niveau national, que les éditeurs de solutions numériques ne sont pas forcément tenus de respecter. Des acteurs, tels que des collectivités territoriales, ne disposant pas, parmi leurs équipes, d'experts en la matière, ni du temps voulu pour se pencher sur la question, sont sommés de se numériser rapidement.

En réalité, il manque une stratégie globale pour garantir une sécurité de bout en bout. À chacun son métier. L'union fait la force. Chacun doit assumer ses responsabilités. Il me paraît crucial de le souligner. La vulnérabilité des données a aujourd'hui un impact sociétal. L'actualité l'a montré. Chacun doit se penser comme un acteur du changement plutôt que comme un simple vendeur indifférent au devenir des solutions numériques qu'il commercialise. Des changements s'observent heureusement déjà en France, en Europe et dans le monde, ce que nous constatons dans certains pays d'Asie où nous sommes présents.

Les soucis qu'a connus Singapour voici quelques années ont amené cette cité-État à une prise de conscience. La simplicité d'utilisation de certaines applications gratuites, c'est-à-dire où le produit n'est autre que l'usager lui-même, n'implique pas qu'elles soient sécurisées. La notion de sécurité *by-design* a été transposée dans le RGPD. Les obligations qu'il comporte doivent s'appliquer à l'ensemble des acteurs du numérique pour garantir la sérénité de la totalité des usagers.

M. Philippe Latombe, rapporteur. Voyez-vous aujourd'hui des pays d'Europe dont la France devrait suivre l'exemple en termes de bonnes pratiques ? Existe-t-il en Europe un pays capable de jouer dans le domaine de la cybersécurité un rôle moteur ? Le campus cyber est en cours de construction, mais il ne concerne que la France, or la souveraineté numérique se bâtira, vous l'avez dit, à l'échelle européenne. Avez-vous eu vent d'initiatives européennes allant dans le même sens ?

M. Guillaume Vassault-Houlière. Nous disposons déjà de tous les outils que l'on pourrait souhaiter. Je ne pense pas seulement à l'ANSSI. La France peut s'appuyer sur son expérience de transposition au niveau national d'outils efficaces. Des certifications européennes existent déjà. Il ne reste plus qu'à entrer en action. La nouvelle version de la directive *NIS* va entraîner des changements. Il ne faut pas créer un entonnoir mais concilier

l'agilité et la capacité de réagir vite avec le respect de plusieurs niveaux d'exigence, qui passera par du marketing européen. Il convient de miser sur la cohésion globale des éléments déjà disponibles, et de suivre une stratégie de souveraineté et de coordination dépassant même le cadre strictement européen.

Mme Rayna Stamboliyska. Beaucoup de pratiques résultent de l'histoire et de la culture propres à chaque pays. Prenons le cas de l'Allemagne, notre plus proche allié européen, avec qui nous partageons une frontière. Sa structure fédérale en Länder implique une organisation des administrations tout à fait différente de ce qu'on observe en France. Dans chaque pays coexistent des usages dont il y a lieu de s'inspirer et d'autres, plus critiquables. Il m'apparaît nécessaire de mener une réflexion collégiale au côté de nos homologues européens pour éviter de rédiger des feuilles de route nationales qui perdront de leur pertinence lorsqu'une mise en conformité aux normes européennes s'imposera.

L'exemple de la fiscalité du numérique le montre assez. Les transpositions nationales divergentes de la directive *NIS* avaient donné lieu à des incohérences problématiques. Plusieurs ateliers se sont attelés l'an dernier à sa révision et à la reformulation de ses exigences. Nous nous y sommes d'ailleurs impliqués. Certains opérateurs de services essentiels en France ignoraient si leurs homologues aussi étaient considérés comme tels dans d'autres pays. Les agences de cybersécurité (les ANSSI locales) édictaient dans chaque pays leurs propres exigences. Des Polonais ont ainsi réclamé aux Français des preuves de conformité au sein d'un même groupe. D'aussi considérables variations, d'une législation nationale à l'autre, apparaissent ingérables et mènent à la catastrophe. On comprend dès lors mieux pourquoi, au moment de réviser la directive *NIS*, d'aucuns ont argumenté en faveur de sa transformation en Règlement, de manière à l'appliquer sans presque aucune modification d'un pays à l'autre. Le texte parvenu au Parlement reste pour l'heure une directive. Toutefois, son périmètre élargi l'amène à concerner de plus nombreux secteurs, ce qui contribue à une meilleure harmonisation des pratiques.

C'est à de tels niveaux qu'il faut transmettre au reste de l'Europe ce que l'expérience de la France lui a appris. La loi de programmation militaire (LPM) a, dans sa version 2014-2019, défini de manière inédite les systèmes d'information d'importance vitale. Autrement dit, une composante technique et cyber est entrée pour la première fois dans cette loi de financement. Cette LPM a impulsé la première mouture de la directive *NIS*. La révision de cette dernière, en discussion, prend appui sur les leçons positives et sur d'autres, tirées des dysfonctionnements liés à la notion de *lex specialis,* selon laquelle prévaut la loi spécifique à un domaine, en l'occurrence nationale.

Lors des ateliers de révision de la directive *NIS*, j'ai avancé comme exemple concret l'appel d'air créé pour les entreprises par la LPM en France. Les exigences inscrites dans cette loi se sont ajoutées à d'autres édictées par l'ANSSI en matière de sécurité des fournisseurs, de services de sécurité ou d'équipement, aux opérateurs d'importance vitale. Des opportunités de développement commercial non anticipées en ont résulté.

On croit en général que l'application d'exigences réglementaires entraîne des frais et prend du temps. On en oublie de considérer leur impact dans son ensemble. Les fournisseurs contraints d'élever leur niveau de sécurité obtiennent au final un retour sur investissement, dans la mesure où ils captent ainsi de nouveaux clients. Il faut en tenir compte dans les discussions en cours sur la construction technologique européenne. On peut s'inspirer, dans le même ordre d'idées, de l'exemple néerlandais en matière de divulgation des vulnérabilités, ou des pratiques allemandes en ce qui concerne la commande publique fédérale.

M. Philippe Latombe, rapporteur. L'État a fait appel à vous pour la mise au point de l'application StopCovid. Faut-il y voir une initiative ponctuelle ou le signe d'un changement de paradigme ? L'État adopte-t-il enfin progressivement une méthode plus agile ? Le recours à vos services vous semble-t-il appelé à perdurer ou à s'intégrer dans le champ de réflexion de l'administration ?

M. Guillaume Vassault-Houlière. Notre rôle dans le lancement de l'application TousAntiCovid, particulièrement médiatisé du fait de l'exigence de transparence et de confiance qu'imposait la généralisation de cet outil, à l'origine, dans un premier temps, d'une certaine défiance, ne constitue qu'un exemple parmi d'autres.

En ce qui concerne l'application StopCovid, les autorités nous ont donné carte blanche pour transposer notre expertise et tout s'est très bien passé. Nous avons noué d'excellentes relations avec les équipes de l'ANSSI et de l'Institut national de recherche en informatique et en automatique (Inria), qui nous ont au final accordé leur confiance, après de nombreux débats sur la question complexe des tests auxquels nous souhaitions soumettre l'application. Ceci dit, cette collaboration ne nous a pas fourni l'opportunité de démontrer l'étendue de notre savoir-faire.

Suite à un incident de sécurité survenu avec la messagerie Tchap, nous avons soumis cet outil public à la communauté des 22 000 *hackers* de Yes We Hack afin de trouver une parade à ses vulnérabilités, de manière à rassurer ses utilisateurs. Nous avons également noué un partenariat avec l'état-major des armées (EMA), c'est-à-dire le commandement de la cyberdéfense. Mme la ministre a d'ailleurs divulgué, en 2019, son recours à des *hackers* éthiques, *via* notre plateforme, en vue de sécuriser différents périmètres du ministère. D'autres administrations encore font appel à notre communauté, forte de son opérationnalité.

En tant que pur produit de la communauté des *hackers* des années 2000, passionné par mon métier, je me rends bien compte, pour avoir travaillé avec des entités ministérielles de France et d'ailleurs, que nos concitoyens éprouvent le besoin d'outils fiables au fonctionnement transparent. Nous nous devons aussi de sécuriser les données, au volume sans cesse croissant. La France a joué un rôle précurseur à travers le commandant de la cyberdéfense, lorsqu'il a cherché comment animer et former les 400 réservistes à sa disposition, et comment élargir les tests de sécurité de ses outils numériques, jusque-là réalisés en interne *via* des audits planifiés. La perception du risque progresse à la vitesse à laquelle se développent les nouvelles technologies. Un besoin se fait jour de compétences adaptées rattachées à des métiers divers et variés.

Le stéréotype du méchant *hacker* ne prédomine plus du tout aujourd'hui comme c'était le cas dix ans plus tôt. Notre communauté incarne une philosophie et un art de vivre dépassant le simple cadre de l'informatique et impliquant la remise en cause perpétuelle de notre écosystème dans la volonté de l'améliorer.

L'article 47 de la loi pour une République numérique protège les lanceurs d'alerte s'adressant à l'ANSSI. Jusque-là, certains *hackers* ne voulaient plus courir le risque de signaler des vulnérabilités aux entreprises ou aux entités ministérielles par crainte de poursuites pénales. Leur action citoyenne n'était en effet pas comprise. Aujourd'hui, de plus en plus de pays cherchent un moyen de dénoncer les vulnérabilités *via* la création de canaux de communication de confiance avec les communautés de *hackers*.

Nous avons réussi avec d'autres experts mondiaux à transposer de telles initiatives dans une note d'un rapport de l'OCDE. L'*European Union Agency for Cybersecurity (ENISA)* se penche en ce moment même sur des changements à venir. La France a joué un rôle moteur

précurseur avec les Néerlandais. L'accroissement des menaces pousse à se tourner vers des outils de plus en plus efficaces garantissant un retour sur investissement rapide. La plateforme Yes We Hack, parfaitement adaptée au monde actuel, a déjà prouvé son efficacité.

Tout le monde souhaite embaucher les meilleurs spécialistes de la cybersécurité. Je rappelle que quatre millions de postes demeurent à ce jour à pourvoir dans ce domaine, sur l'ensemble de la planète. La numérisation croissante de la société et des États génère un fort besoin de cybersécurité. Nous travaillons en ce moment sur des dispositifs de vote en ligne. Il n'est plus envisageable de s'en remettre à l'expertise d'une seule entreprise. Il convient au contraire de solliciter une communauté de passionnés, dans toute sa diversité. Nous savons tous que l'union fait la force. L'intelligence collective a démontré son efficacité dans beaucoup de domaines. Nous sommes très fiers que les acteurs étatiques aient compris notre démarche et fassent appel à nos services.

Œuvrer en partenariat avec le ministère des armées relevait d'un rêve d'enfant. Aux États-Unis, de nombreux *hackers* souhaitaient s'attaquer au Pentagone. Des initiatives américaines relatives à l'*US Air Force* ont vu le jour. Nous avons quant à nous réussi à mettre en avant, auprès du ministère des armées, notre modèle fondé sur des valeurs françaises et européennes et sur la confiance, pour œuvrer en bonne intelligence avec la communauté de l'EMA.

Nous préconisons que tout outil commercialisé au grand public, y compris les voitures, dispose d'un outil de signalement de ses vulnérabilités afin d'éviter toute utilisation malveillante. Nous prônons aussi de placer à l'abri des poursuites judiciaires tout citoyen révélant une faille de sécurité. On assiste en somme à un changement sociétal. Chaque État avance désormais, certes à sa vitesse, dans la bonne direction. La remarque est transposable aux ministères et à d'autres strates administratives encore. Nous nous efforçons depuis des années de montrer ce que peut apporter une collaboration avec des *hackers* de bonne volonté.

M. Philippe Latombe, rapporteur. Nous avons auditionné la semaine dernière l'Imprimerie nationale et, quelques jours auparavant, la responsable du projet « identité numérique ». Cette identité numérique vous apparaît-elle comme une opportunité ou plutôt comme une faille ? Comment percevez-vous ce projet en termes de cybersécurité ? Constitue-t-il un point de vigilance supplémentaire ? Les pays qui l'ont adoptée s'y sont-ils pris de manière suffisamment sécurisée ?

J'ai jusqu'ici recueilli deux réponses fort éloignées à mes questions. La responsable interministérielle affirme que la mise en place de l'identité numérique passera par des marchés exclusivement publics, alors que l'Imprimerie nationale avance que les entreprises privées y auront leur place. Les données liées à l'identité numérique, du fait de leur considérable importance, ne feront-elles pas l'objet d'attaques permanentes mobilisant des technologies de plus en plus avancées ? Que vous inspire sa mise en place, en France et dans d'autres pays, en Europe et ailleurs ?

M. Guillaume Vassault-Houlière. Il faut aujourd'hui, pour minimiser le risque, immuniser les données. Il convient de déterminer, dans chaque projet, les mesures de sécurité qui relèvent ou non de l'utile. L'identité numérique sera attaquée au même titre que tout vecteur, peut-être plus encore en raison de la quantité de données qui y sont liées. L'identité numérique implique une interconnexion avec différents satellites, IdP (*identity provider*) et SP (*service provider*). Il faudra donc sécuriser toute la chaîne. En réalité, le risque zéro n'existe pas.

Je prône dans tous les cas d'atteindre l'efficacité par les moyens les plus simples. Je m'interroge à ce titre sur l'intérêt d'imposer des mesures de sécurité additionnelles uniquement pour ne pas confier la gestion de l'identité numérique à un seul et unique acteur global.

J'ai travaillé dans la haute disponibilité durant de nombreuses années. Mes clients exigeaient de moi, il y a quinze ans, de la réversibilité et de la résilience, la seconde supposant de toute façon la première. Peu importe le nombre d'acteurs impliqués dans un projet, à partir du moment où son niveau de documentation et d'interopérabilité atteint un certain seuil, le risque apparaît maîtrisé. Chacun a les mêmes exigences techniques, en matière de cybersécurité comme de stockage. Il me semble important de construire un projet qui en tienne compte. On en revient à la souveraineté. Il faut bien analyser et gérer le risque dès le début du projet, ce que résume d'ailleurs parfaitement le concept de sécurité *by-design*, et garantir la réversibilité en cas de problème.

L'identité numérique relève désormais d'une nécessité. Il convient toutefois de l'utiliser avec parcimonie, dans un premier temps, de manière à capitaliser sur les projets à venir pour garantir son efficacité, plutôt que de laisser l'initiative à des acteurs incompétents, incapables de garantir ne serait-ce que nos numéros de téléphone. Les identités numériques qu'ils gèrent sont censées permettre l'accès à une multiplicité de service ; or ce sont toujours les mêmes qui gardent la mainmise dessus. Nous avons la chance de disposer de l'excellente initiative Franceconnect. Il faut continuer en ce sens. Il m'apparaît tout à fait possible d'aboutir à une réalisation susceptible de servir de modèle, en Europe comme dans le reste du monde, en s'appuyant justement sur les valeurs européennes.

Mme Rayna Stamboliyska. Je ne suis pas du tout spécialiste de l'identité numérique. Je m'excuse donc par avance des inexactitudes qui m'échapperaient.

Il m'apparaît nécessaire de clarifier rapidement le modèle économique sur lequel repose l'identité numérique. La révision du Règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (eIDAS) le montre assez. Elle pourrait d'ailleurs figurer parmi les actions notables portées par la future présidence française de l'Union européenne.

On évalue le marché de l'identité numérique à un peu plus d'un milliard d'euros de revenus à l'horizon 2030. Une question se pose : comment permettre aux acteurs français et à l'État de mettre en œuvre une structure économique susceptible de préserver ce marché face à des initiatives déjà lancées par des acteurs privés extra européens tels que Google, Apple, Facebook, Amazon et Microsoft (les GAFAM) ?

Le scénario le plus probable m'apparaît encore être celui où le schéma de l'identité numérique se structurerait autour d'un fédérateur d'identité unique offrant aux utilisateurs le choix d'un fournisseur d'identité, dans l'hypothèse d'un Règlement eIDAS substantiel aux exigences élevées. Ce fournisseur, public ou privé, permettrait d'accéder à l'ensemble des services publics et privés.

Une autre question émerge dès lors : celle des garanties dont bénéficieront les données des citoyens français et européens. Là encore, l'ANSSI tient lieu de source d'inspiration avec sa récente publication d'un référentiel d'exigences en matière de sécurité de l'identité numérique. Dans la révision du Règlement eIDAS, il apparaît primordial de continuer à promouvoir un niveau élevé de sécurité et de préserver les fournisseurs d'identité privés au sein de l'Union européenne, à condition bien sûr qu'ils soient réellement européens et non de

simples entités juridiques au siège sis en Irlande ou au Luxembourg. L'identité numérique fonctionne à une double échelle, nationale et européenne.

Franceconnect peut assumer en France un rôle important, aussi bien d'acteur assurant l'ensemble des fonctions requises, que de *hub* technique pour les fournisseurs.

Quoi qu'il en soit, il est impératif de maintenir au niveau européen les exigences du Règlement eIDAS, destiné, en l'état, à prévenir l'apparition de fournisseurs d'identité numérique extra européens privés. À cela doit s'ajouter ce qui émerge à travers la stratégie européenne relative aux données, les préconisations de l'ANSSI en France, ainsi qu'un projet du ministère de la transformation et de la fonction publique, à savoir l'idée d'un *cloud* au cœur de l'État, imposant clairement une exigence de localisation de données sur le territoire européen, voire dans le pays concerné. Ce projet obéit au mot d'ordre du commissaire, M. Thierry Breton, soucieux que les données des pays européens restent en Europe.

Il faudra, pour y parvenir, livrer une grande bataille, qui s'avère d'autant plus indispensable qu'aujourd'hui, 90 % des données produites en Europe, personnelles ou non, ne sont pas stockées sur le continent européen, encore moins par des acteurs européens. Il faut s'assurer que la révision du Règlement eIDAS et de la directive *NIS*, la stratégie européenne en matière de données et les initiatives entre autres françaises dans ce domaine demeurent en cohésion et en harmonie pour se soutenir mutuellement, afin d'éviter la dispersion des capacités, de manière à permettre l'émergence d'un modèle économique hybride acceptable par une majorité d'acteurs européens et par les citoyens eux-mêmes.

On a pu constater une défiance de certains vis-à-vis du rôle de l'État en tant que responsable du traitement des données, contrastant avec leur méfiance moindre envers certains acteurs privés d'envergure. À l'inverse, l'État inspire à d'autres moins de doutes que certaines entreprises privées.

Il semblerait donc intéressant de construire un modèle hybride associant, à la fonction étatique publique, la fourniture de services, en l'occurrence d'identité numérique, par des acteurs privés, en conformité avec des exigences réglementaires et législatives européennes communes, impulsées par les États.

M. Philippe Latombe, rapporteur. Il faut aussi se demander si l'identité numérique fera l'objet d'attaques, quoique M. Vassault-Houlière ait déjà répondu à cette question par l'affirmative, en raison du profit qui pourrait être retiré de son usurpation.

Les attaques d'hôpitaux et de collectivités territoriales se sont multipliées dernièrement, sans même parler de l'incendie d'OVH. Il est apparu que beaucoup d'entreprises et d'administrations ne disposaient ni de plan de reprise d'activité (PRA) ni de plan de continuité d'activité (PCA). Il a beaucoup été question des attaques russes contre le centre national d'enseignement à distance (CNED) et des problèmes de connexion aux espaces numérique de travail avant-hier.

Les mesures de sécurité mises en place aujourd'hui vous semblent-elles suffisantes ? N'avez-vous pas le sentiment d'une perte de certains réflexes ? Du temps où l'on ne disposait que d'archives papier, il était d'usage d'en réaliser des copies. La généralisation du numérique ne nous a-t-elle pas rendus naïfs ou imprévoyants à certains égards ? Ne faudrait-il pas, selon vous, réintroduire dans nos habitudes quelques règles de bon sens ?

M. Guillaume Vassault-Houlière. Je vous répondrai par l'affirmative. Ceci dit, votre remarque ne s'applique-t-elle pas aussi aux téléphones ? Beaucoup, par méconnaissance ou

pour gagner du temps, installent sur leurs appareils des applications qu'ils ne maîtrisent pas. Il me paraît important de démystifier les questions de sécurité. Nous devons creuser sous la surface, loin de nous fier aux apparences.

L'anticipation de menaces ou de soucis techniques n'est jamais simple.

L'incendie d'OVH a impacté notre activité. Nous étions toutefois préparés à une telle éventualité, vu que la construction d'infrastructures indestructibles relève des préoccupations de notre métier. J'ai la chance de disposer d'équipes techniques performantes, qui ont résolu rapidement les problèmes.

Les achats, aujourd'hui facilités, ne s'effectuent plus dans les mêmes conditions qu'avant. Le métier de la haute disponibilité souffre d'une méconnaissance. Pour l'anecdote, j'ai mis en place des infrastructures destinées à la presse et aux citoyens, en vue de l'annonce des résultats d'élections, voici dix ans. La haute disponibilité n'est pas un sujet simple à aborder, surtout si l'on y inclut les risques d'attaques. Je ne jette la pierre à personne. Les PRA et PCA ont un coût. La question des compétences dans le numérique ne concerne pas que la cybersécurité mais aussi les infrastructures.

Indépendamment du recours au *cloud*, il existe de bonnes pratiques, entre autres d'achat. Il convient de se poser les bonnes questions. Selon moi, il appartient aux établissements de formation de revenir aux bases. Quand on construit une infrastructure, il faut penser à sa résilience, à l'analyse des risques, ce que l'on faisait à l'époque où l'on avait affaire à des serveurs physiques. La virtualisation liée à l'usage du *cloud* rend ces risques moins palpables, or en tant qu'êtres humains, nous éprouvons le besoin de toucher du doigt les menaces pour nous les représenter. Au final, on ignore où sont stockées les sauvegardes, ni même si elles existent. Ces questions relèvent d'une problématique de transparence. Tout est lié. La situation ne s'améliorera pas d'elle-même. Il nous appartient à nous, acheteurs, de poser les bonnes questions.

Il a beaucoup été question de réversibilité à propos du RGPD, toutefois, ce concept s'est quelque peu égaré dans les méandres de l'histoire des infrastructures. Nous devons nous demander où sont stockées nos données. Il nous revient à nous, acheteurs, de changer les habitudes liées à l'usage des plateformes *software as a service* (SaaS). La transparence engendrera la confiance. Ensemble, elles constituent les meilleures alliées du marketing.

Il n'en faut pas moins garder à l'esprit que toute une catégorie d'acteurs comme les collectivités territoriales, dont la cybersécurité n'est pas le cœur de métier, n'ont pas les moyens de se pencher sur ces questions, ce qui les oblige à s'en remettre à leurs fournisseurs. Ces acteurs accordent leur confiance aux experts qu'ils ont mandatés. Il faudrait peut-être revenir aux *requests for proposal* (RFP), c'est-à-dire aux appels d'offres tels qu'ils étaient rédigés voici quinze ans. Leurs exigences d'alors sont depuis passées à la trappe, car il est plus facile de passer une commande en quelques clics. Il ne faut toutefois jamais perdre de vue les principes fondamentaux de construction d'une architecture, tels que la disponibilité ou la résilience.

M. Philippe Latombe, rapporteur. Voyez-vous des sujets que nous n'aurions pas abordés, que vous souhaiteriez mettre en lumière ?

Mme Rayna Stamboliyska. Il nous apparaît vraiment urgent et nécessaire de disposer d'une feuille de route concrète, aussi bien au niveau national qu'européen.

Quand on commence à regarder de plus près ce qui se passe au niveau européen, comme m'y oblige par chance mon travail, on voit comment les différentes entités et structures s'imbriquent et s'interfacent. Cependant, nous ne sommes qu'un petit nombre à disposer d'une telle vision. Il m'apparaît donc impératif d'édicter une feuille de route claire, dans l'esprit de l'annonce, par le président Emmanuel Macron, du milliard d'euros consacrés à un plan global en matière de cybersécurité. Il manque aussi davantage de communication simple et accessible, à destination des administrations, des entreprises du CAC 40, des collectivités territoriales, des hôpitaux et des usagers, etc.

Nous continuerons à voir des hôpitaux victimes d'attaques nous concernant tous, dans la mesure où nous sommes tous des patients, tant que nous ne prendrons pas conscience que les outils numériques incluent aussi l'ordinateur de la secrétaire ou le téléphone du directeur, puisqu'eux aussi permettent à l'infrastructure de fonctionner. Au-delà des serveurs ou des câbles, de tels composants structurels ne sauraient pâtir plus longtemps de notre négligence, tout cela parce qu'il nous manque le temps, l'envie ou l'argent pour nous en préoccuper.

Il nous faut en somme une feuille de route concrète, indiquant des objectifs précis et les moyens de les atteindre, et détaillant les actions opérationnelles à réaliser par différents acteurs, de même que leurs sources de financement. Une telle feuille de route devrait faire la part belle à la recherche et à l'innovation. Nous parlons de souveraineté numérique à l'échelle européenne, or l'avenir se construit dès aujourd'hui et, pour y parvenir, il faut réfléchir à la dette technique, technologique et décisionnelle qui nous poursuit depuis des années, mais aussi à notre manière de préparer et de concevoir le futur proche.

Il est beaucoup question aujourd'hui de 5G. Je n'évoquerai pas les théories complotistes selon lesquelles il faudrait se faire vacciner pour en disposer. Heureusement, la réalité leur oppose un démenti. Une dette technique nous handicape, qu'il faut éponger vite et bien sans en générer de nouvelle.

L'indispensable feuille de route nationale et européenne que nous appelons de nos vœux doit aussi prévoir selon quelles modalités, à l'avenir, s'opéreront les justifications d'identité, les connexions, l'envoi de données, la maîtrise des interconnexions entre différentes entités, en somme, comment le risque cyber sera géré. On parle souvent de boîte à outils 5G. Que signifie concrètement ce terme ? Comment le fonds de relance européen se décline-t-il au niveau national ? Comment développer le volet technologique de manière à ce qu'on puisse se saisir des leviers aujourd'hui disponibles, souvent réglementaires et en tout cas légaux, afin d'aboutir à une réalisation concrète que tout le monde soit en mesure d'utiliser ?

M. Guillaume Vassault-Houlière. Les enjeux du numérique, dont la cybersécurité, concernent tous les pans de la société. Nous disposons de tous les leviers et de tous les acteurs voulus, sans même parler de l'intelligence collective, pour avancer dans la bonne direction. Il ne reste plus qu'à donner un coup d'accélération au processus.

Il faut continuer, surtout, à prôner la cohésion. Ensemble, nous sommes plus forts. La remarque vaut pour l'Europe, mais pas seulement. La transparence revêt une importance cruciale. Il faut faire confiance à la communauté de passionnés de cybersécurité que nous défendons depuis des années et dont je fais moi-même partie.

Je salue tous ceux qui mettent du cœur à l'ouvrage pour sécuriser les différentes infrastructures en gardant leur esprit critique constructif. Il faut continuer à démystifier la profession de *hacker* pour que tout le monde comprenne que ce merveilleux métier conviendra à tous ceux qui ont soif d'apprendre au quotidien, à base d'échanges, car il ne s'agit pas d'œuvrer seul dans son coin.

Notre communauté a montré sa capacité à innover et à améliorer le quotidien de tous depuis des années. La communauté des radioamateurs partageait la même philosophie. Nous lui devons aujourd'hui des quantités de brevets. Nous souhaitons tous aboutir à des réalisations intelligentes. Passons à présent à des actions concrètes en assurant, encore et toujours, la promotion de nos valeurs européennes partout dans le monde. Des acteurs d'autres pays parviennent très bien à diffuser leur culture.

Notre petite entreprise, qui a connu une croissance fulgurante, évolue dans un monde où règne une exigence de confiance et de transparence majeure. Élargissons aujourd'hui nos initiatives au plus haut niveau et prouvons notre capacité à construire un système opérationnel dans un monde en accélération constante. Protégeons enfin ces passionnés de cybersécurité pour qu'ils continuent de garantir la transparence de tous les outils numériques mis à notre disposition, afin de protéger à leur tour notre quotidien, aujourd'hui comme à l'avenir.

Audition, ouverte à la presse, de M. Michel Van Den Berghe, président de la mission Campus Cyber
(13 avril 2021)

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. M. Michel Van Den Berghe, directeur général d'Orange Cyberdéfense, est président du Campus Cyber. Notre mission s'intéresse à la cybersécurité et à la cyberdéfense, qui constituent en un sens le cœur de la souveraineté numérique. Nous les avons abordées sous plusieurs angles – la sécurité des systèmes d'information de l'État et des administrations publiques, l'adéquation entre l'offre cyber française et européenne et la demande des entreprises, en particulier pour celles qui ont des moyens limités, et enfin les enjeux de la formation, afin de conserver un potentiel d'innovation dans un secteur à fort contenu technologique.

Votre parcours fait évidemment écho, M. le directeur général, à ces différents sujets, puisque vous êtes à la fois le fondateur d'Atheos, entreprise de cyberdéfense rachetée par Orange, et président du Campus Cyber.

M. Philippe Latombe, rapporteur. M. le directeur général, je souhaiterais d'abord vous interroger sur la façon dont vous appréhendez la notion de souveraineté numérique. Il s'agit d'une question rituelle de cette mission, qui procède de la grande diversité des définitions existante. Que recouvre selon vous ce concept, que l'on rapproche parfois d'une forme d'autonomie stratégique et décisionnelle ? De quelle façon les politiques menées par les États peuvent-elles ou doivent-elles évoluer pour mieux intégrer cette composante stratégique ?

Je voudrais en second point revenir sur le Campus Cyber, évidemment, et sur les enjeux de formation attenants. J'aimerais que nous fassions ensemble un état des lieux de l'avancement de ce projet et que nous revenions sur ses principales spécificités. Je me demande également comment nos voisins européens s'organisent dans ce domaine. Très concrètement, disposent-ils de campus similaires ? Des coopérations ont-elles vocation à intervenir entre le Campus Cyber et d'autres structures d'États membres de l'Union européenne ? Enfin, je voudrais connaître le calendrier de déploiement de ce campus, et savoir quels objectifs vous vous fixez afin d'atteindre une taille critique pour peser dans ce domaine.

Enfin, je vous propose d'échanger sur l'écosystème des entreprises de cybersécurité et de cyberdéfense, dont Orange Cyberdéfense fait partie. Je pose à titre liminaire quelques questions pour lancer nos échanges, mais elles ont évidemment vocation à être plus larges. Comment jugez-vous le niveau de maturité de l'écosystème entrepreneurial français ? Les relations entre acteurs privés et publics en matière de cybersécurité et de cyberdéfense sont-elles suffisamment développées selon vous ? Comment pouvons-nous faire le maximum pour essayer de ne pas manquer les innovations qui pourraient se présenter dans ce domaine à l'avenir ?

M. Michel Van Den Berghe. Le premier grand point est celui de la souveraineté, qui consiste à maîtriser ses données et ses équipements informatiques, ce qui est particulièrement compliqué dans le contexte international des entreprises, pour deux raisons. La première est qu'une grande partie des solutions utilisées ne sont pas françaises et souveraines. Par ailleurs, si l'on prend l'exemple du chiffrement, chaque pays possède ses propres normes, ce qui complique le partage des données. Nous insistons également beaucoup sur le fait que pour que

les entreprises choisissent des solutions souveraines, il convient de porter ces dernières au moins au niveau des solutions américaines par exemple, afin qu'il n'y ait pas de freins à leur adoption.

C'est ce que nous voulons faire avec Orange Cyberdéfense : nous essayons de construire un leader européen, de nationalité européenne, si je puis dire, en expliquant aux grands clients internationaux qu'à expertise égale, ils ont le choix de confier le traitement de leurs données sensibles à un acteur européen.

Le Campus Cyber est un projet à l'initiative du président de la République. J'ai reçu une lettre de mission du Premier ministre en juillet 2019, me demandant d'examiner si l'écosystème français était prêt à se rassembler autour d'un seul lieu pour coopérer et partager les différentes informations dont il dispose, afin d'élever le niveau de cybersécurité de la nation et la protection des entreprises françaises.

J'ai remis un rapport au Premier ministre en janvier 2020, intitulé *Fédérer et faire rayonner l'écosystème de la cybersécurité*, et que vous pouvez retrouver sur le site de l'agence nationale de la sécurité des systèmes d'information (ANSSI). Nous avions interrogé une quarantaine d'entreprises pour leur demander si elles étaient prêtes à venir travailler ensemble dans un même lieu, malgré leurs relations de concurrence. Nous avons également visité une dizaine de campus dans le monde (à Beer-Sheva en Israël, Skolkovo en Russie et New York), avons fait travailler les ambassades pour savoir ce qu'il se passait dans les différents pays.

On m'a demandé d'opérationnaliser ce Campus Cyber. En septembre 2020, le président de la République a acté deux décisions. La première est le lieu, qui sera La Défense, car 90 % des entreprises qui ont accepté de venir travailler dans cette structure ont demandé qu'elle soit localisée dans Paris intra-muros ou en très proche banlieue. Par ailleurs, la gouvernance de ce Campus Cyber sera réalisée par une société par actions simplifiée (SAS), détenue à 51 % par le privé et à 49 % par des capitaux publics.

Le président de la République a dévoilé, il y a à peu près un mois, le plan d'accélération cyber, auquel j'ai participé, annoncé ce Campus Cyber et les moyens qui lui seront donnés.

Nous finalisons en ce moment la phase de capitalisation privée : une soixantaine d'entreprises entreront au capital de cette SAS jusqu'au 15 avril. Nous espérons faire entrer environ 3,5 millions d'euros dans cette entreprise, avec un actionnariat qui sera représentatif de la mixité des différentes sociétés : il y aura de très grandes entreprises du CAC 40 et du SBF 120, les grands acteurs de la cybersécurité, mais également des petites et moyennes entreprises (PME), des entreprises de taille intermédiaire (ETI) et même des *start-up* et associations. Les tickets d'actionnariat sont de 100 000 euros pour les grandes entreprises, 30 000 euros pour les PME et 10 000 euros pour les toutes petites entreprises et les associations. L'État, par l'intermédiaire de l'agence des participations de l'État (APE), abondera pour entrer au capital à hauteur de 49 % de l'ensemble.

Nous créons un campus regroupant quatre grands écosystèmes, ce qui est unique dans le monde. Les entreprises déporteront une partie de leurs activités dans le Campus Cyber, pour qu'il s'agisse d'un lieu opérationnel où des gens travailleront au quotidien. Elles sont incitées à y installer des équipes, qui ont tout intérêt à partager avec d'autres équipes, y compris lorsqu'elles appartiennent à des concurrents. L'exemple que je prends souvent est celui du village d'Astérix : les gens se disputent un peu sur le territoire, mais lorsque des ennemis viennent les attaquer, ils se rassemblent, prennent un peu de potion magique et luttent contre les pirates. Dans *Astérix*, comme vous le savez, les pirates se sabordent eux-mêmes quand ils voient arriver les Gaulois. C'est l'objectif que nous poursuivons. 2 000 personnes travailleront

sur ce Campus Cyber. Nous avons déjà pré-vendu 1 900 postes. De nombreuses entreprises viendront positionner une partie de leurs troupes.

Le deuxième point est la recherche et l'innovation. La France est extrêmement performante en matière de cybersécurité. L'objectif de la structure est d'offrir un lieu permettant de continuer à être très innovant, et surtout d'industrialiser les innovations lorsque cela a du sens. La proximité avec les grands industriels aidera à accélérer les développements, qui pourront être mis à leurs catalogues. Nous créerons un laboratoire de recherche et d'innovation, des zones d'expérimentation et un espace d'amorçage et d'accélération de ce qui viendra de la recherche et de l'innovation.

La formation est également un sujet important. Nous souffrons d'un manque de ressources en cybersécurité. L'objectif est de rassembler plusieurs écoles pour pouvoir former plus de personnes dans le domaine : cinq à six écoles nous rejoindront. L'école pour l'informatique et les techniques avancées (EPITA) créera un bachelor dédié à la cybersécurité. Nous voulons également susciter des vocations. Nous ne manquons pas tant de formations, mais beaucoup de personnes pensent aujourd'hui que la cybersécurité est limitée à ce que nous voyons à la télévision, avec des geeks à capuche qui travaillent devant des écrans verts, alors que nous avons besoin de très nombreux talents pour nous accompagner.

La quatrième activité de ce Campus Cyber sera l'animation des projets communs. L'événementiel et les prestations en matière de cybersécurité seront réalisés sur ce Campus Cyber. Nous ne voulons pas constituer une galerie marchande ou un hôtel d'entreprises, mais faire en sorte qu'il y ait beaucoup de collaboration. 30 % d'espaces seront réservés par des acteurs privés, 15 % par des acteurs publics, 11 % seront dédiés à l'accélération (espaces « pépites », visant à aider les PME françaises à se développer, grâce à la proximité avec les grands acteurs internationaux ou les grands clients), 6 % à la formation et 35 % constitueront des espaces collaboratifs. Lorsque vous louez 10 mètres carrés d'espace personnel, on vous facture 13 mètres carrés, pour financer ces espaces collaboratifs.

L'augmentation de capital sera finalisée le 15 avril : l'entrée au capital de l'État par l'intermédiaire de l'agence des participations de l'État (APE) sera réalisée le 30 avril. Nous sommes également en train de finaliser la prise à bail avec le propriétaire de l'immeuble, qui devrait être effective le 30 avril, pour pouvoir démarrer l'agencement du Campus Cyber et lancer les groupes de travail afin de déterminer ce qui y sera fait.

En France, l'écosystème de la cybersécurité est très morcelé. On retrouve de grandes entreprises comme Orange Cyberdéfense, Atos, Capgemini, Thales, mais également une myriade de petites entreprises assez spécialisées. La grande difficulté est de trouver des ressources, de l'expertise dans ce domaine.

Des travaux ont été menés par l'ANSSI, qui a créé les opérateurs d'importance vitale (OIV), référencé un certain nombre de prestataires.

Les grandes entreprises commencent à avoir un niveau de sécurité leur permettant de se protéger contre certaines typologies d'attaques, ce qui n'est pas le cas des petites entreprises. Les ransomwares visant les hôpitaux, les administrations, les collectivités territoriales et les petites entreprises créent systématiquement des dommages très importants. Or, le métier de ces établissements n'est pas la cybersécurité. Nous devons trouver des solutions pour pouvoir les sécuriser de la façon la plus transparente possible, et amener de l'expertise chez eux. 66 % des PME qui sont touchées par un ransomware déposent le bilan. Je pense que les 30 % restant ont payé la rançon. Nous faisons un vrai constat d'échec sur la

sécurisation des petites entreprises en France, qui nécessite une mobilisation pour les protéger au moins vis-à-vis des attaques basiques, du type des rançongiciels.

M. Philippe Latombe, rapporteur. Si nous revenons au Campus Cyber, avez-vous connaissance de projets similaires, y compris en gestation, dans d'autres pays européens ?

M. Michel Van Den Berghe. Non, nous sommes en avance sur le sujet. Nous avons cependant créé de l'envie, et je commence à être en relation avec des confrères en Italie, en Belgique et en Allemagne, qui estiment que notre projet est très intelligent et demandent que nous élaborions un kit de création d'un campus cyber. Pour l'instant, nous sommes vraiment en avance par rapport aux autres pays européens.

M. Philippe Latombe, rapporteur. Avez-vous des contacts avec la Commission européenne, pour essayer de faire de l'initiative quelque chose de plus européen et généraliste ?

M. Michel Van Den Berghe. Nous avons postulé pour constituer un *« European digital innovation hub » (EDIH)*, de sorte que le Campus Cyber puisse être annoncé comme un dispositif d'innovation européen. Nous sommes portés par la région Île-de-France dans cette démarche. Ce sera peut-être un moyen de nous faire connaître.

Je suis un entrepreneur et j'avance donc, pas à pas. La première étape était de créer cette SAS française et la capitaliser, en faisant en sorte que tous les acteurs aient leur voix dans la gouvernance. Malgré l'entrée au capital de grandes entreprises, j'ai tenu à ce que le conseil d'administration soit représentatif de l'ensemble de l'écosystème. Il y aura un siège pour les *start-up*, un pour les associations, un pour les personnes de la formation, un autre pour ceux de la recherche. Je suis en train de finaliser cette phase du travail.

Par ailleurs, lorsque l'on crée une entreprise, on ne prend généralement pas un immeuble de 26 000 mètres carrés. J'ai donc aussi pour tâche de rassurer le propriétaire de l'immeuble, qui est neuf, quant à la pérennité de la SAS et à sa capacité à payer ses loyers. Je travaille également à l'établissement des contrats de sous-location : sur 2 000 postes de travail disponibles, 1 920 sont d'ores et déjà pré-vendus, ce qui montre que l'écosystème répond présent. Certaines entreprises prendront un étage complet de l'immeuble, d'autres occuperont seulement un ou deux postes de travail, qui leur permettront de s'immerger au sein de ce Campus Cyber.

M. Philippe Latombe, rapporteur. Il est dit que le campus ne sera pas localisé uniquement à La Défense, mais qu'il essaimera en province. Avez-vous déjà un plan d'essaimage ?

M. Michel Van Den Berghe. Oui, nous avons rencontré l'ensemble des présidents de région. Certaines sont déjà en train de créer leur campus cyber, comme la région des Hauts-de-France, qui l'a fait avec la métropole de Lille et la ville de Lille. Nous avançons en parallèle : ils démarreront leur structure dès 2022 également. Je suis aussi en relation avec la région des Pays-de-Loire, pour examiner comment ils pourraient démarrer un campus cyber dans leur pôle d'innovation. Chaque région a manifesté son intérêt. Nous tenons absolument à pouvoir le réaliser : nous devons pouvoir amener la cybersécurité aux endroits où se font les grandes transformations numériques dans le pays. La région Rhône-Alpes est par exemple très en pointe sur l'industrie 4.0 : un campus cyber dédié à ces transformations doit y être constitué. Dans les Hauts-de-France, nous voulions travailler sur la sécurisation de l'écosystème des PME et la mise en place de solutions les plus transparentes possible. Dans les Pays-de-Loire, le travail porte sur la sécurisation des *smart cities*. L'idée est d'amener le concept de campus

cyber dans les régions, pour constituer des satellites communiquant entre eux, de sorte que l'on ne fasse pas un projet jacobin où toute l'expertise serait centralisée à Paris.

M. Philippe Latombe, rapporteur. Il s'agissait de ma question suivante, à laquelle vous avez commencé à répondre. Chaque nouveau centre régional aura-t-il une spécificité ou une thématique particulière et pourra-t-il communiquer directement avec les autres centres, sans nécessairement passer par le campus parisien ?

M. Michel Van Den Berghe. Exactement.

M. Philippe Latombe, rapporteur. Comment percevez-vous l'appétence des chefs d'entreprises et des élus locaux sur le sujet ? Sont-ils suffisamment informés des risques cyber aujourd'hui, ou reste-t-il de l'éducation à faire ?

M. Michel Van Den Berghe. Le risque cyber est considéré comme majeur dans les grandes entreprises : la prise de conscience est faite. On nous demande de plus en plus d'organiser de la sensibilisation, des exercices de gestion de crise, etc. Nous percevons que ce risque est aujourd'hui identifié, et nous nous faisons aider par les grandes compagnies d'assurance pour rappeler qu'en cas de risque cyber, les dommages sont assez importants. Une vidéo a circulé sur Twitter, diffusée par un maire qui a subi une attaque par un rançongiciel. Il notait que l'on a toujours l'impression de ne pas être concerné, et que les pirates ne s'intéressent pas à nous. Or, aucune municipalité n'est particulièrement visée : les pirates lancent l'attaque sur le réseau, et ceux qui ont les portes ouvertes laissent entrer le rançongiciel et se font encrypter leurs données, qui sont dès lors perdues, si elles n'ont pas été sauvegardées.

Dans l'automobile, la sécurité du véhicule est un critère de choix, sans que l'on demande aux utilisateurs de connaître le fonctionnement de l'ABS ou des airbags. Nous devons développer cette approche en matière de cybersécurité, par des campagnes de sensibilisation, sur le modèle des campagnes-chocs qui ont été menées en matière de sécurité routière. Il y a un vrai travail de sensibilisation à mener de la part de l'État, pour rappeler qu'Internet n'est pas le pays de Candy et que l'on est visible de tous et très fortement attaquable dès lors que l'on ne se protège pas. Il faut mener un vrai travail de sensibilisation, d'éducation, pour que les gens comprennent que le risque est avéré, et que l'on parvient très souvent, avec très peu d'investissement, à se protéger de 90 % des attaques.

M. Philippe Latombe, rapporteur. Pensez-vous que cela aille de pair avec le manque de candidats au suivi des formations et à l'entrée dans le monde de la cybersécurité ? Ce domaine n'est-il pas suffisamment attractif ? N'en parle-t-on pas assez ?

M. Michel Van Den Berghe. Vous avez tout à fait raison. La cybersécurité souffre d'un problème d'image. Nous avons une image anxiogène. Tous les reportages télévisés présentent des spécialistes de la cybersécurité avec des capuches devant leurs écrans, ne parlant à personne. Or, ce n'est pas du tout notre métier.

Lorsque nous intervenons sur des crises sensibles (celles des hôpitaux, celle de Pierre Fabre, etc.), nous sommes confrontés à une première étape de stupéfaction et de panique, les victimes pensant jusqu'à ce qu'elles soient atteintes qu'elles n'étaient pas ciblées. Nous aidons très souvent à calmer, à structurer la réponse et à éviter la propagation de l'attaque. Lorsque les pompiers interviennent sur un incendie, ils n'envoient pas de l'eau partout, mais coupent l'électricité, le gaz, s'assurent qu'il n'y a plus personne dans les locaux, etc. Dans une crise cyber, le réflexe est exactement le même. Dans une deuxième phase, nous essayons de faire fonctionner les systèmes du mieux que nous pouvons. La troisième phase est celle de la reconstruction.

Nous devons changer l'image des personnes de la cybersécurité, donner du sens à notre métier. Je pense qu'un jeune sur dix mille en terminale indiquerait vouloir travailler dans le domaine de la cybersécurité si on lui posait la question. Nous avons besoin de communicants, de personnes capables d'aider à reconstruire des systèmes d'information, de spécialistes du chiffrement de données, etc. Il existe de nombreux autres métiers que ceux de pentester ou de hacker éthique, que l'on cite très souvent. Nous devons changer l'image du métier de la cybersécurité. Nos grands dirigeants eux-mêmes, lorsqu'ils ont l'occasion de communiquer sur le numérique, préfèrent parler du quantique que de cybersécurité, car ils estiment que cela est moins anxiogène. Or, notre métier n'est pas anxiogène. Nous sommes les Casques bleus du numérique : nous devons protéger un territoire, protéger des personnes. Notre métier a beaucoup de sens, et nous devons le valoriser pour créer des vocations. Les formations existent, mais ne sont pas remplies ; nous devons faire venir les jeunes vers ces métiers de la cybersécurité, en changeant son image qui est aujourd'hui trop anxiogène.

M. Philippe Latombe, rapporteur. Ces métiers sont-ils pratiquement toujours tenus par des hommes, ou commence-t-il à y avoir des femmes ?

M. Michel Van Den Berghe. Des femmes commencent à y être présentes, surtout dans les équipes de conseil. Orange Cyberdéfense est par exemple passé de 8 % à 17 % de personnel féminin entre 2018 et 2020. Il reste beaucoup à faire, mais nous y travaillons, toujours en changeant cette image du monde de la cybersécurité.

M. Philippe Latombe, rapporteur. Nous avons parlé de formation initiale et d'attirer des jeunes, en changeant l'image de la cybersécurité. La formation professionnelle continue est-elle pour sa part suffisante afin que des directeurs des systèmes d'information (DSI) ou des responsables de la sécurité des systèmes d'information (RSSI) soient mis à niveau des menaces existantes, de leur évolution technologique, etc. ? Le Campus Cyber proposera-t-il des formations dans ce domaine ?

M. Michel Van Den Berghe. C'est exactement ce que nous souhaitons faire.

Les formations doivent, en premier lieu, mettre à niveau les professionnels de la cybersécurité par rapport aux nouvelles typologies d'attaque. Les pirates sont extrêmement créatifs, et chaque innovation crée de nouvelles fenêtres de vulnérabilité. L'Internet des objets (IoT) créera de nouvelles vulnérabilités. Si ces objets ne sont pas référencés et, un minimum, sécurisés lorsqu'ils seront connectés au réseau, ils constitueront des portes d'entrée supplémentaires. La 5G créera également de nombreuses possibilités de connexions d'objets, et augmentera donc la vulnérabilité. Nous devons donc former les acteurs, ce qu'il est prévu de faire sur le Campus Cyber pour que les RSSI et les DSI soient mis à niveau.

Nous essaierons en deuxième lieu de réaliser du *rescaling* d'ingénieurs réseau, d'ingénieurs de production informatique, de développeurs, qui ont envie d'aller vers le métier de la cybersécurité. Certaines grandes entreprises ont monté leurs propres formations pour faire du *rescaling* de ressources : nous l'avons fait chez Orange, EDF l'a fait, de même que BNP. Plutôt que laisser chaque entreprise mener ce travail de façon artisanale en son sein, nous voulons structurer la démarche, en nous faisant aider, par exemple, par l'ANSSI, qui pourrait dispenser des formations. La formation de ce type de populations à la cybersécurité est très rapide.

Le troisième point est que beaucoup d'écoles d'ingénieurs forment à la cybersécurité, mais que nous avons également besoin de techniciens supérieurs dans ce domaine. D'où la création de ce *bachelor* avec l'EPITA, pour augmenter le nombre de spécialistes en cybersécurité. Lorsque vous placez des ingénieurs derrière des consoles de cyberSOC (le

système qui permet de surveiller ce qu'il se passe sur les réseaux), ils partent après trois mois. Nous devons également former des personnes à bac+2 ou bac+3 en école d'ingénieur, pour que l'expertise ne se trouve pas uniquement chez des personnes titulaires d'un bac+5. Nous avons besoin de bac+2 pour installer des matériels destinés à la sécurité périmétrique dans les entreprises, paramétrer des sondes réseau, etc. C'est ce que nous voulons faire sur le Campus Cyber.

M. Philippe Latombe, rapporteur. Beaucoup de projets de *smart cities* démarrent actuellement, pour des raisons de calendrier – puisque les maires ont été élus l'année dernière. Intègrent-ils suffisamment la cybersécurité dès l'origine, ou s'agit-il d'une préoccupation qui émerge à la fin du projet ? De même, les PME et ETI qui développent leurs systèmes d'information intègrent-elles la cybersécurité dès le départ ? Si ce n'est pas le cas, comment faire en sorte que la cybersécurité soit à l'avenir prise en compte en amont des projets ?

M. Michel Van Den Berghe. C'est toute la problématique que nous essayons de traiter par le *secure by design*. La cybersécurité est toujours traitée à la fin des projets, et comme ces derniers sont toujours en retard, elle est fréquemment oubliée. Je suis intervenu à la suite des attaques des hôpitaux : quand on voit les « cochonneries » qui sont connectées aux réseaux de ces établissements, il ne faut pas s'étonner qu'ils subissent des cyberattaques. Il faut en premier lieu interdire la connexion à des réseaux sensibles d'outils, d'objets connectés, de systèmes d'information qui ne sont absolument pas protégés. Il convient également d'inculquer le *secure by design*, en expliquant aux fournisseurs de ces solutions que la cybersécurité est un facteur différenciant, et qu'à prix égal, un client préférera retenir une solution dans laquelle la cybersécurité a été pensée.

Nous revenons au fait qu'il s'agit d'un problème d'éducation et de sensibilisation. Si la cybersécurité est prise en compte à l'origine, le projet n'est absolument pas ralenti, au contraire, et les systèmes d'information ne seront pas complètement piratables.

On attaque aujourd'hui les données des entreprises. Dans cinq ans, les rançongiciels toucheront les particuliers : lorsque les maisons seront complètement connectées, on exigera des personnes qu'elles paient une rançon directement avec leur smartphone pour pouvoir ne serait-ce qu'entrer chez elles. De même, la numérisation des *smart cities* est une bonne chose, mais si le pirate prend la main sur une ville connectée, il est capable de faire n'importe quoi. Il faut donc vraiment sensibiliser maintenant les personnes à prendre en compte le risque. Pour être très franc, ce n'est pas du tout fait aujourd'hui.

M. Philippe Latombe, rapporteur. En ce sens, le gouvernement a débloqué des fonds dédiés aux collectivités territoriales en matière de cybersécurité. Sont-ils suffisants ?

M. Michel Van Den Berghe. Il s'agit d'un premier pas très important. La création d'antennes régionales permettant de mettre en place des systèmes sécurisant les collectivités locales, les hôpitaux, etc., est un excellent premier pas. Le plan de relance et d'accélération cyber, avec le milliard d'euros consacré au développement des outils cyber est extrêmement important. La prise de conscience est là : il faut maintenant accompagner l'ensemble des collectivités territoriales et protéger les plus faibles. On le voit : pour attaquer une grande entreprise, le pirate vise fréquemment son sous-traitant, qui est plus vulnérable, et peut faire entrer le virus dans le système d'information de la grande entreprise. Nous devons nous mobiliser pour proposer des solutions aux très petites entreprises (TPE), qui n'ont parfois même pas de DSI. Si nous ne les aidons pas, elles constitueront des portes d'entrée vers les administrations ou les grandes entreprises.

M. Philippe Latombe, rapporteur. Qui serait selon vous le bon prescripteur ? Serait-ce Bpifrance ? Je ne parle pas des grands groupes, qui peuvent par ruissellement demander à leurs sous-traitants de se sécuriser, ce qu'ils ont commencé à faire, mais pour tous les acteurs qui ne se trouvent pas dans cette situation, quel serait le bon prescripteur de la réflexion cyber, au-delà du Campus Cyber, qui constitue en soi un centre de ressources ? Le prescripteur devrait-il être Bpifrance, lorsqu'elle investit pour numériser ou modifier le système d'information, l'expert-comptable, l'un des interlocuteurs assez naturels des dirigeants de PME, TPE ou même ETI ? Quel est selon vous le bon niveau ?

M. Michel Van Den Berghe. C'est véritablement la question que nous nous sommes posée. Selon nous, trois acteurs atteignent un maximum de ces entreprises. Le premier est le banquier, car toutes les entreprises ont un compte en banque : les banquiers pourraient proposer une solution la plus simple possible à télécharger sur un kiosque pour protéger les PC. La Poste est également un interlocuteur évident : tout le monde reçoit du courrier, et il existe une relation de confiance avec le facteur. Enfin, les opérateurs réseau qui apportent de la connectivité pourraient également proposer des solutions simples à installer, pour fournir un minimum de cybersécurité.

Sans faire de publicité à Orange Cyberdéfense, je suis précisément en train de travailler sur le sujet, en essayant d'inciter Orange France à mettre en place une solution que nous sommes en train de construire avec les sociétés françaises Tehtris et Vade Secure. Il s'agit d'une solution de type *endpoint detection and response (EDR)*, qui remplace l'antivirus et isole un poste de travail du réseau lorsqu'elle y détecte des comportements malveillants, afin d'éviter la contamination de l'ensemble de l'entreprise. Vade Secure apporte une solution d'*antifishing*, qui détecte les pièces malveillantes dans les mails et les met de côté, permettant d'éviter que les utilisateurs cliquent dessus et infectent leur poste de travail. Nous essayons également de faire en sorte que la solution soit très peu chère : la campagne que nous mènerons sera intitulée « Votre cybersécurité pour le prix d'un café ». Nous souhaitons que cette solution coûte moins de 40 centimes d'euro par jour.

J'incite Orange France à proposer cette application avec les *box* pour professionnels. Nous pourrions le faire également avec les banquiers, avec les assureurs, qui pourraient diminuer la police d'assurance moyennant cette amélioration de la sécurité.

Chez Orange, le marché des professionnels et des PME, constitué des entreprises de moins de cinquante salariés, regroupe cinq millions de clients. En Europe, ces sociétés représentent 99 % des entreprises. Il existe donc un intérêt y compris financier à proposer ce type de solutions. Je me bats chez Orange pour qu'une solution soit proposée sur un kiosque, à destination des entreprises d'un à cinq salariés, afin qu'elles disposent d'un dispositif d'antivirus, de détection comportementale et d'*antifishing* pour trente ou quarante centimes d'euro par poste de travail et par jour. Les clients adhéreraient assez facilement à un tel outil.

M. Philippe Latombe, rapporteur. Nous avons parlé des clients. Si nous parlons de l'offre, vous avez évoqué dans votre propos liminaire le morcellement des acteurs, qui travaillent sur des segments parfois compatibles ou complémentaires les uns des autres. Comment structurer l'ensemble ? L'objet du Campus est-il précisément d'agréger les solutions, pour pouvoir aborder les marchés de façon commune, ou s'agit-il simplement de faire émerger les entreprises en dehors de cette logique ? À terme, le marché peut-il rester aussi hétérogène ?

M. Michel Van Den Berghe. Vous pointez bien la faiblesse du marché de la cybersécurité. Les quatre grandes entreprises industrielles du secteur représentent 80 % du marché, ce qui n'est pas idéal. Orange Cyberdéfense cherche à faire de la croissance externe,

mais ne trouve pas d'entreprises à acheter, y compris en Europe, hormis des sociétés qui réalisent 20 à 25 millions d'euros de chiffre d'affaires. Nous trouvons peu de cibles potentiellement accessibles.

Il faut parvenir à structurer ce marché de la cybersécurité, l'amener dans les régions, car la proximité est extrêmement importante. L'objectif du Campus Cyber est précisément d'aider à faire connaître ces PME, qui apportent de la cybersécurité dans les régions. Quelques entreprises sont assez fortes dans leurs différentes régions – Advens à Lille, Tehtris à Bordeaux, etc. Nous devons créer un maillage, et faire en sorte que les gens se parlent pour élever le niveau global de cybersécurité. Notre premier objectif est de créer une base de marqueurs, pour que les personnes qui font de la détection puissent s'y connecter. Chacun doit oublier un peu la concurrence pour que le même niveau de détection soit possible partout dans le pays.

Nos *start-up* doivent également pouvoir évoluer et s'internationaliser sans nécessairement aller chercher des fonds outre-Atlantique. Il ne faut plus que les entreprises françaises qui commencent à bien fonctionner sur le territoire national soient obligées de créer un siège social à San Francisco pour pouvoir rayonner aux États-Unis. Il est possible de procéder autrement, mais nous devons nous en donner les moyens. Nous devons conserver des entreprises françaises capables de s'adresser à des clients internationaux sans basculer leur siège social aux États-Unis.

M. Philippe Latombe, rapporteur. On nous dit très régulièrement, lors des auditions, que l'amorçage est une bonne chose, mais qu'il importe plus d'avoir des clients que des subventions. L'État joue-t-il aujourd'hui correctement son rôle de client ? Peut-il mieux faire, et le cas échéant comment ? Les grandes entreprises, qui ne suivent pas des procédures de marchés publics, mais ont de grands besoins, font-elles, de leur côté, suffisamment d'efforts pour recourir à des *start-up* ?

Par ailleurs, vous indiquez ne pas trouver de cibles à acheter. Or, on nous explique depuis le début des auditions que personne ne veut les acheter en France, et qu'il est obligatoire de se vendre à l'étranger. Comment résolvons-nous ce paradoxe ?

M. Michel Van Den Berghe. La question est très pertinente. En France, nous sommes très doués pour incuber. De très nombreuses sociétés sont placées dans des couveuses, soutenues par des banques, bénéficient de bureaux, de moyens de se développer, etc. La phase la plus compliquée est celle de l'industrialisation et du décrochage de grands clients permettant à ces entreprises d'avoir une autonomie de financement assez importante.

J'ai été entrepreneur. Lorsque vous créez votre solution, même si elle est extrêmement pertinente, et que vous vous retrouvez face aux acheteurs des grandes sociétés françaises, ils constatent que les techniciens ont validé la solution, mais vous demandent vos trois derniers bilans, demandent la garantie que vous êtes capable de payer un million d'euros de pénalités si la solution détériore le système d'information de l'entreprise, etc. Toutes ces contraintes liées aux politiques d'achat expliquent qu'il n'est pas possible de servir ces grandes sociétés.

Le combat que j'ai mené avec Orange Cyberdéfense vise à répondre à cette difficulté. Lorsqu'une société est pertinente d'un point de vue technologique, nous la plaçons très rapidement à notre catalogue, pour rassurer les clients potentiels. Orange Cyberdéfense, société qui réalise 800 millions d'euros de chiffre d'affaires, prend en charge la contractualisation, couvre les risques de pénalité, etc. Cela accélère véritablement la possibilité pour des petites entreprises d'atteindre de très grands comptes.

Le dernier exemple en date est la société Alcide, créée à Annecy.

M. Philippe Latombe, rapporteur. Nous en avons entendu parler.

M. Michel Van Den Berghe. Orange Cyberdéfense a mis Alcide à son catalogue et a incité ses propres clients à acheter ses solutions, en prenant en charge les problématiques de référencement et d'achat. *In fine*, Alcide a été racheté par une société américaine, pour un montant de 100 millions d'euros – ce qui est heureux pour les fondateurs, mais casse la concurrence. Personne en France ne peut investir 100 millions d'euros pour acheter Alcide. Cette valorisation est complètement délirante. La valorisation des cibles du marché de la cybersécurité est pour nous de l'ordre de 20 à 25 % de l'EBITDA. Je ne peux pas demander au conseil d'administration de valider l'acquisition d'une entreprise pour un montant de vingt à vingt-cinq fois son EBITDA, quand Orange Cyberdéfense est pour sa part valorisée deux à trois fois son EBITDA. Le marché est survalorisé. Aucune entreprise française ne peut débourser 100 millions d'euros pour acheter Alcide, qui réalise 8 millions d'euros de chiffre d'affaires.

M. Philippe Latombe, rapporteur. Pour quelle raison l'acquéreur est-il prêt à payer cette somme ? Il existe bien une raison économique chez l'acheteur. Nous ne parlons pas de philanthropie, ou de l'achat du *Salvator Mundi*. Alcide n'est pas un trophée que l'on affiche dans une vitrine.

M. Michel Van Den Berghe. Il existe certainement un intérêt. Je suis plus un technicien qu'un financier, mais c'est la rareté des opportunités qui explique des valorisations aussi délirantes. Alcide propose une technologie excellente, qui gère la sécurisation du référencement des utilisateurs. Son seul concurrent est Microsoft. Cela peut effectivement être intéressant pour une entreprise américaine, qui, vu sa portée, pourra peut-être dégager très rapidement de la rentabilité. Lorsque vous achetez une entreprise vingt-cinq fois la valeur de son EBITDA, cela signifie cependant qu'il faut vingt-cinq ans pour rentabiliser l'investissement. Il faut donc être certain que les synergies d'acquisition permettront de diviser le coût par deux. Dans notre métier, les valorisations sont de manière générale un peu délirantes.

M. Philippe Latombe, rapporteur. Les grandes entreprises achètent relativement cher ces sociétés, c'est-à-dire une vingtaine de fois l'EBITDA plutôt que deux à trois fois l'EBITDA. Est-ce parce qu'elles achètent quelque chose qu'elles ne maîtrisent pas, ou qui est en concurrence potentielle avec ce qu'elles sont en train de développer et qu'elles veulent donc détruire ? Que faudrait-il faire en France pour préserver ces sociétés, ou pour procéder de même ? Ne disposons-nous pas de suffisamment de grandes entreprises capables de réaliser ces acquisitions ?

M. Michel Van Den Berghe. C'est un peu ce que nous essayons de construire : nous voulons créer des industriels européens capables de « challenger » les grands acteurs américains. Si nous étions déjà capables d'accompagner toutes les entreprises européennes dans leur mondialisation, on offrirait un terrain de jeu extrêmement important. Nous devons créer des acteurs européens capables de « challenger » ces grands acteurs américains, et de peser face aux GAFA. Palo Alto, etc., qui sont visionnaires dans la transformation numérique et achètent des *start-up* qui ont déjà développé des solutions, pour ne pas avoir à le faire eux-mêmes. Même s'ils ont commencé à travailler dans le domaine, mais qu'une *start-up* est allée plus vite, ils l'achètent, la mettent à leur catalogue et sont en avance sur le marché. Nous devons créer ces acteurs français, européens, capables de rivaliser avec les grands acteurs américains pour acquérir les entreprises innovantes et positionner leurs offres sur le marché mondial.

Nous commençons à le faire. Nous l'avons par exemple aux États-Unis et; c'est la première fois qu'un acteur européen pénètre le marché américain, peut-être grâce à l'image plus transparente des entreprises européennes en matière de données. Nous devons créer de grands acteurs européens, avec la même expertise que les grands acteurs américains, pour créer de la valeur. Toutes les grandes entreprises européennes doivent être accompagnées dans leur conquête du marché mondial. Nous avons, par exemple, créé un *data center* en Chine pour accompagner un géant du luxe souhaitant pénétrer le marché chinois. Nous avons fait de même pour un fabricant de meubles suédois, qui voulait attaquer le même marché, car les données du personnel et des clients doivent rester sur le territoire chinois. Nous sommes capables de le faire, mais nous devons accélérer pour atteindre une taille nous permettant de lutter contre les GAFA et un jour peut-être investir les mêmes montants pour éviter que nos pépites françaises soient achetées par des entreprises américaines.

M. Philippe Latombe, rapporteur. Le Campus Cyber permettra-t-il aux *start-up* françaises, mais également à l'ensemble de l'écosystème, de « chasser en meute » ?

M. Michel Van Den Berghe. C'est exactement ce que nous voulons faire. Nous voulons nous rassembler pour pouvoir « chasser en meute », et créer la connexion. La France réussit très bien la phase d'incubation. Nous devons désormais créer des liens pour que les *start-up* devenues des PME soient très rapidement mises au catalogue des grands industriels, et que ces derniers les aident à se développer et à proposer leurs solutions dans l'ensemble du territoire. Lorsque Thales ou Atos mettent à leur catalogue la technologie d'une PME française, celle-ci se développe beaucoup plus vite, car elle peut atteindre de grands comptes. C'est la phase d'industrialisation qui est compliquée pour les PME.

J'ai revendu Atheos à Orange, parce que les grands comptes estimaient que l'entreprise commençait à prendre trop de poids à l'intérieur de grands industriels français, et que sa puissance financière les dérangeait. J'ai donc décidé de m'adosser à un grand industriel pour continuer à monter en expertise et en puissance au sein de ces grands comptes. Il s'agit d'une belle réussite : le chiffre d'affaires d'Atheos était de 30 millions d'euros en 2014, en y ajoutant les activités d'Orange, le périmètre était de l'ordre de 80 millions d'euros. Orange Cyberdéfense réalise en 2020 près de 800 millions d'euros de chiffre d'affaires.

Lorsque nous créons un acteur français capable d'apporter la même expertise que les sociétés américaines, les clients suivent. Tout le CAC 40 est aujourd'hui client d'Orange Cyberdéfense, et a choisi, à expertise égale, l'acteur français plutôt que son concurrent américain.

M. Philippe Latombe, rapporteur. J'en viens à ma dernière question. Comment gérer l'extraterritorialité américaine ? Devons-nous jouer avec, créer nos propres règles en Europe ? Comment voyez-vous les choses ?

M. Michel Van Den Berghe. Nous devons créer nos propres règles en Europe.

Lorsque nous avons créé le Campus Cyber, de nombreux acteurs américains et chinois m'ont demandé d'y participer, de prendre des actions, etc. Je leur ai demandé de nous laisser nous organiser avec des acteurs français, peut-être des acteurs européens, en remarquant qu'un Campus Cyber aux États-Unis n'accepterait pas Orange Cyberdéfense dans sa gouvernance sans rien lui demander en contrepartie. L'Europe doit s'organiser pour créer une régulation du marché de la cybersécurité. Cette « meute » française doit être organisée au niveau de l'Europe, pour que nous puissions faire émerger ces grands acteurs de la cybersécurité et pouvoir attirer les grandes sociétés internationales.

M. Philippe Latombe, rapporteur. Quels points n'aurions-nous pas abordés, que vous voudriez évoquer ?

M. Michel Van Den Berghe. Il ne s'agit pas de votre première audition, et vous avez à mon avis bien cerné les questions. Les sujets sur lesquels nous devons travailler ensemble sont la sensibilisation de l'écosystème industriel à la problématique de la cybersécurité et le changement d'image de la cybersécurité, pour créer des vocations, expliquer que la cybersécurité n'est pas anxiogène, que ce métier a beaucoup de sens. Nous avons besoin de spécialistes de la législation, de la communication, etc., et de supprimer l'image que nous voyons trop souvent dans les reportages du geek avec une capuche, que je ne supporte plus.

M. Philippe Latombe, rapporteur. Nous ne vous en présenterons pas.

M. Michel Van Den Berghe. Nous devons changer cette image.

La perception du sujet par les dirigeants doit aussi évoluer. Au départ, lorsque nous voulions intervenir dans les comités exécutifs, on nous expliquait que le sujet était trop anxiogène et technique. Les mentalités commencent à changer. Il faut expliquer que la cybersécurité fait partie de la transformation numérique et qu'en la prenant en compte le plus rapidement possible, par le *secure by design*, on s'évite bien des problèmes.

Audition, ouverte à la presse, de M. Arnaud Dechoux, responsable des affaires publiques « Europe », de la société Kaspersky (13 avril 2021)

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. Nous poursuivons nos auditions consacrées aux enjeux du cyber, en présence de M. Arnaud Dechoux, responsable des affaires publiques de la société Kaspersky France.

Notre mission s'intéresse au sujet de la cybersécurité et de la cyberdéfense, qui constituent le cœur de la souveraineté numérique, entendue dans le sens le plus fondamental. Nous avons souhaité vous entendre comme représentant d'une société multinationale russe, spécialisée dans la sécurité des systèmes d'information, et connue évidemment pour sa solution antivirus. Nous sommes intéressés par votre regard et celui de votre société, en tant qu'acteur n'appartenant pas à l'Union européenne, sur la préoccupation croissante des États membres de celle-ci vis-à-vis de l'enjeu de souveraineté numérique. Nous aurons également l'occasion, je l'espère, d'aborder votre manière de voir l'actualité cyber européenne. Vous avez organisé le 23 mars dernier un échange sur le sujet avec plusieurs acteurs importants, dont M. Guillaume Poupard, le directeur général de l'agence nationale de sécurité des systèmes d'information (ANSSI), M. Bart Groothuis, eurodéputé et rapporteur de la directive NIS2. J'espère que vous pourrez nous en dire un mot.

M. Philippe Latombe, rapporteur. Je souhaite évoquer trois sujets.

La première question est rituelle dans cette mission et porte sur la façon dont vous appréhendez la notion de souveraineté numérique. Dans nos différentes auditions, nous avons entendu une grande diversité de définitions. Je voudrais donc savoir ce que recouvre, sous l'angle cyber, ce concept que l'on rapproche parfois d'une forme d'autonomie stratégique et décisionnelle. Comment vous positionnez-vous face au souhait de certains États membres de privilégier des solutions de sécurité européennes pour des raisons de souveraineté ?

En second point, je voudrais que nous échangions sur le secteur de la cybersécurité. Quel est votre positionnement sur le marché des antivirus, et son actualité en Europe et dans le monde ? Comment faites-vous en sorte de rester à l'état de l'art face à l'évolution des menaces ? J'aimerais que vous partagiez votre regard sur l'évolution de la menace, tant en ce qui concerne sa nature que ses modalités. Très concrètement, comment les attaques subies par vos clients ont-elles évolué ? Ceux-ci avaient-ils renforcé leur protection numérique pendant la crise sanitaire ? Comment inciter les entreprises à mieux se protéger dorénavant, afin de limiter autant que possible les conséquences d'éventuelles atteintes à leurs systèmes d'information ?

Enfin, j'aimerais revenir sur la question de la protection des données personnelles, qui est un sujet majeur en Europe. Comment percevez-vous cet impératif, en tant qu'acteur non européen ? Comment garantissez-vous la sécurité des données de vos clients, alors que certains vous accusent d'avoir favorisé l'installation de *backdoors* au sein de systèmes informatiques au profit de la Russie ?

Je rejoins M. le président pour conclure sur l'actualité cyber européenne, sur laquelle nous aimerions aussi évidemment vous entendre.

M. Arnaud Dechoux, responsable des affaires publiques « Europe », de la société Kaspersky. Si vous me le permettez, je voudrais présenter très rapidement Kaspersky, pour expliquer qui nous sommes, ce que nous faisons et ce que nous ne faisons pas. L'entreprise a été fondée en 1997 par Eugène Kaspersky, qui reste aujourd'hui son président-directeur général et son propriétaire. Avec un chiffre d'affaires d'environ sept cents millions de dollars, Kaspersky est la première entreprise privée de cybersécurité au niveau mondial. Elle emploie environ quatre mille salariés dans le monde, dont plus d'un tiers en R&D. L'entreprise a l'originalité d'être une multinationale d'origine russe, dans un secteur où les grands acteurs sont souvent d'origine anglo-saxonne. L'Europe constitue aujourd'hui, de loin, notre première zone d'activité : 40 % environ de notre chiffre d'affaires sont aujourd'hui réalisés en Europe. Nous attachons donc beaucoup d'importance aux considérations européennes, entre autres sur les sujets de souveraineté numérique.

Kaspersky est initialement connu pour son moteur antivirus très efficace, mais est aujourd'hui bien autre chose. Nous avons deux segments d'activité. En premier lieu, le segment grand public constitue environ 50 % de notre activité : il s'agit de la protection des ordinateurs, de gestionnaires de mots de passe, de réseaux privés virtuels (VPN) ou encore de solutions de contrôle parental. La deuxième moitié concerne les services aux entreprises et organisations ; environ deux cent soixante-dix mille organisations sont clientes de Kaspersky, de la très petite entreprise (TPE) ou petite et moyenne entreprise (PME) à la multinationale, en passant par de nombreuses organisations publiques. Nous parlons en l'occurrence de solutions de protection des postes de travail, mais aussi de sondes réseau ou de protections pour le milieu industriel, qui est également très ciblé aujourd'hui par les cyberattaques, d'outils de protection des objets connectés, ou encore de chiffrement des infrastructures *cloud*, mais aussi de programmes de sensibilisation à la cybersécurité.

La dernière activité sur laquelle je voulais insister est celle des services *threat intelligence*, autrement dit de renseignement cyber sur les menaces avancées. Très concrètement, ce sont des flux d'informations à destination des agents de cybersécurité, des grandes entreprises, des intégrateurs, qui possèdent en interne des *computer emergency response teams* (CERT) ou des *security operations centers* (SOC), c'est-à-dire des équipes chargées de réaliser de la veille cyber. L'objectif pour ces acteurs est de mieux connaître la menace, de mieux s'y préparer et de mieux gérer les risques cyber. Chez Kaspersky, cette activité est gérée par une équipe appelée *Global research analysis team* (GReAT) : quatre chercheurs en France sont spécialisés sur ces sujets.

Nous comptons quatre cents millions d'utilisateurs dans le monde pour nos différents services. C'est précisément cette présence internationale qui nous permet de suivre en temps réel l'évolution des cybermenaces dans les différents pays. Les utilisateurs qui le souhaitent nous remontent, après avoir accepté cette modalité par un système d'*opt-in,* des données de télémétrie, qui permettent d'analyser les fichiers malveillants auxquels ils sont confrontés, en particulier ceux que nous ne connaissons pas encore. L'objectif est d'analyser ces derniers pour mieux les identifier à l'avenir.

Kaspersky emploie 70 personnes en France, où elle existe depuis une quinzaine d'années. L'entreprise est membre de la plateforme Cybermalveillance depuis 2017, acteur que vous avez auditionné et qui nous semble extrêmement important pour sensibiliser et instaurer une véritable culture d'hygiène numérique parmi les citoyens et les petites entreprises. L'entreprise est également signataire, depuis 2018, de l'Appel de Paris pour la confiance et la sécurité du cyberespace. Dans ce cadre, nous codirigeons depuis quelques mois avec le Cigref l'un des groupes de travail mis en place par le ministère de l'Europe et des affaires étrangères, pour apporter des outils concrets aux signataires de l'Appel.

L'un des maîtres mots de Kaspersky, en France comme dans le monde, est la transparence, pour répondre à des risques, fussent-ils théoriques, et à un éventuel manque de confiance, tel qu'il a pu exister. L'entreprise a mis en place depuis 2017 une initiative mondiale de transparence (*global transparency* initiative, GTI), qui nous semble l'un des programmes les plus avancés, voire le plus avancé dans le domaine. Il s'agit également d'une réponse aux enjeux de souveraineté de nos clients. Nous pourrons y revenir si vous le souhaitez.

Je vous propose de revenir sur quelques évolutions récentes du paysage des cybermenaces, notamment du fait de la crise sanitaire, mais non uniquement.

Kaspersky distingue classiquement trois types de menaces. Le premier est celui de la cybercriminalité traditionnelle, qui représente environ 80 % du volume des fichiers que nous détectons. Ces menaces sont en réalité assez faciles à détecter, et se traitent automatiquement. Il s'agit souvent de criminels traditionnels qui se sont mis au cyber, en considérant qu'il procédait d'un bon *business model*, avec des risques limités.

Le deuxième étage est celui des menaces ciblées, qui visent principalement des organisations. Elles représentent environ 20 % du volume total des détections, et sont déployées par des groupes d'attaquants beaucoup plus spécialisés, organisés, voire très professionnels. Les rançongiciels en sont un très bon exemple.

La dernière catégorie est celle des cyberarmes, déployées par des groupes étatiques ou paraétatiques ; elles ne représentent que 0,01 % du volume, mais ces attaques sont très visibles. Elles peuvent avoir des objectifs d'espionnage ou de sabotage, voire des visées financières dans certains cas très précis – je pense notamment aux attaques de la Corée du Nord cherchant à obtenir des devises. Dans cette dernière catégorie, la question de l'attribution des cyberattaques est une tâche très complexe.

Nous constatons une augmentation constante des cyberattaques depuis la création de Kaspersky. En 1994, on détectait un nouveau virus ou fichier malveillant par heure : le rythme est passé à un virus par minute en 2006, un virus par seconde en 2011. Les chiffres continuent à augmenter : 350 000 virus étaient détectés chaque jour en 2019 ; en 2020, en partie à cause de la situation sanitaire et du confinement, on atteignait 428 000 virus par jour, soit une progression de 25 % des détections en un an. La situation liée à la covid-19 et aux restrictions de déplacements a entraîné une augmentation de certains types de cyberattaques. Je pense notamment aux attaques de services d'accès à distance (*remote desktop protocol*, RDP) ou aux rançongiciels ciblés sur les établissements de santé, par exemple. Nous essayons néanmoins de relativiser ce constat en observant qu'il n'y a pas eu de progression exponentielle, mais une progression stable des attaques. La progression de ces derniers mois est également due à l'élargissement de la surface d'attaque : augmentation du temps passé sur Internet, du travail à distance, avec des équipements souvent moins bien protégés que ceux des entreprises, et recours à des ressources éducatives en ligne. Dans ce dernier cas, nous avons vu d'autres types d'attaques, comme celles par déni de service (DDoS), qui se sont beaucoup développées lors du premier confinement en mars dernier, et la semaine dernière encore en France. Ceci est dû aussi bien sûr au développement des objets connectés.

Pour finir, je voudrais revenir sur plusieurs tendances récentes que nous avons observées.

La première est le développement des attaques sur mobile. On protège aujourd'hui largement son ordinateur, mais on pense rarement à son smartphone, qui contient pourtant toute notre vie numérique. Il s'agit selon nous d'un axe de progrès important.

L'explosion des rançongiciels ciblés, qui visent beaucoup les entreprises, collectivités territoriales et établissements de santé, est une autre tendance majeure. Nous avons constaté au cours des deux dernières années un transfert des rançongiciels non discriminés, visant des dizaines de milliers de personnes, dont beaucoup de simples utilisateurs, à un ciblage ces derniers mois des grandes organisations, en particulier les grandes entreprises, qui ont les moyens de payer et sont plus susceptibles de le faire, car la perturbation de l'activité risque de fortement impacter la vie de leurs utilisateurs.

Un troisième phénomène est la structuration importante et la professionnalisation de l'écosystème cybercriminel. C'est notamment le cas pour les rançongiciels dont nous venons de parler. On a souvent l'impression que l'entreprise a affaire à un seul groupe de hackers, mais elle est en réalité confrontée à une dizaine de parties prenantes distinctes, l'un des groupes se chargeant du développement du rançongiciel, le deuxième fournissant les accès, un troisième se chargeant du contact client (certains faisant même appel à un standard téléphonique pour faire des relances), un autre encore se chargeant du blanchiment d'argent. Il s'agit aujourd'hui d'un écosystème très complexe, très structuré, et contre lequel il est d'autant plus difficile de lutter. C'est pour cette raison que la collaboration nous semble importante.

Enfin, les attaques dites par chaîne d'approvisionnement (*supply chain)* visent la chaîne logistique, et consistent souvent à passer par un sous-traitant pour atteindre la cible finale. Un exemple a fait beaucoup de bruit, depuis le mois de décembre 2020, avec l'attaque, sans doute liée à de l'espionnage, de Sunburst sur les produits SolarWinds, qui a notamment affecté des entités américaines. Sur ce type de sujets, de même que pour les attaques d'infrastructures critiques, nous avons constaté une montée en compétences des cyberattaquants, et un activisme accru de certains acteurs que l'on ne voyait pas auparavant. Je pense en l'occurrence à des États, qui ont développé leur capacité cyber et montent en compétences sur les cyberarmes, éventuellement en achetant des outils sur les marchés noirs à d'autres acteurs.

En conclusion, je dirais qu'au vu de tous ces enjeux, il est essentiel de promouvoir la cybersécurité par conception, voire la cyberimmunité des produits. C'est un concept que nous essayons de promouvoir, et qui consiste à redémarrer sur la base de systèmes d'exploitation totalement sécurisés. Beaucoup de systèmes de contrôle industriel (*supervisory control and data acquisition*, SCADA) ont été *designés* il y a des dizaines d'années et ne sont plus au niveau. Ils imposent de redémarrer de zéro. La sécurité par conception, le partage d'informations et les partenariats publics-privés sont essentiels.

Cyber Malveillance et le Cyber Campus, que vous avez je crois auditionnés, nous semblent des acteurs clefs dans ce domaine. La collaboration est le seul moyen qui nous permettra de répondre efficacement aux cybermenaces en constante évolution.

M. Philippe Latombe, rapporteur. Selon vous, qu'est-ce que la souveraineté numérique ? Vous êtes Européen, mais travaillez pour une société non européenne : comment voyez-vous cette notion monter ? Progresse-t-elle assez vite pour être perçue comme un enjeu, par exemple un frein, pour Kaspersky ?

M. Arnaud Dechoux. Nous sommes nés en Russie, mais pas un acteur tout à fait russe aujourd'hui. La société est immatriculée à Londres. Kaspersky France est une structure totalement française.

M. Philippe Latombe, rapporteur. Vous restez non européens.

M. Arnaud Dechoux. Ce n'est effectivement plus un bon argument, sinon pour les aspects culturels.

La notion de souveraineté numérique est évidemment un sujet extrêmement important. Un acteur international comme Kaspersky a pu observer la montée de ces enjeux de souveraineté partout dans le monde. Le terme de souveraineté numérique n'est pas forcément celui qui est utilisé ailleurs, et l'on peut nous demander, en Russie ou dans d'autres pays, ce que signifie exactement cette notion, qui est surtout utilisée en Europe.

Le concept se décline selon nous à trois niveaux – la souveraineté des États, celle des organisations et celle des utilisateurs ou citoyens, avec des enjeux distincts. Pour ce qui est de la souveraineté des solutions et des services numériques, nous pensons à plusieurs grands principes. Sans surprise, elle implique pour les utilisateurs le contrôle complet de leurs données (savoir où elles vont, pouvoir choisir avec qui elles sont partagées). Du point de vue du commanditaire, que ce soit un État ou une entreprise, elle renvoie à la maîtrise et à la connaissance des solutions informatiques utilisées. Le Cigref soulignait que les outils informatiques sont censés faire ce qu'ils doivent faire, et rien d'autre. Nous adhérons pleinement à cette définition. Cela passe beaucoup par la transparence des éditeurs des solutions de cybersécurité ou d'autres solutions. La possibilité d'auditer le code source, que nous avons essayé de promouvoir par notre initiative mondiale de transparence, nous semble à cet égard un axe clef.

Vous avez mentionné le fait d'être ou non européen. Cela ne vous surprendra pas, mais la souveraineté doit selon nous, en vertu des valeurs européennes, passer par la libre concurrence et la non-discrimination. À ce titre, la nationalité d'origine de l'éditeur ne nous semble pas un élément pertinent. On peut bien sûr en tenir compte, mais elle doit être associée à d'autres facteurs, comme la confiance en l'éditeur, sa structure capitalistique, sa manière de gérer les données, l'assurance que l'on peut avoir que les données ne sont pas transmises.

Le dernier principe qui nous semble important pour qu'un État ou une entreprise puissent assurer leur souveraineté numérique est le fait que les prestataires de services ou de solutions respectent les valeurs européennes et coopèrent avec les autorités. Ce point est particulièrement important dans le secteur de la cybersécurité en particulier, où l'on voit beaucoup de coopérations entre les entreprises et les forces de l'ordre, pour des investigations conjointes ou pour du partage d'expertise plus généralement avec la société civile et le monde académique.

Pour ce qui est des opérations conjointes, citons l'exemple de la saisie du serveur de *command and control* d'un groupe cybercriminel par des forces de police : ces dernières peuvent faire appel à une société comme Kaspersky pour aider à l'analyse du serveur afin d'essayer de remonter à la source et de trouver des clefs de déchiffrement de rançongiciels. Une initiative a très bien fonctionné sur le sujet, la plateforme No More Ransom, lancée en 2016 par la police néerlandaise, Europol, Kaspersky et McAfee. Cette plateforme réunit aujourd'hui plus de cent soixante parties prenantes, dont beaucoup de polices européennes. La police et la gendarmerie françaises en font partie. L'objectif est de donner des clefs de déchiffrement gratuitement aux personnes victimes de rançongiciels. Cette plateforme est bien sûr moins utile aujourd'hui, puisque les rançongiciels sont désormais beaucoup plus ciblés et complexes qu'auparavant. Il s'agit en tout cas d'un bon exemple de partenariat qui fonctionne.

En conclusion sur la souveraineté numérique, la non-dépendance vis-à-vis d'un fournisseur unique nous paraît un élément important pour un État ou une entreprise. En l'occurrence, la cybersécurité est un secteur relativement fragmenté, à la différence de celui de l'hébergement *cloud.* Il existe de nombreuses solutions, européennes ou non, permettant à

un État de choisir au mieux et de ne pas être pieds et poings liés avec un éditeur. La question n'est pas tout à fait la même.

M. Philippe Latombe, rapporteur. La question n'est effectivement pas tout à fait la même entre le *cloud* et la cybersécurité, mais percevez-vous chez vos clients une demande de plus en plus importante de solutions de type souveraines ? Cela fait-il partie des critères mis en avant, et recevez-vous des questions sur le sujet, ce qui vous obligerait à le déminer, sachant que vous n'êtes pas directement européen ? Une campagne a été menée disant que Kaspersky avait ouvert des *backdoors* pour les services russes. Cette situation vous pénalise-t-elle ? Quel est votre état d'esprit sur le sujet ?

M. Arnaud Dechoux. Je vous remercie de cette question très pertinente. Notre réponse est tout à fait positive. Nous percevons chez tous les clients, en particulier les grandes entreprises ou les intégrateurs qui revendent leurs services à d'autres entreprises, la montée de ces enjeux de souveraineté. Je ne saurais pas vous dire si le sujet est formalisé de manière juridique dans les appels d'offres, mais la question nous est systématiquement posée. Cette question est d'ailleurs peut-être moins posée à des acteurs d'origine anglo-saxonne.

En 2017, Kaspersky a été accusé, selon nous de façon complètement infondée, d'avoir installé des *backdoors* ou transmis des informations récoltées. Le manque de confiance généré n'aide pas la communauté à mieux se protéger. Nous pensons qu'il faut rétablir la confiance, ce qui passe par de la collaboration, pour mieux se protéger contre ces cyberattaques, qui peuvent venir de l'étranger, et en tout cas pas de la porte d'à côté.

Nous avons essayé de répondre au manque de confiance à travers une initiative lancée en 2017, qui répond également aux enjeux de souveraineté, même si le terme n'existait pas encore à l'époque.

Le premier socle est la relocalisation du cœur de l'infrastructure de stockage et de traitement des données de nos clients en Suisse. Les données étaient auparavant hébergées dans des *datacenters* localisés à Moscou : la Suisse a été choisie, car elle est un symbole d'indépendance, et parce que nous possédions déjà des *datacenters* à proximité de Zurich. Toutes les données des clients européens y ont été relocalisées dans un premier temps. Nous y avons ensuite, en 2018, 2019 et 2020, transféré celles des clients nord-américains et d'une partie importante des pays asiatiques. De nombreuses réticences ont été soulevées en interne par des personnes qui estimaient que la localisation des données n'était pas un facteur pertinent pour la cybersécurité, mais les mentalités ont ensuite changé. Nous avons vu tout l'intérêt de ce genre d'approche, que nous poursuivrons.

Le deuxième pilier est l'ouverture de centres de transparence. Des centres ont été adossés au *datacenter* de Zurich, nous en avons également ouvert à Madrid, au Brésil, en Malaisie et depuis peu au Canada. L'objectif est de permettre à nos clients et partenaires, qui sont souvent des agences de cybersécurité nationales, de venir auditer notre code source, et toutes les mises à jour des solutions. Vous évoquiez l'accusation de mise en place de *backdoors* : cela peut notamment se faire par des mises à jour. Pour un client, entreprise ou autre, la possibilité d'auditer l'ensemble de l'historique des mises à jour nous semble un facteur capital. Nous ne sommes pas la seule entreprise à avoir mis en place ce type de dispositif de transparence, mais le nôtre est particulièrement avancé. Je vous mentirais si je vous indiquais que des centaines d'entreprises viennent auditer notre code source : vingt à trente parties prenantes sont venues le faire depuis l'ouverture des centres de transparence. Il faut beaucoup de ressources pour auditer complètement les solutions informatiques, même si elles restent plus faciles à auditer qu'une infrastructure 5G, qui représente des millions de

lignes de code. En tout cas, cette possibilité existe, et il s'agit d'une preuve de confiance importante pour les entreprises ou les autorités publiques.

L'avant-dernier pilier est l'audit des processus internes par des tiers que sont les grands cabinets d'audit reconnus mondialement, lesquels passent en revue le développement et les bases des règles de détection des menaces, pour s'assurer qu'ils sont protégés de toute modification non autorisée, par de robustes mesures de sécurité. Un certain nombre de certifications existent dans le domaine de la cybersécurité, notamment la norme ISO 27001, que nous avons obtenue auprès d'un organisme autrichien.

Le tout dernier pilier, qui me semble également intéressant pour votre question relative à la souveraineté numérique, est la gestion des vulnérabilités. Nous en retrouvons dans à peu près toutes les solutions informatiques, en particulier celles qui ont été conçues il y a très longtemps. Les solutions de Kaspersky n'échappent pas à la règle. Nous avons mis en place un dispositif clair pour faire en sorte que les chercheurs puissent auditer nos solutions, sans être attaqués en justice – comme cela s'est fait dans d'autres entreprises. Nous avons également publié nos principes éthiques de gestion des vulnérabilités que nous trouvons dans les solutions d'autres entreprises. Un certain nombre d'étapes doivent être suivies : il faut bien sûr prévenir en premier lieu l'entreprise victime, faire en sorte qu'elle puisse corriger la vulnérabilité, avertir ses clients en temps et en heure, de façon privée dans un premier temps, puis publiquement par la suite. Il y a un certain nombre de bonnes pratiques à suivre. Il est à l'avantage des autorités publiques, au niveau français ou européen, de promouvoir ces bonnes pratiques en matière de gestion des vulnérabilités.

M. Philippe Latombe, rapporteur. Vous avez évoqué dans votre propos liminaire le fait que l'on parlait beaucoup de cybersécurité pour les ordinateurs, les *datacenters*, les applications dans le *cloud*, et moins pour les téléphones mobiles, smartphones et, à terme, les objets connectés. Est-ce normal, dans le sens où nous avons déjà suffisamment à penser pour les ordinateurs, et où la réflexion sur les mobiles viendra plus tard ? De grandes entreprises ou organisations pensent-elles d'ores et déjà à la cybersécurité de leurs systèmes de télécommunications ?

M. Arnaud Dechoux. Nous assistons à un basculement très rapide des utilisations vers le mobile. Les smartphones sont aujourd'hui utilisés pour toute notre vie numérique, que ce soit pour les activités professionnelles ou personnelles. De plus en plus d'attaques visent spécifiquement les mobiles, déployées par des cybercriminels classiques ou par des États – les cyberarmes ciblant ainsi de plus en plus les mobiles.

Les enjeux sont probablement différents pour les objets connectés, qui sont produits par des entreprises qui ne sont pas spécialisées dans le numérique – qu'il s'agisse de dispositifs médicaux connectés, des imprimantes, des systèmes de ventilation, qui constituent autant de portes d'entrée pour ces cybercriminels. Beaucoup d'intrusions informatiques ont eu lieu ces dernières années à cause de portes qui n'étaient pas fermées.

Il convient pour y faire face de développer des certifications pour tous ces appareils. L'agence de l'Union européenne pour la cybersécurité (ENISA) travaille activement à l'élaboration d'un certain nombre de certifications, notamment pour les objets connectés. Cela nous semble une piste importante : il est nécessaire d'harmoniser l'approche européenne sur le sujet. L'ANSSI effectue d'excellentes qualifications et certifications, mais il est particulièrement important, surtout pour des acteurs internationaux comme nous, de mettre en œuvre une certaine harmonisation

Le deuxième enjeu est la sensibilisation. Les utilisateurs pensent encore très peu à sécuriser leurs objets connectés. De nombreuses solutions existent pourtant, notamment des solutions gratuites : nous essayons d'insister sur ce point. De très nombreux antivirus pour mobile fonctionnent très bien, détectent les mêmes attaques que sur les ordinateurs, et ont souvent des versions gratuites. De même, les gestionnaires de mots de passe changent la vie, permettent de créer des mots de passe beaucoup plus sécurisés et font gagner beaucoup de temps. Le fait de sensibiliser les entreprises et le grand public permettra d'atteindre très rapidement les objectifs, et de renforcer l'hygiène numérique au niveau national.

M. Philippe Latombe, rapporteur. Comment Kaspersky travaille-t-il avec des *start-up* ? Examinez-vous comment elles fonctionnent, pour savoir dans quelle voie il serait intéressant de travailler ? Collaborez-vous avec elles ? Les achetez-vous ? Les incubez-vous pour nouer ensuite des partenariats ? Comment rester à la pointe ? Les GAFAM achètent pour intégrer directement. Comment procédez-vous ?

M. Arnaud Dechoux. Notre *business model* est tout à fait différent. Kaspersky développe historiquement beaucoup en interne : un tiers des salariés travaille en recherche et développement. L'entreprise n'a pas l'habitude de réaliser du développement externe et d'acquérir des entreprises. Nous regardons ce qui se fait ailleurs, investissons beaucoup dans certaines technologies comme l'Intelligence artificielle (même si nous n'aimons pas le terme) et le *machine learning*, qui permet d'améliorer la détection des fichiers malveillants, en utilisant différentes techniques, notamment l'analyse comportementale. Il ne s'agit pas seulement aujourd'hui de détecter un fichier entrant, mais d'examiner des comportements inhabituels, qui peuvent générer certaines alertes. Nous investissons dans ces technologies, mais rachetons peu de sociétés.

Nous pouvons nouer des partenariats : l'un des axes importants de développement de Kaspersky est constitué des systèmes industriels, qui sont très visés. En 2019, 45 % des ordinateurs industriels protégés par les technologies Kaspersky étaient visés par des cyberattaques, qu'il s'agisse de fichiers malveillants classiques ou spécifiquement calibrés pour l'industrie. Pour développer des sondes réseau, des systèmes d'exploitation sécurisés, nous nouons des partenariats.

Kaspersky n'a pas racheté récemment d'entreprises françaises ou européennes. Tout peut changer, mais ce n'est pas la manière dont nous fonctionnons aujourd'hui.

M. Philippe Latombe, rapporteur. Excluez-vous totalement de tels rachats, ou pourraient-ils se produire à la marge si une opportunité se présentait ?

M. Arnaud Dechoux. Cela ne s'est pas fait pour l'instant, mais je ne pense pas que ce soit exclu si nous trouvons le bon partenaire pour telle utilisation particulière, ou pour faire une acquisition. L'essentiel est de trouver le bon partenariat. Nous travaillons par exemple beaucoup avec Siemens dans le domaine de la cybersécurité industrielle, les Allemands étant en pointe sur le sujet, notamment dans le secteur énergétique automobile. Nous poursuivrons ce type de démarche, sans nous interdire de faire une acquisition. Je n'ai cependant pas de scoop à ce stade.

M. Philippe Latombe, rapporteur. Je ne vous en demandais pas.

Comment voyez-vous le marché de la cybersécurité dans les deux à trois ans à venir ? Se développera-t-il fortement ? Sur quels types de technologies se développera-t-il ? À quoi sera lié le développement : les attaques extérieures qui lui feront de la publicité, la prise de

conscience des directeurs des services informatiques (DSI) et responsables de la sécurité des systèmes informatiques (RSSI) ou la publicité des pouvoirs publics ?

M. Arnaud Dechoux. Les trois facteurs cités joueront. Nous nous attendons, sans surprise, à une progression stable du secteur de la cybersécurité, notamment pour les entreprises grandes et petites, en lien avec le développement des attaques elles-mêmes, de la part de groupes cybercriminels ou de groupes étatiques ou paraétatiques. Ces derniers mois, les rançongiciels ont fait l'actualité. Il n'y a aucune raison qu'ils disparaissent. Tout porte à croire que les cybercriminels continueront à mener ce genre d'attaques, d'autant que les entreprises paient fréquemment. Divers rapports parus ces derniers mois mentionnaient 30 %, 50 %, voire 70 % de paiements, ce qui alimente tout un écosystème criminel.

Des technologies de rupture sont parfois citées comme étant importantes dans le domaine de la cybersécurité. Nous pensons notamment à l'informatique quantique ; les ordinateurs quantiques parviendront-ils à casser les outils de chiffrement aujourd'hui utilisés pour protéger les données ? Beaucoup d'incertitudes demeurent sur le sujet. *A priori*, les algorithmes de chiffrement les plus avancés permettront de résister à des attaques quantiques, mais il faut continuer à investir et à utiliser dès maintenant les solutions de chiffrement les plus avancées pour prévoir cette nouvelle phase, qui peut intervenir d'ici cinq, dix ou quinze ans.

La deuxième technologie de rupture est le *machine learning*.

Pour ces différentes raisons, nous estimons que la cybersécurité continuera à progresser, peut-être davantage dans le secteur des entreprises et des organisations. Pour les particuliers, elle est de plus en plus intégrée aux outils mis à disposition par les constructeurs informatiques. Le paysage évolue beaucoup dans ce domaine, et continuera à se structurer en tout cas pour les entreprises.

M. Philippe Latombe, rapporteur. La cybersécurité des smartphones, mais aussi de l'ensemble des *devices* 5G (objets, antennes, etc.) fera-t-elle l'objet d'une attention croissante et d'un marché spécifique de la cybersécurité ?

M. Arnaud Dechoux. La réponse est ici encore clairement positive. Nos chercheurs du GReAT estiment que l'on découvrira de plus en plus de vulnérabilités dans la technologie 5G. C'est mathématique : quand une nouvelle technologie apparaît, tout le monde en cherche les vulnérabilités, et on en trouve forcément, que ce soient des chercheurs ou les cybercriminels, qui sont sans doute ceux qui investiront le plus de temps et de moyens. En matière de 5G, ces questions de cybersécurité arriveront nécessairement dans les prochains mois, avec des attaques, des opérations d'espionnage ou de sabotage. Une vraie attention est donc requise de la part des commanditaires comme des utilisateurs, dès lors que la 5G augmentera fortement la surface d'attaque. Je n'ai pas une vision claire des dispositions de cybersécurité existantes pour la 5G, mais tout laisse à penser qu'elles seront amenées à se développer dans les prochains mois. Le phénomène est le même que pour le *cloud,* qui s'est développé de manière exponentielle ces dernières années, et a bénéficié de nouvelles technologies de cybersécurité, notamment pour le chiffrement des infrastructures. Amazon Web Services et Microsoft Azure proposent déjà une brique de chiffrement : les entreprises peuvent y ajouter une brique, pour obtenir une protection supplémentaire. Je pense que ce sera la même chose pour la 5G.

M. Philippe Latombe, rapporteur. Puisque nous parlons de *cloud*, la sécurité dans ce domaine est-elle au niveau de celle qui existe pour un serveur physique propriétaire ?

M. Arnaud Dechoux. C'est une question complexe. Tout dépend de la manière dont est protégé et configuré le serveur physique.

M. Philippe Latombe, rapporteur. On nous dit que le *Cloud Act* a invalidé le *Privacy Shield*, et que les clauses contractuelles types et les mesures de protection doivent localiser les données en Europe et les chiffrer, au repos comme en mouvement. De votre point de vue d'expert, sommes-nous en capacité de garantir (Kaspersky étant réputé pour cela) que des données au repos ou en mouvement sur le *cloud* sont chiffrées de sorte qu'elles soient quasi inaccessibles ? Ces données ne peuvent pas être considérées comme inaccessibles, par nature : mathématiquement, il existe toujours une possibilité de les déchiffrer, mais est-ce tellement compliqué que cela en devienne une vraie protection ? Est-on capable de le garantir ? C'est une des questions qui font que l'on utilise encore pour des données sensibles des *clouds* américains, en se protégeant derrière cette sorte de bouclier. Ce bouclier est-il aujourd'hui suffisant selon Kaspersky ?

M. Arnaud Dechoux. Le niveau général de protection des infrastructures du *cloud* nous paraît très bon. Pour se protéger contre des accès tiers, il faut utiliser une brique de chiffrement et de gestion d'accès tierce. Beaucoup d'acteurs français proposent ce service – Atos ou autres –, en plus du service de l'hébergeur américain ou autre. Avec ces prestataires tiers, on arrive à un excellent niveau de protection.

Au-delà de l'aspect technique, la question se pose ensuite des assurances que l'hébergeur *cloud* peut apporter que personne d'autre ne pourra avoir accès aux données, et de la manière dont il peut gérer les vulnérabilités. Ces derniers mois, des vulnérabilités ont été trouvées sur les serveurs Microsoft Exchange : cette découverte a été largement exploitée par tous types d'acteurs, *a priori*, d'autant qu'elle n'a pas pu être corrigée suffisamment tôt. Des acteurs malveillants ont pu en tirer profit. La question est celle de la manière dont ces vulnérabilités sont gérées, depuis le moment auquel les clients sont informés, pour que l'éditeur puisse *patcher* la vulnérabilité et tous les utilisateurs mettre à jour leur logiciel en temps et en heure. Dans les petites entreprises et les petites collectivités territoriales, le problème est souvent que les mises à jour ne sont pas faites rapidement, même si l'information est rapidement disponible. Le CERT de l'ANSSI est extrêmement efficace et reconnu : il publie des alertes très régulièrement. Encore faut-il que les petits acteurs en aient connaissance et mettent à jour leurs solutions rapidement pour corriger les failles. Nous en revenons aux questions de sensibilisation et d'hygiène numérique. C'est probablement ici que le bât blesse : les mises à jour et la gestion des vulnérabilités.

M. Philippe Latombe, rapporteur. Parmi les menaces existantes, nous avons constaté l'existence d'une mode d'attaque sur les hôpitaux, pour ainsi dire. Ont-ils été attaqués en raison de la crise sanitaire, parce qu'ils possédaient des informations sensibles, ou parce qu'ils étaient faciles à attaquer ? Vous avez indiqué dans votre propos liminaire que la fréquence de circulation des virus était beaucoup plus importante aujourd'hui, d'un par jour à un par heure et un par seconde. S'agit-il d'abord d'attaques criminelles, ou d'attaques géopolitiques ? Quelles sont leurs proportions respectives ? Comment s'en prémunir en France et en Europe, en parvenant à distinguer ce qui est de nature criminelle de ce qui relève du géostratégique ?

Je prends l'exemple de l'attaque du Centre national de l'enseignement à distance (CNED) la semaine passée, attribuée aux Russes. Pourquoi effectuer une attaque en déni d'accès au service ? Quel est l'intérêt ? S'agit-il vraiment d'une attaque criminelle ? Aucune rançon n'a manifestement été demandée. À quoi servait l'attaque ?

M. Arnaud Dechoux. C'est une excellente question. Pour ce qui est des établissements de santé, les attaques s'expliquent, d'une part, parce qu'ils sont moins bien

protégés, et, d'autre part, parce qu'un rançongiciel perturbe fortement leur activité, et qu'ils sont bien plus susceptibles de payer. En Allemagne, l'année dernière, on a fait état du premier décès dû à un ransomware, un hôpital touché ayant dû transporter un patient dans un autre hôpital, lequel patient est mort pendant le transfert. Je ne connais pas les détails de cette affaire, qui montre cependant bien les impacts concrets qui peuvent inciter un établissement de santé à payer une rançon plus qu'une autre victime d'attaque. Au début du confinement, l'année dernière, un collectif de hackers s'est engagé publiquement à ne pas attaquer des établissements de santé. Cela a fait long feu : les attaques ont été multipliées par quatre ou cinq pour les établissements français, selon les chiffres de l'ANSSI.

Il s'agit ici à mon sens plutôt d'attaques criminelles à visée financière. Néanmoins, vous avez raison de souligner cette question : il existe une vraie porosité entre cybercriminels et acteurs étatiques.

Ils peuvent, d'une part, se revendre des outils ou des accès sur le marché noir. On a constaté une vraie progression de ce phénomène au cours des derniers mois, sinon pour la Chine ou la Russie, du moins avec des acteurs secondaires comme l'Iran, qui avaient moins de capacités cyber, mais ont fortement progressé au cours des dernières années.

D'autre part, une attaque à visée économique peut cacher autre chose. Un service de renseignement voulant réaliser des actions d'espionnage peut compromettre certains postes et y installer des sondes ou autres, puis revendre les accès sur le marché noir à un groupe cybercriminel y déployant par la suite un ransomware. Il est parfois très compliqué de dire qui est derrière une attaque. Plusieurs acteurs peuvent être impliqués. Il s'agit d'un vrai enjeu aujourd'hui, et nous avons besoin de travailler avec les différents pays et acteurs industriels et académiques pour y répondre mieux.

Pour ce qui est des attaques du CNED, je ne suis pas dans le secret des dieux. J'ai lu dans la presse que l'attaque viendrait de Russie ou de Chine. Néanmoins, je doute que des services de renseignements ou autres groupes étatiques aient commandité ce genre d'attaque. Un scénario que nous pouvons envisager est que des acteurs français ou étrangers aient fait appel à des *botnets*, ou réseaux d'ordinateurs zombies, envoyant beaucoup de requêtes sur le site du CNED ou d'un espace numérique de travail (ENT) pour le faire tomber. C'est déjà ce qui s'était largement produit en mars 2020, au début du premier confinement, lorsque de nombreux instituts éducatifs passaient au numérique. Nous avions déjà constaté une forte augmentation de ces attaques par déni de service, venant de réseaux d'ordinateurs situés à l'étranger. Nous voyons effectivement des adresses IP venant de l'étranger, mais je doute que ces attaques soient commanditées par un État – même si je n'ai pas d'information précise sur l'attaque du CNED de la semaine dernière. Cela illustre en tout cas encore une fois l'interaction constante entre tous ces acteurs, et le fait que ce soit une problématique mondiale.

M. Philippe Latombe, rapporteur. Avec l'incendie d'OVH à Strasbourg, nous avons constaté qu'un certain nombre d'entreprises ou d'administrations, qui lui avaient confié leurs données, avaient complètement oublié les règles de base des plans de continuité et de reprise d'activité (PCA et PRA). Lorsque Kaspersky contracte avec un client, a-t-il pour rôle de le conseiller sur ce type de sujet ? Votre objectif est d'éviter qu'un rançongiciel bloque l'entreprise cliente, mais vous ne pouvez pas tout protéger. La sensibilisation à ce sujet fait-elle partie de la prophylaxie que vous mettez en place lorsque vous contractez avec vos clients ?

M. Arnaud Dechoux. Sur le principe, cela est le cas, mais dans les faits, le rôle de Kaspersky est limité à la fourniture de solutions informatiques ainsi qu'à l'aide et au support à sa configuration et à son maintien. L'établissement de plans de résilience et de restauration

est plutôt du rôle du consultant, de l'intégrateur ou du revendeur de la solution. Nous ne sommes pas toujours aux côtés du client directement : ce sont souvent des intégrateurs ou des sociétés de conseil qui assurent ce rôle. L'incendie d'OVH a effectivement très bien montré cette nécessité, qui n'est pas encore une réalité en France.

M. Philippe Latombe, rapporteur. Qui serait le bon interlocuteur pour des TPE, PME et entreprises de taille intermédiaire (ETI) sur des questions de cybersécurité ? S'agit-il de Bpifrance, lorsqu'elle finance la montée en compétences numériques des entreprises ? S'agit-il de l'intégrateur, qui est leur interlocuteur au moment de la mise en œuvre ? S'agit-il de l'expert-comptable, qui est l'interlocuteur naturel de ce type d'entreprise ? Est-ce l'assureur, qui doit augmenter ou baisser ses primes en fonction du niveau de protection ? Tout le monde doit-il prendre sa part ? Est-ce suffisant dans ce cas ? Selon vous, comment faire pour diffuser cette culture de la cybersécurité *by design*, plutôt qu'après avoir pensé le système d'information ? Quel est l'interlocuteur le plus facile pour l'entreprise ?

M. Arnaud Dechoux. Cette question est compliquée. Il peut exister plusieurs canaux. La puissance publique a sans doute un rôle à jouer dans la commande, en instaurant des seuils de budgets dédiés à la cybersécurité. C'est ce que le gouvernement a fait pour la première fois dans le volet cyber du plan de relance, qui impose aux établissements de santé de consacrer 5 % à 10 % de leur budget IT à la cybersécurité. Cela me semble une première piste.

Pour le reste, il convient de passer par les acteurs que vous avez mentionnés. J'y ajoute Cybermalveillance, né en 2017 seulement, mais qui s'est beaucoup développé depuis cette date. Il s'agit d'un réel succès, qui manque toutefois encore de notoriété. Alors que l'ANSSI se charge très bien des grands opérateurs, collectivités territoriales ou autres, Cybermalveillance doit mener les mêmes tâches pour tous les autres acteurs. Je pense qu'il faut leur donner plus de moyens et de visibilité, en réalisant des campagnes grand public.

Un autre type d'acteurs pour les collectivités territoriales est celui des opérateurs publics de services numériques (OPSN). Ils sont une cinquantaine en France, regroupés au sein de l'association Déclic. Ils aident à la mutualisation et au soutien informatique, en particulier cyber, de toutes les petites collectivités territoriales, qui sont souvent celles qui se font attaquer aujourd'hui. Il faut miser sur ces acteurs. De manière générale, la mutualisation et la régionalisation sur lesquelles le gouvernement a souhaité insister dans son plan de relance cyber me semblent de très bons axes d'action. Les OPSN sont des interlocuteurs existants sur lesquels il est pertinent de se baser, pour les collectivités locales en particulier.

M. Philippe Latombe, rapporteur. Nous en prenons bonne note. Voyez-vous un sujet que nous n'aurions pas abordé et que vous voudriez mentionner ?

M. Arnaud Dechoux. Non, c'était très complet. Nous n'avons pas parlé beaucoup du niveau européen. Je voudrais simplement souligner que la dernière stratégie européenne de cybersécurité me semble très solide. Les autorités françaises et l'ANSSI ont elles-mêmes indiqué être satisfaites de ce nouveau plan, même s'il doit sans doute être renforcé sur certains points. Pour notre part, nous insistons sur le nécessaire renforcement des dispositifs de partage d'information et de collaboration entre public et privé, qui nous semble un moyen important de progresser. En tout cas, beaucoup de choses peuvent et doivent se faire au niveau européen. Nous continuerons à suivre ces sujets.

Audition, ouverte à la presse, de M. Laurent Degré, président-directeur général de la société Cisco Systems France et de M. Bruno Bernard, directeur des affaires publiques de la société Cisco Systems France *(13 avril 2021)*

Présidence de M. Jean-Luc Warsmann, président.

M. le Président Jean-Luc Warsmann. M. Laurent Degré est président-directeur général de la société Cisco Systems France, M. Bruno Bernard, son directeur des affaires publiques.

Cisco Systems est une entreprise informatique américaine fondée en 1984 et spécialisée dans les matériels informatiques et les solutions de cybersécurité. Vous avez un large champ d'action, qui devrait nous permettre de balayer un grand nombre de sujets, des enjeux cyber à l'identité numérique, en passant par la transformation numérique des entreprises.

M. Philippe Latombe, rapporteur. M. le président-directeur général, j'aimerais d'abord vous interroger sur votre acception de la notion de souveraineté numérique. Cette notion revêt une grande diversité de définitions. Que recouvre pour vous ce concept, que l'on rapproche parfois d'une forme d'autonomie stratégique et décisionnelle, et de quelle façon les politiques menées par les États peuvent-elles ou doivent-elles évoluer pour mieux intégrer cette composante stratégique ?

En second lieu, je voudrais que nous échangions sur l'écosystème des entreprises du numérique. Cisco mène des activités variées, dans des domaines comme le matériel informatique, mais aussi la cybersécurité. Comment vous positionnez-vous sur le marché européen ? Comment appréhendez-vous notamment le sujet de l'identité numérique, sur lequel nous travaillons au sein de cette mission d'information ?

De façon plus générale, je voudrais vous entendre sur les attentes de vos clients, dont certaines entreprises françaises font partie. À l'occasion de cette crise sanitaire durable, avez-vous observé des changements dans leur comportement numérique ? Peut-on dire que la crise sanitaire a accéléré leur sensibilisation face au risque cyber, par exemple ? À l'inverse, comment peut-on expliquer les difficultés que certaines entreprises continuent de rencontrer à l'heure actuelle pour se numériser ? Quelles seraient selon vous les solutions ?

Enfin, je voudrais évoquer la question de la formation aux compétences numériques. Quel regard portez-vous sur le niveau du système de formation français à cet égard ? Un Campus Cyber est par exemple en cours de déploiement, visant à rassembler un vivier d'acteurs de pointe. Comment jugez-vous ces différentes initiatives mises en œuvre en France ? Existe-t-il leur équivalent dans les pays au sein desquels vous êtes présents ?

M. Laurent Degré, président-directeur général de la société Cisco Systems France. Je voudrais en premier lieu revenir sur ce qu'est Cisco, ce que nous faisons et ce que nous ne faisons pas, ce qui peut être important pour la suite des questions que vous avez abordées. Cisco est comme vous l'avez précisé une société née en 1984. Notre métier est simple : il s'agit de connecter les applications, les équipements, les personnes, de transporter les flux d'information et de les sécuriser. L'entreprise compte 77 000 salariés dans le monde, dont 700 en France, un certain nombre d'entre eux étant des chercheurs. Ces derniers ont

notamment intégré la société anciennement appelée Sentryo, une pépite de la cybersécurité dans le monde industriel.

Notre métier n'est pas le commerce de la donnée : nous la transportons et la sécurisons. La cybersécurité est en revanche notre métier, du point de vue de l'outillage, des solutions logicielles et matérielles, ainsi que de la manière dont nous développons nos produits, dont nous interagissons avec nos prestataires et dont nous intégrons la sécurité de la conception à la fabrication.

Notre modèle de vente est exclusivement indirect. Tout ce que nous fournissons en termes de technologie est intégré, distribué, déployé et opéré par nos partenaires. Nous avons 1 200 partenaires français, dont certaines grandes entreprises comme Atos, Thales, Orange ou SFR, ainsi que tout un réseau de distributeurs à valeur ajoutée. Notre *business model* s'appuie donc sur les acteurs de confiance de l'écosystème français.

Nous contribuons à la formation aux métiers du digital dans l'écosystème, en formant 30 000 personnes par an – demandeurs d'emploi, formations certifiantes, cursus de formation intégrés (dans les IUT notamment) dans l'Éducation nationale.

La souveraineté numérique est un mouvement que nous observons en France, et auquel nous sommes très sensibles. Il se manifeste également au niveau global et dans de très nombreux pays. Nous y sommes très attentifs. Encore une fois, notre métier n'est pas de conserver ou de commercer des données, mais nous nous intéressons aux problématiques de souveraineté.

L'autonomie est un premier aspect, mais le contrôle des données est également très important. Parmi toutes ces plateformes de type *cloud*, nous proposons la solution Webex. La souveraineté renvoie à la notion de frontières, alors que le *cloud* et Internet de manière générale ont été conçus en s'affranchissant de ces règles. Nous devons néanmoins absolument disposer de la capacité de réglementer, de nous adapter à ces problématiques, pour conserver le contrôle des données au niveau d'un pays, mais aussi d'une entreprise.

Il convient de distinguer souveraineté numérique et protectionnisme. Nous pensons qu'il est important d'utiliser la technologie telle qu'elle est mise en place par les acteurs du marché, dont Cisco, tout en créant des garde-fous réglementaires et les processus nécessaires. Une fermeture ou un cloisonnement ne peut pas répondre à l'ensemble des questions. Bénéficions de la technologie, travaillons avec des acteurs tels que l'ANSSI en France, qui est très en avance en termes de recommandations et de réglementation. C'est un travail qui doit se faire avec les industriels. Mettons les bons outils en place pour faire en sorte que tout cela se passe sous un contrôle, ou du moins une protection des États.

Reste une dimension importante, celle de l'industrialisation. Selon les pays, les demandes que recouvre la notion de souveraineté numérique sont bien souvent différentes. On parle de localisation des données dans un cas, de centre de données localisées dans un autre, de cybersécurité ailleurs, ou encore de possibilités de contrôler et de débrancher des applications. L'aspect industriel est extrêmement important pour des acteurs comme Cisco ou d'autres. Élaborer une solution pour chaque pays est très compliqué si l'on veut concilier l'innovation, l'aspect industriel, la capacité à proposer des applications et des services bénéficiant de cette innovation, tout en répondant aux réglementations.

M. Bruno Bernard, directeur des affaires publiques de la société Cisco Systems France. En matière de souveraineté, la question du droit applicable aux données est également essentielle. Si nous voyons des demandes de localisation émaner de beaucoup de pays, nous

pensons que la vraie question de la souveraineté se joue sur le droit applicable. Tout l'enjeu est de trouver un modèle permettant aux États de garantir une sécurité des données de leurs citoyens et de leurs entreprises, tout en permettant à ces derniers de continuer à bénéficier des meilleures solutions technologiques disponibles. L'entente est donc nécessaire entre les États. Nous y incitons, que ce soit aux États-Unis ou ailleurs dans le monde, pour que des formes juridiques soient trouvées pour garantir ces transferts de données.

M. Philippe Latombe, rapporteur. Vous parlez de la manière de trouver une réglementation applicable. Comment faire dans le contexte actuel où il existe une extraterritorialité forte des règles américaines ? Comment assurer aux Européens que les données hébergées dans le *cloud* ou utilisées dans des algorithmes sont bien localisées et opérées sur le territoire européen, sans possibilité de prise de la part de la réglementation américaine ? Les clauses contractuelles-types telles que la localisation des données dans des serveurs européens et le chiffrement sont-elles suffisantes ? Que ferait par exemple Cisco si une agence américaine lui demandait de fournir des informations ?

M. Laurent Degré. Vous faites référence au *Cloud Act*.

M Philippe Latombe, rapporteur. Ce n'est pas la seule loi dans ce domaine, même si elle est celle qui a fait le plus de bruit avec *Schrems* II. Il existe des règles extraterritoriales américaines assez fortes en dehors du *Cloud Act*.

M. Laurent Degré. Nous sommes une société américaine, sujette à ces lois.

M. Philippe Latombe, rapporteur. C'est bien pour cette raison que je vous pose cette question.

M. Laurent Degré. Même si nous sommes une filiale française du Groupe, nous sommes soumis à ces contraintes. Un processus existe en la matière, que j'invite M. Bruno Bernard à rappeler.

M. Bruno Bernard. L'extraterritorialité est malheureusement un concept à la mode en ce moment. Beaucoup de règlements sont extraterritoriaux en matière numérique : le RGPD est, par exemple, extraterritorial de fait. C'est toute la problématique de l'application du droit dans des sphères qui ne sont pas traditionnelles. Les sollicitations que nous sommes susceptibles de recevoir d'agences gouvernementales ne se limitent pas aux États-Unis.

Pour ce qui concerne le *Cloud Act* précisément, nous rappelons que son application suppose la demande d'un juge, sollicité par une agence gouvernementale.

Notre processus est standard, mais relativement fort. La question se pose de savoir où se trouve la donnée. La plupart du temps, elle est chez le client. Nous demandons donc que l'agence ou le juge s'adresse directement à notre client. Si la demande est adressée directement à Cisco, nous en notifions le client, pour éviter toute rupture de confiance. Il est possible qu'une décision judiciaire nous l'interdise, auquel cas nous la contestons devant la juridiction compétente.

Ensuite, nous communiquons des données aux autorités qui ont réellement compétence. Dans le cas du *Cloud Act*, par exemple, nous ne communiquons pas de données en l'absence de la décision d'un juge. Nous cherchons également toujours à réduire la portée de la requête au strict minimum correspondant à la demande.

Dans la configuration où la demande légale d'un gouvernement nous mettrait dans une situation de conflit de lois entre deux législations ayant autorité sur les données (par exemple, entre un pays européen et les États-Unis), nous irions devant un juge pour réfuter cette demande, en invoquant les traités d'assistance judiciaire mutuelle existants.

Je tiens également à signaler que nous publions un rapport de transparence (*transparency report*), dans lequel nous listons les demandes de transmissions de données par pays. Elles sont très peu nombreuses, notamment depuis l'entrée en vigueur du *Cloud Act*.

M. Philippe Latombe, rapporteur. Comment percevez-vous le marché européen du numérique ? S'agit-il d'un marché mature, ou encore adolescent ? Je voudrais que l'on sépare pour traiter cette question la partie relative au numérique de manière générale et celle de la cybersécurité en particulier, car il existe peut-être deux types de maturité différents.

M. Laurent Degré. Il existe plusieurs aspects dans cette question : la maturité digitale de manière globale, celle des éditeurs et la question de notre force de frappe en Europe.

Nous avons la chance en France de disposer de beaucoup de champions dans le domaine numérique – Atos, Thales –, de champions en matière de cybersécurité, qui nous sont enviés, d'une agence de régulation, d'excellents cursus de formation. Je n'ai donc pas le sentiment que nous ayons des lacunes en matière de cybersécurité. Nous sommes peut-être derrière les États-Unis concernant les éditeurs capables de fournir du software et des solutions dans leur globalité pour servir l'Europe. Du point de vue de l'intégration, des compétences et de l'écosystème, nous avons en revanche quelque chose de très fort en France.

Cybermalveillance est par exemple une excellente initiative, dont nous faisons d'ailleurs partie. De même, nous officialiserons notre contribution au Cyber Campus. Il s'agit de la meilleure des réponses. Nous ne sommes pas du tout en retard, et disposons du bon écosystème et des bons acteurs pour pouvoir avancer sur la cybersécurité.

Il existe de nombreux classements relatifs à la maturité digitale des entreprises de manière générale, que nous serions heureux de partager avec vous. Pour faire simple, nous pouvons formuler deux constats pour la France :

– nos grands groupes sont bien équipés : nous avons vu, dans la crise du Covid, qu'ils étaient capables de réagir ;

– en revanche, il existe certainement un déficit, par rapport à d'autres pays, parmi les PME et ETI, en termes d'acculturation, de formation et de perception du numérique en général et de ce qu'il représente en matière de valorisation de l'entreprise, de relation client, d'amélioration des modes de fonctionnement et de performance industrielle ou économique. En matière de cybersécurité en particulier, nous avons un travail d'éducation à mener. Je considère que la cybersécurité doit être un investissement, plutôt qu'un coût de fonctionnement. Protéger vos données et vos salariés revient à valoriser votre entreprise. Une accélération de l'acculturation, de la prise de conscience et de la gouvernance est nécessaire sur le sujet.

M. Philippe Latombe, rapporteur. Est-ce lié au mouvement d'externalisation de l'informatique dans les entreprises ?

M. Laurent Degré. Les sujets sont selon moi décorrélés. Le numérique est de toute façon omniprésent, comme nous l'avons vu dans la crise sanitaire. Le Covid est ni plus ni moins qu'un accélérateur de la transformation. Le digital est partout, dans l'Internet des objets,

la relation client, le management, l'interaction avec les fournisseurs. Qu'il soit dans le nuage ou non, beaucoup d'activités se numérisent de toute façon, ce qui conduit à une augmentation de la surface d'attaque. La prise de conscience est donc nécessaire, indépendamment de la question de l'externalisation.

M. Philippe Latombe, rapporteur. Les plans européen et français de relance sont-ils une bonne manière d'aborder le sujet ? Le financement n'est-il à l'inverse que la partie émergée de l'iceberg, et y a-t-il d'autres champs (comme l'éducation) à investir d'abord ?

M. Laurent Degré. Ces programmes d'investissement sont bons. Le plan de relance européen et les investissements prévus en France constituent une démarche excellente. Son orchestration est une question d'écosystème.

L'Éducation nationale doit faire partie intégrante du processus. La cybersécurité est un marché en constante évolution. On parle d'un poids de la cybercriminalité de plus de 4 000 milliards d'euros dans le monde, ce qui donne une idée de sa puissance, si l'on rapporte ce chiffre au PIB. Il s'agit d'un processus continu, qui évolue. L'éducation, quelles que soient les filières, doit être au cœur des investissements. À côté des aspects technologiques et de formation pour les industriels, l'éducation doit être un pilier de la démarche. Nos étudiants, nos élèves, ne sont pas toujours conscients de ce qu'ils font, ce qui peut se traduire par la suite dans l'entreprise. L'éducation est donc selon moi un point critique. Nous essayons autant que possible de contribuer, au travers de beaucoup d'initiatives, à ces aspects d'acculturation et de formation, mais ce n'est pas suffisant : il faut faire encore beaucoup plus.

M. Bruno Bernard. La clef est de faire pénétrer les réflexes numériques dans la vie de tous les jours. Lorsque vous prenez un crédit bancaire, que vous vous assurez, que vous vous engagez dans votre vie de tous les jours, on pourrait imaginer un volet numérique, et un volet relatif à la cybersécurité, puisque ces questions peuvent avoir des impacts tout à fait concrets pour les entreprises, mais aussi pour les particuliers.

Les plans de relance et d'investissement sont la bonne manière de faire, mais le moment est venu de pleinement infuser ces problématiques dans le quotidien des entreprises et des citoyens.

M. Philippe Latombe, rapporteur. Comment inscrire le numérique et la cybersécurité dans les formations ? Faut-il créer des filières spécifiques ? Doit-il s'agir uniquement de filières d'excellence, d'ingénieurs ? Certaines personnes auditionnées nous ont expliqué que nous manquions également de techniciens, de personnes capables de coder, de « mettre les mains dans le cambouis », et qu'il existait un besoin de formations de niveau BTS ou IUT sur ce type de sujets. Comment faire pour trouver des personnes ?

M. Laurent Degré. La formation de spécialistes existe d'ores et déjà. Nous n'avons pas de problème de formation d'experts, mais l'acculturation et l'infusion de principes fondamentaux des bonnes pratiques du digital dans l'ensemble des filières sont essentielles. Il me semble que cette approche doit être aussi évaluée.

M. Bruno Bernard. Cisco faisait, à l'époque où les interventions physiques étaient possibles, de l'acculturation pour des collégiennes dans le département des Hauts-de-Seine, en leur montrant comment fonctionnait un réseau et quel était le parcours de la donnée. Nous pensons que c'est à cette période de la vie, qu'il faudrait former les personnes à se servir d'un smartphone, à publier sur les réseaux sociaux, à savoir quels types de données partager. À notre avis, c'est à ce moment que l'on peut former des personnes qui soient totalement *digital natives*. Ils savent pour le moment se servir des applications, mais ignorent comment

elles fonctionnent et quels sont les tenants et aboutissants de cette économie numérique. Nous recommandons donc des interventions au niveau du collège, qui ne soient pas du tout spécialisées, mais au contraire touchent l'ensemble de la population de cet âge.

M. Philippe Latombe, rapporteur. Selon vous, la crise sanitaire et le recours au numérique, tel que nous l'avons vécu de manière forcée, et tel qu'il s'est prolongé depuis un an, changent-ils la manière de fonctionner des entreprises en interne, par exemple pour les réunions, les pratiques de management ? La situation les a-t-elle renvoyés à un mode projet ? Cette question est valable pour les entreprises, mais également pour les administrations, si vous en avez une vision.

M. Laurent Degré. Indéniablement, cette crise sanitaire, qui a forcé beaucoup d'entreprises à accélérer leur digitalisation, a changé les comportements. Prenons l'exemple de ce que nous appelons le travail hybride : la relation au travail et au lieu physique a changé. Le digital, la connectivité, le *cloud* ont été un moyen de résilience économique pour les entreprises.

Nous avons vu plusieurs étapes. La première était celle de l'équipement, parfois sans garde-fous, sans acculturation, avec parfois des erreurs. Nous l'avons vu avec l'utilisation de certaines applications de collaboration, qui ont été bannies par certains États. Nous revenons aux thèmes de la formation, de l'acculturation, des bonnes pratiques, du choix des bons partenaires. Je pense que nous sommes maintenant dans une phase où le digital est plus important qu'auparavant, parce qu'il change la relation au travail, les modes de fonctionnement, mais qu'il y a encore beaucoup à faire sur les bonnes pratiques.

M. Bruno Bernard. Pour ce qui est des administrations, nous constatons un changement d'attitude, mais il demeure certains blocages, notamment vis-à-vis de l'utilisation d'outils de vidéoconférence. Nous avons essayé de porter ce message auprès du ministère de l'éducation nationale, pour venir en aide aux professeurs et aux élèves consignés chez eux. La volonté existe, mais cela reste compliqué, car non encore tout à fait naturel.

M. Philippe Latombe, rapporteur. Au-delà de la numérisation, les modes de fonctionnement des entreprises ont-ils durablement changé, en termes de gestion en mode projet, de rapidité, de capacité d'évolution, d'agilité ? Les entreprises et les administrations ont-elles compris que le temps n'était plus aussi long qu'auparavant, qu'il fallait se préparer à quasiment tout, que l'incertitude était chaque fois présente ?

M. Laurent Degré. Votre question n'est pas évidente, M. le rapporteur.

M. Philippe Latomb, rapporteur. Lorsqu'ils recourent à vos services, demandent-ils que leur système puisse évoluer presque instantanément, en fonction de ce qui arrive ? Veulent-ils se laisser en permanence des portes ouvertes dans les services qu'ils vous demandent ?

M. Laurent Degré. Le numérique, l'accès à ces applications, à ces outils, est critique pour la pérennité du fonctionnement des entreprises, leur vélocité. Il s'agit d'un sujet très important pour nous, sur lequel nous possédons beaucoup d'études que nous pourrons vous partager.

En matière de relation au travail, il y a la notion de temps long et de temps court, celle de résilience, apportée par le digital. Dans les entreprises comme les administrations, l'utilisation du digital et de ses outils change la relation au travail et au management. Lorsque vous travaillez à distance, comme nous sommes en train de le faire, les notions d'horaire, de

lieu physique et de relation avec votre manager changent. On est obligé de faire travailler les personnes sur un mode de confiance, d'objectifs. Je pense que cela est en train de révolutionner les modes de fonctionnement dans certaines entreprises. La technologie est une chose, mais les modes de gouvernance et la manière dont elle est utilisée pour le bien de l'entreprise ou de l'administration en est une autre. La relation hiérarchique n'est plus la même qu'auparavant en raison de l'utilisation de ces outils. J'ignore si je réponds à l'ensemble de vos questions, mais c'est un point qui me vient à l'esprit et qui est extrêmement important.

M. Philippe Latombe, rapporteur. Vous êtes acteur de l'identité numérique. Comment voyez-vous ce sujet émerger ?

M. Bruno Bernard. Nous avions participé à la mission d'information de l'Assemblée nationale sur le sujet de l'identité numérique.

M. Philippe Latombe, rapporteur. Elle était menée par M. Jean-Michel Mis, qui participe également à la présente mission.

M. Bruno Bernard. Nous avions positionné ce que nous percevions comme le futur de l'identification numérique d'une personne. Cela correspond tout à fait à notre démarche de cybersécurité. Nous préconisons une augmentation du nombre de critères de vérification de l'identité de la personne, de son comportement en ligne et de son positionnement géographique, grâce à des outils liés aux smartphones notamment. Nous sommes très favorables à une sécurité fondée sur le principe *zero trust* : il ne suffit pas de s'identifier une fois, et la posture doit être cohérente pour que l'identité des personnes sur Internet soit garantie.

Nous considérons qu'il revient aujourd'hui aux États et aux organisations internationales de prendre la main sur la définition de l'identité numérique – comme l'a fait l'Union européenne, et comme, me semble-t-il, le gouvernement français s'est engagé à le faire prochainement.

M. Philippe Latombe, rapporteur. Comment percevez-vous le retard pris sur le sujet ? Le rapport date d'il y a quelque temps. Or, nous n'avons fondamentalement pas avancé, même si la carte nationale d'identité électronique, réceptacle de l'identité numérique, arrivera prochainement. Nous n'avons pas grand-chose sur l'identité numérique pour l'instant, à part France Connect, qui n'a pas évolué. Comment percevez-vous ce retard ?

M. Bruno Bernard. J'ai cru comprendre que France Connect faisait partie des sujets qui seraient accélérés dans les quatre cents derniers jours, ainsi que Mme la ministre, Amélie de Montchalin, l'a récemment indiqué.

Malheureusement, la France aime prendre son temps. Nous sommes donc fréquemment un petit peu en retard, car nous souhaitons voir comment les choses se passent, pour bien les mesurer. Notre retard n'est pas irrattrapable, mais comme souvent, en matière de numérique en particulier, il serait bon de ne pas laisser ce retard se creuser.

M. Philippe Latombe, rapporteur. Vous êtes une entreprise qui travaille dans de nombreux pays, vous avez une activité mondiale. Cette question de l'identité numérique est-elle abordée de la même façon partout en Europe ? Une comparaison avec l'Estonie n'est peut-être pas pertinente, car les niveaux de maturité sur l'identité numérique, les tailles de populations, les administrations, les histoires ne sont pas les mêmes. Mais parmi les pays qui nous ressemblent le plus, le retard pris par la France générera-t-il un retard supplémentaire ? Si nous sommes en train de rattraper le retard pris depuis quelques années, mais qu'eux ont

avancé sur l'identité numérique, avons-nous besoin de faire un saut qualitatif dans ce que nous devons atteindre dans les quatre cents prochains jours ?

M. Bruno Bernard. Les quatre cents jours sont peut-être un peu ambitieux.

M. Philippe Latombe, rapporteur. Ce n'est pas mon calendrier.

M. Bruno Bernard. Il faut essayer de combler le retard d'il y a trois ans et atteindre un système à parité avec celui de nos voisins allemands et britanniques, toujours dans l'idée d'élaborer une identité numérique à l'échelle européenne, qui est le grand enjeu en la matière. Les processus de décision à cette échelle peuvent réserver des surprises et ne pas être optimaux, mais nous pouvons espérer que la présidence française de l'Union européenne qui s'annonce soit un accélérateur en Europe et en France sur nombre de ces sujets, dont l'identité numérique.

M. Philippe Latombe, rapporteur. Quand on parle d'identité numérique, on parle d'usages. Vous avez souligné tout à l'heure l'importance de l'éducation des collégiens, pour qu'ils ne soient pas uniquement des consommateurs, mais sachent comment le numérique fonctionne. Comment voyez-vous les usages du numérique dans les années à venir ? Quels sont les domaines dans lesquels la France et l'Europe doivent investir maintenant pour être à la pointe de ce qui se passera dans quelques années ?

En matière de *cloud*, par exemple, on nous a expliqué que nous ne serions jamais au niveau des géants actuels. Nous mettrons beaucoup de temps à les rejoindre, et cela nécessitera beaucoup d'efforts. On nous a dit à l'inverse que nous étions très en avance sur de nombreux sujets, dont l'Intelligence artificielle des objets, par exemple. Identifiez-vous des domaines sur lesquels les Européens devraient davantage capitaliser pour rester à la pointe ?

M. Laurent Degré. Dans le domaine de l'Intelligence artificielle et du quantique, nous avons des choses à faire et à dire. Le quantique révolutionnera les capacités de calcul et ouvrira des cas d'usage et des possibilités jamais connus. Il ne faut pas rater ce virage. Dans le domaine de l'Intelligence artificielle, nous avons de très bons acteurs.

En matière de cybersécurité, nous avons des champions français en Europe. Faisons encore plus d'investissements, aidons-les dans cet écosystème, dont nous faisons partie. Capitalisons sur ces atouts : nous ne sommes pas en retard dans le domaine de la cybersécurité, bien évidemment.

Il faut également travailler sur plusieurs technologies – la 6G, le *edge computing*, visant à ramener la capacité de calcul au plus près de l'utilisateur, l'Internet des objets.

M. Bruno Bernard. J'ajoute, si vous le permettez, la technologie *open RAM*, qui est la virtualisation des accès radio. Ce n'est pas une technologie tout à fait mature, mais Cisco est par exemple partenaire de Rakuten au Japon pour déployer un réseau téléphonique virtualisé. Il s'agit de l'une des grandes révolutions à venir dans le domaine des télécommunications. Les opérateurs européens, dont Orange, se sont engagés sur le sujet. Les opérateurs américains le sont déjà, et nous pensons que cela peut faire partie du futur des télécommunications en France. Cela impliquera une réflexion sur le *cloud* et la nécessité de réaliser des investissements lourds. Si votre réseau téléphonique fonctionne demain de façon complètement virtualisée, il faudra le localiser quelque part, ce qui pose la question du contrôle de la donnée, des infrastructures.

À mon sens, ce qui permettrait de grandir à l'échelle européenne et d'avoir enfin des acteurs mondiaux serait de disposer d'un véritable marché unifié, où l'on puisse à la fois lever des capitaux, mais aussi se développer en partenariat les uns avec les autres, en s'appuyant sur des acteurs de confiance, dont Cisco ou d'autres, pour grandir tous ensemble. L'environnement est aujourd'hui encore, un peu, voire très, morcelé, ce qui freine l'émergence de ces champions européens.

M. Philippe Latombe, rapporteur. Nous voyons que l'innovation des GAFAM est permise par des succès commerciaux forts qui leur permettent de dégager des moyens en R&D, qui est réalisée soit en interne, soit par des acquisitions. Comment fonctionne Cisco avec l'environnement des *start-up* ? Collaborez-vous avec elles ? En incubez-vous certaines, pour les absorber ensuite ? Les laissez-vous vivre, en les plaçant sous votre aile pour en faire des avantages commerciaux dans vos offres ? Comment fonctionnez-vous avec cet écosystème ?

M. Laurent Degré. Il n'existe pas de modèle unique, mais plusieurs options. En matière de R&D, Cisco ne se limite pas aux États-Unis, car l'intelligence n'est pas disponible en un seul endroit : elle est distribuée partout. Par ailleurs, l'expertise est difficile à trouver, car il s'agit d'un marché en constante innovation. Nous comptons plus d'une centaine d'ingénieurs en R&D en France. Cisco compte au total 26 000 ingénieurs dans le monde.

Notre équipe française de R&D travaille constamment dans des modes sinon d'incubation, du moins de codéveloppement avec des *start-up*, qui viennent nous présenter des idées et ont besoin de support, ou vers lesquelles nous nous tournons. Nos équipes ont pour mission de mener des activités de R&D au sens strict, mais également de réaliser une veille technologique du marché, d'accompagner l'écosystème. Parfois, au lieu de développer en interne, nous procédons à une acquisition – mais ce n'est pas systématique. Cybervision est par exemple issu de la *start-up* villeurbannaise Sentryo, avec laquelle nous travaillions en codéveloppement. Nous les avons accompagnés dans leur croissance. Il y avait à un moment donné un besoin de capital. Cisco a fait le choix d'en faire l'acquisition. Cybervision est devenu un acteur mondial de la cybersécurité dans le monde industriel, présent partout en Europe et dans le monde.

Nous ne poursuivons pas une stratégie unique : les décisions sont prises *ad hoc* en fonction de la course à l'innovation et des meilleures opportunités. Certaines choses peuvent être faites en interne, d'autres sont cherchées ailleurs. Il n'y a pas de schéma tout tracé.

M. Philippe Latombe, rapporteur. Nous avons ce matin auditionné le responsable de la cybersécurité d'Orange, qui nous expliquait que certaines entreprises françaises étaient achetées vingt-cinq fois la valeur de leur EBITDA, et qu'il était impossible de rivaliser avec les entreprises américaines sur ce plan. Partagez-vous le sentiment d'une survalorisation ? Pourquoi ces entreprises sont-elles valorisées à ce point ?

M. Laurent Degré. Si ces sociétés sont achetées à ces prix, cela signifie qu'il existe de la compétence et de l'expertise en France. II s'agit donc d'une bonne nouvelle. Par ailleurs, ce n'est pas de la survalorisation, mais une valorisation de la compétence qui a un prix sur ce marché. La question se pose ensuite de savoir si nous avons la capacité de le faire, au niveau français ou européen, mais c'est une autre discussion. Il n'y a pas de survalorisation de ces sociétés, mais une simple valorisation de leur compétence.

M. Philippe Latombe, rapporteur. Voyez-vous un sujet que nous n'aurions pas abordé et que vous voudriez évoquer ?

M. Laurent Degré. Non. J'espère que nous vous avons apporté quelques éléments de réflexion. Nous restons à votre entière disposition. Il y a bien d'autres choses à couvrir, mais je n'ai rien à ajouter pour ma part.

M. Bruno Bernard. Nous nous tenons à votre disposition pour tout suivi ou complément d'information dont vous auriez besoin. De manière générale, Cisco a toujours la capacité de fournir une certaine expertise sur ces sujets. Nous sommes ravis de la partager.

Audition commune, ouverte à la presse, de Mme Bénédicte Roullier, cheffe du pôle « Transformation numérique des TPE/PME », et de M. Aurélien Palix, sous-directeur des réseaux et des usages numériques à la direction générale des entreprises (ministère de l'économie, des finances et de la relance)

(15 avril 2021)

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. L'audition de Mme Bénédicte Roullier, cheffe du pôle « Transformation numérique des TPE/PME » à la direction générale des entreprises (DGE) du ministère de l'économie, des finances et de la relance et de M. Aurélien Palix, sous-directeur des réseaux et des usages numériques au sein de cette même direction, doit nous permettre de faire un point d'ensemble sur la digitalisation des TPE et PME dans notre pays, sur ses progrès et aussi sur les difficultés des entreprises. Nous souhaitons également évoquer l'initiative France Num, renforcée dans le plan de relance. Nous nous intéressons à l'ensemble de ces sujets sous l'angle de la souveraineté, en interrogeant la capacité des entreprises, y compris les plus petites, à trouver une offre française ou européenne satisfaisante pour leurs besoins et dimensionnée en fonction de leurs besoins.

M. Philippe Latombe, rapporteur. Je souhaite vous interroger sur trois sujets. Le premier concerne votre approche de la notion de souveraineté numérique. Il s'agit d'une question rituelle lors de nos auditions qui provient de la grande diversité des définitions de cette notion. Comment définissez-vous cette notion et, surtout, comment est-elle prise en compte dans vos actions au service de la numérisation des entreprises ? Les échanges que nous avons conduits ont fait apparaître la force de frappe des grands acteurs du numérique, notamment étrangers, souvent mis en avant par des intégrateurs qui offrent des solutions clés en main aux petites entreprises. Nous aimerions avoir votre opinion et savoir quels sont les comportements d'achat des TPE et PME dans ce domaine.

Ma deuxième question porte sur votre action au sein de la DGE. Je voudrais que vous nous présentiez à grands traits France Num, les réflexions menées durant la crise sanitaire sur la numérisation des entreprises et, surtout, votre analyse de ses impacts sur le souhait des TPE et PME de passer au numérique. J'aimerais aussi savoir si les entreprises rencontrent pour se numériser des difficultés plus ou moins connues qu'il conviendrait de traiter prioritairement.

Mon dernier point concerne le risque cyber. Nous avons constaté durant l'année 2020 un essor des cyberattaques par rançongiciel contre les acteurs privés et publics. Les TPE et PME ont souvent des moyens réduits pour se protéger. Comment pouvons-nous les inciter à consentir cet investissement rentable à moyen terme et diffuser une culture de la cybersécurité au sein de ces petites structures ?

M. Aurélien Palix, sous-directeur des réseaux et usages numériques. Vous avez déjà auditionné notre directeur général, M. Thomas Courbe. Au sein de la direction générale des entreprises, nous partageons la vision d'une souveraineté numérique qui consiste, d'une part, à pouvoir définir des règles encadrant les usages du numérique et, d'autre part, à être autonome dans les technologies à la base de ces usages. L'action spécifique de ma sous-direction porte plutôt sur la seconde partie. Il s'agit de proposer des technologies souveraines, françaises, pour certains blocs qui nous paraissent stratégiques.

Nous travaillons à identifier ces blocs stratégiques avec l'ensemble de nos partenaires, en interministériel mais aussi avec des partenaires publics et privés, et nous nous assurons que la France dispose d'une autonomie pour des technologies clés telles que l'intelligence artificielle, le *cloud*, la *blockchain*, la cybersécurité. Dans le plan de relance, nous travaillons à la stratégie nationale de cybersécurité, afin que les entreprises françaises puissent avoir un large choix de solutions numériques et que ce choix inclue des solutions souveraines, qu'elles soient françaises ou européennes.

Lorsque je parle d'entreprises, je pense aux grands groupes, aux entreprises de taille intermédiaire (ETI) et aux PME qui ont déjà les épaules suffisamment larges pour s'engager dans le numérique. La mission de M. Nicolas Guérin et Mme Juliette de Maupeou à laquelle mes services contribuent et que vous aurez à auditionner porte sur ces questions.

Je pense aussi aux TPE pour lesquelles la problématique est complètement différente. Certaines sont très éloignées du numérique. Elles n'ont pas toujours conscience de l'intérêt qu'a pour elles le numérique ou le vivent comme une sorte d'injonction au numérique. Notre but n'est donc pas uniquement de leur proposer des solutions françaises mais aussi de les convaincre de l'intérêt de se numériser et de les accompagner au mieux lorsqu'elles entreprennent cette démarche de digitalisation.

Réussir à « embarquer » ces TPE est tout le but de France Num. Toutefois, nous avons vocation à accompagner les entreprises dans leurs démarches mais non à prescrire des solutions. Nous ne forçons pas les entreprises à se détourner d'offres de solution étrangères. Nous avons tous conscience que, actuellement, être référencé sur certaines plateformes ou moteurs de recherche internationaux est absolument indispensable. Notre but est plutôt d'« embarquer » les TPE dans le numérique, de les orienter vers les acteurs et les dispositifs les plus pertinents. France Relance a lancé plusieurs dispositifs, mais les entreprises restent libres de leurs choix entrepreneuriaux, de recourir à des solutions françaises ou étrangères. Nous voulons seulement qu'elles le fassent en connaissance de cause, qu'elles sachent que la gestion de leurs données sera différente selon la solution choisie.

Mme Bénédicte Roullier, cheffe du pôle « Transformation numérique des TPE/PME ». Je commencerai par quelques données sur la numérisation des entreprises françaises et notre positionnement comparé à nos voisins. Il existe de nombreuses études et il est important de savoir, d'un point de vue méthodologique, que le public concerné est complexe et hétérogène. Nous regardons toujours si les études résultent d'un recueil de données uniquement en ligne ou en ligne et hors ligne : il est impossible de connaître un public peu connecté en ne recueillant les données que par questionnaire en ligne.

Nous avons déterminé les actions de France Num à partir de notre connaissance de ce public, basée notamment sur une étude que nous avons réalisée au début de l'année 2020, juste avant la crise. Nous refaisons actuellement une étude pour voir quelle est l'évolution au moyen d'un baromètre dont nous connaîtrons les résultats en juin.

Ce baromètre nous donne des chiffres relatifs à la perception et des indicateurs sur les freins. Ainsi, sur un échantillon représentatif, 68 % des TPE et PME sont aujourd'hui convaincues des bénéfices concrets du numérique. Cela signifie donc que 32 % ne sont pas convaincues. Le taux de convaincus monte à 72 % sur le thème de communication avec les clients ce qui montre que le numérique appliqué à leurs problématiques leur parle, plutôt que le numérique en général. Début 2020, 36 % des entreprises avaient peur de perdre leurs données. Il faut donc trouver un équilibre entre freins et leviers pour les amener au numérique.

En ce qui concerne les équipements et les usages, les dirigeants de TPE et PME sont des personnes très connectées. 88 % possèdent un smartphone. Seuls 37 % ont un site Internet institutionnel ce qui semble être un chiffre très particulier à la France. Nous retrouvons cela dans l'indicateur européen *Digital economy and society index* (DESI) qui comporte une dimension concernant l'intégration des technologies par les entreprises : la France est en retard en visibilité Internet, globalement et plus particulièrement par rapport aux pays du Nord. Le chiffre est encore plus bas pour les sites de e-commerce, puisque seulement 9 % des entreprises avaient un site au début de l'année 2020.

En revanche, une spécificité de la France est que 40 % des entreprises ont un logiciel de gestion, ce qui nous met en tête du peloton européen. La France est donc assez faible en visibilité mais assez forte sur l'équipement en logiciel de gestion, ce qui est probablement lié à l'obligation – datant de 2018 ou 2019 – d'avoir un logiciel de caisse. Cette contrainte peut donc devenir un avantage pour les TPE et PME qui disposent ainsi de données de gestion.

Nous avons aussi quantifié les TPE et PME à accompagner. Notre cible maximale, avant la crise, était de 2,6 millions d'entreprises en nous centrant sur les structures productives. En entités juridiques, nous montons à 3,8 millions d'entreprises, mais il ne s'agit pas que d'entreprises ayant réellement une activité économique.

Nous avons aussi réalisé une segmentation des dirigeants de TPE et PME, puisque ce public est très hétérogène. Nous avons effectué cette segmentation suivant la dynamique de projet et la maturité numérique des entreprises. Nous ne nous sommes pas limités à leur maturité numérique car nous n'accompagnons pas de la même façon un dirigeant d'entreprise qui a des projets et un dirigeant qui n'en a pas, un dirigeant qui est sur le point de transmettre son entreprise ou un dirigeant qui vient de racheter une entreprise. Nous avons donc cinq segments : prudents, demandeurs, réceptifs, statiques, opportunistes. Nous concentrons les actions de France Num sur 1,7 million d'entreprises qui correspondent aux trois segments des prudents, demandeurs et réceptifs. Tout l'enjeu des dispositifs d'aide est de bien atteindre ces cibles prioritaires pour que les mêmes réceptifs voire opportunistes n'en soient pas toujours les bénéficiaires.

L'indicateur européen DESI paraîtra bientôt. Il est basé sur des enquêtes Eurostat et n'interroge annuellement que les PME, pas les TPE. Une grande enquête sur les TPE est réalisée tous les six ans : la prochaine occurrence aura lieu en 2022. Ce sont des enquêtes de l'institut national de la statistique et des études économiques (INSEE) dans le cadre d'Eurostat.

Les difficultés rencontrées par les acteurs sont d'abord le manque de conviction sur les apports du numérique. Nous considérons que France Num a pour mission d'améliorer le terrain afin que l'action de nos partenaires et des acteurs privés puisse se déployer plus facilement.

Le deuxième sujet qui revient partout est le manque de temps : le dirigeant de TPE est pris par le temps de tous les côtés, y compris à cause d'un numérique subi qui lui prend du temps. Il faut donc convertir le numérique à son avantage, faire en sorte qu'il ne constitue pas seulement une charge avec des démarches administratives, des factures, des paperasses.

Nous constatons également une difficulté à percevoir le retour sur investissement, à voir ce que le numérique apportera concrètement. Les dirigeants ont du mal à choisir, à décider comment faire, par quoi commencer. Nous travaillons aussi spécifiquement à la complexité des aides, des dispositifs, de l'offre, des acteurs.

La crise sanitaire a eu un impact positif de prise de conscience et constitue globalement une opportunité pour les filières numériques française, européenne et internationale, y compris pour les géants du Web (GAFAM). Nous entendons énormément parler de ce sujet aujourd'hui, ce qui peut aboutir aussi à une saturation et à la création d'arnaques. Il faut faire attention, lorsque nous communiquons beaucoup sur un sujet, au risque d'apparition de pièges et nous surveillons ces problèmes. L'enjeu est donc de convertir l'urgence en progrès à long terme.

Une progression évidente est visible dans les baromètres réguliers de la fédération du e-commerce et de la vente à distance (Fevad) pour les volumes de vente en ligne. La proportion de TPE et PME passées au numérique est toutefois assez différente et nous attendons sur ce point les retours de notre baromètre. Nous avons des indicateurs de l'association française pour le nommage Internet en coopération (Afnic) qui montrent une nette progression des demandes de nom de domaine en « .fr », donc certainement une augmentation de la présence sur Internet des TPE et PME.

Dans la crise sanitaire, nous avons aussi observé des actions de débrouillardise très utiles. Elles concernent des TPE et PME qui utilisent le *click and collect* ou différentes solutions permettant à leurs clients de commander à distance et de venir chercher leurs produits. Nous voyons là l'enjeu crucial d'avoir un fichier clients. À France Num, notre travail consiste aussi à identifier de tels leviers spécifiques pour faire basculer les TPE et PME.

Nous avons conduit une action « Clique mon commerce » lors du deuxième confinement pour sélectionner une petite centaine d'offres permettant de faire du *click and collect*, de la livraison, de la gestion et de la logistique. Un appel à projets effectué en urgence nous a permis de proposer ce site pour faciliter le choix aux commerçants, artisans et restaurateurs.

Lors du premier confinement, nous avions conçu un guide pour les commerçants et artisans sur les sujets de livraison et de *click and collect*. Nous avions aussi démarré une chronique radio dans laquelle nous communiquions par des témoignages sur la webradio Frenchweb. En effet, communiquer par des témoignages est très efficace auprès des TPE et PME, en leur montrant ce que passer au numérique a apporté à un de leurs pairs.

France Num a trois grandes missions dont la première est de piloter cette politique publique, d'animer et d'outiller les acteurs. Ce n'est pas un moindre sujet que d'avoir chacun la même vision de la transformation numérique et de savoir où nous en sommes. Nous ne sommes ni les derniers ni les premiers. Nous suivons un chemin et il est important de partager cette même vision de la transformation numérique, les mêmes priorités et d'adapter les dispositifs en fonction de nos objectifs.

L'écosystème de France Num est constitué de soixante partenaires et de 3 000 activateurs : conseillers publics des réseaux consulaires, consultants privés, offreurs de solutions, banques… Dans le pilotage de la politique publique, nous gérons la marque France Num qui est une marque collective. Nous n'agissons pas par des actions propres à France Num mais nous coordonnons des actions de l'écosystème.

Nous avons un site Internet qui présente les actions des partenaires, sur lequel le public peut demander des recommandations ou avoir accès aux aides. Une plateforme collaborative avec nos soixante partenaires nous permet d'accélérer la diffusion de l'information, avec une offre de référencement des activateurs et une offre d'animation. Nous avons également des projets pour renforcer ce réseau de terrain constitué des activateurs.

Une autre de nos missions est de démontrer les bénéfices concrets du numérique. À ce titre, une émission télévisée *Connecte ta boîte* se déroule actuellement en trois épisodes. Il s'agit de démontrer concrètement l'intérêt du numérique pour des métiers très traditionnels puisque nos exemples concernent un ferronnier d'art, un couple de boulangers-pâtissiers et une guide de moyenne montagne. Nous valorisons les métiers et nous montrons les apports du numérique.

Notre rôle consiste aussi à soutenir des actions, voire en conduire en propre puisque le plan de relance donne à France Num un financement qui le lui permet. Nous finançons ainsi des diagnostics proposés gratuitement par les réseaux consulaires aux entreprises. Nous avons mis en place le chèque numérique de 500 euros. Nous faisons des appels à projets pour sélectionner des opérateurs proposant des accompagnements-actions afin de répondre au besoin induit par le fait que l'offre est riche mais qu'il faut accompagner le passage à l'action.

Un prêt France Num est en cours de mise en place. Il est destiné à sécuriser les banques pour prêter à de petites entreprises pour des petits projets de transformation numérique d'un volume maximal de 50 000 euros.

La particularité de France Num, en tant qu'initiative publique, est que notre réseau inclut des acteurs privés, donc des offreurs de solutions. France Num est géré en partenariat avec les régions. Nous présentons notre réseau de façon territoriale car la relation de confiance de la TPE s'établit avec un contact de proximité. Nous travaillons sur l'animation du réseau avec les régions et avec les filières numériques régionales. Nous avons un enjeu de qualité de la description sur la base de données des activateurs pour permettre à une TPE de choisir en connaissance de cause, les critères pouvant aller du respect du Règlement général sur la protection des données (RGPD) au fait que la société est française ou non, mais nous ne référençons pas uniquement des sociétés françaises ou européennes.

France Num ne s'associe, en tant qu'initiative de l'État, qu'à des partenaires institutionnels même si nous avons beaucoup de demandes de partenariat de grandes sociétés privées.

M. Philippe Latombe, rapporteur. Vous avez dit que de nombreuses PME et TPE disposent d'un logiciel de gestion du fait d'une obligation réglementaire mais qu'elles n'ont que rarement un site Internet ou un site marchand. Comment expliquez-vous ce décalage ? Le numérique n'est-il pas un levier commercial pour les TPE et PME ? Est-ce la raison pour laquelle vous faites cette émission télévisée de témoignages de professionnels ?

Mme Bénédicte Roullier. Nous constatons aussi un retard de la France en ce qui concerne la consultation individuelle des réseaux sociaux. Il semblerait donc qu'il existe un comportement français particulier sur les réseaux sociaux, la France se trouvant en retrait. Je n'en connais pas la raison. L'indicateur européen contient une partie sur les usages de l'Internet et la France se trouve plutôt en tête pour l'utilisation des outils bancaires, mais les Français utilisent en revanche moins que les autres pays les réseaux sociaux pour s'informer.

Nous essaierons de mieux comprendre la vente en ligne dans l'enquête que nous réalisons actuellement. Nous observons, comme dans d'autres pays européens, une stagnation pour les PME et nous étudierons plus finement la vente en ligne qui utilise aujourd'hui de multiples canaux.

En ce qui concerne la visibilité et la présence sur Internet, je pense que vous avez raison et c'est effectivement la raison pour laquelle nous lançons l'émission *Connecte ta boîte* avec de nombreux témoignages. Il se pose un problème de perception, de crainte, de manque de

confiance. Je pense aussi que, tout simplement, certaines entreprises sont présentes sans le savoir sur Internet, par exemple sur Google, et sont même parfois très bien notées. J'ai ainsi recherché des entreprises de la petite ville de Figeac. J'ai trouvé un boucher et un plombier très bien notés que j'ai appelés pour leur demander s'ils avaient des besoins de numérique, s'ils étaient sur Internet. Ces entreprises savaient à peine qu'elles étaient présentes sur Internet. Je pense que nous avons donc un problème de représentation concrète. Il faut que l'entreprise se mette à la place de son client qui la trouvera sur Internet. Entrer dans cette perception est la première étape pour 32 % des TPE et PME.

M. Aurélien Palix. L'émission *Connecte ta boîte* fait un focus sur la relation client et la vente en ligne, mais a aussi pour objectif de promouvoir l'utilisation d'outils de gestion.

M. Philippe Latombe, rapporteur. Quand vous demandez aux TPE et PME si elles sont présentes sur un site marchand et qu'elles répondent non, quels sont les freins qu'elles signalent ? Pourquoi est-ce facile de les convaincre d'aller sur un site ou quels sont les freins qu'il faut lever ?

Mme Bénédicte Roullier. Dans l'enquête du Boston Consulting Group (BCG) et de Ernst Young et associés (EY), nos prestataires ont réalisé avec des dirigeants éloignés du numérique trente entretiens de deux heures et demie. Nous avons assisté à certains d'entre eux.

Certains de ces dirigeants ne font même pas partie de la cible de France Num parce qu'ils sont statiques ou prudents selon notre segmentation. Ce sont des dirigeants d'un certain âge, qui ont l'impression d'avoir beaucoup donné, qui ont une certaine vision de la qualité de leur travail et se sentent un peu malmenés par le numérique. Ils disent que ce n'est pas eux qui feront cette transition, ce qui nous conduit à réfléchir à plusieurs leviers.

Nous discutons en particulier avec le conseil supérieur de l'ordre des experts-comptables du fait que la numérisation permet de valoriser une entreprise pour la transmettre. Nous aurons besoin d'arguments plus précis pour faire levier. Par exemple, combien vaut l'entreprise selon qu'elle dispose ou non d'un fichier numérisé de ses clients ? Combien vaut l'entreprise selon qu'elle a ou non un site Internet ? Ceci nous donnera des leviers lorsque le discours général sur le numérique ne fonctionne pas.

Dans le cas d'un hôtel, vous ne le ferez pas « bouger » en lui disant qu'il faut être sur Internet de façon générale. Ce qui l'intéresse est de savoir combien cela lui rapportera d'être sur Internet. Ce qui le convaincra est le fait qu'un pair est sur Internet, que cela lui apporte tant de clients en plus et que la commission s'élève à tant, donc que cela bénéficie à son modèle économique. Nos leviers doivent être appliqués à un métier. Il faut pouvoir comparer avec les pairs.

Par ailleurs, l'énorme problème du temps revient constamment. Le dirigeant d'entreprise n'a pas le temps et c'est un énorme frein pour le passage au numérique.

M. Aurélien Palix. Un frein évident au référencement en ligne est le coût, pas forcément le coût financier, mais le coût en termes de temps. Créer une boutique en ligne signifie référencer les produits, ce qui nécessite un investissement en temps. Certains patrons de TPE et PME n'en disposent pas.

Le confinement a changé la donne et nous espérons le voir dans le baromètre France Num dont nous aurons bientôt les résultats. La vente en ligne a été un moyen de survie pour beaucoup de commerces.

M. Philippe Latombe, rapporteur. Il existe deux coûts : le coût en temps et le coût commercial de l'accès aux plateformes. Est-ce un frein mis en avant par les TPE et PME ? Nous avons beaucoup parlé de la taxe imposée aux plateformes, qui a été répercutée aux vendeurs. Cela a-t-il marqué ? Est-ce un frein ?

M. Aurélien Palix. Je ne sais pas si ce frein a été visible dans l'étude BCG, mais ce n'est pas particulièrement un frein ces derniers mois, étant donné que nous avons mis en place suite au deuxième confinement le programme « Clique mon commerce » qui recense justement les offres gratuites ou à tarif réduit. Nous avons constaté une importante mobilisation de l'ensemble des offreurs de solutions, y compris les places de marché qui ont proposé des taux réduits pendant le confinement. Ces offres perdurent encore aujourd'hui. Si ce frein a existé avant la crise, je pense qu'il est moindre depuis le confinement.

Mme Bénédicte Roullier. Les cas de figure sont différents pour de petites entreprises dans le secteur industriel pour lesquelles les investissements peuvent être importants. Nous ne parlons pas seulement de gens qui vendent en ligne : il peut s'agir de contrats, de réservations et pas uniquement de commerce.

Toutefois, pour notre cœur de cible, je ne considère effectivement pas que l'argent soit un frein d'autant plus que beaucoup de modèles économiques prennent la forme d'abonnement et que le chèque de 500 euros permet de couvrir environ six mois d'abonnement. Pour un site institutionnel, il existe des abonnements à 50 ou 100 euros par mois ce qui ne constitue *a priori* pas un frein pour démarrer.

De plus, une bonne politique de numérisation est « j'investis et cela me rapporte » donc je ne considère pas que l'argent soit un frein.

M. Philippe Latombe, rapporteur. Vous avez aussi parlé du temps. Les TPE et PME ont-elles le réflexe de confier la création et la maintenance de leur site à des sous-traitants ?

Mme Bénédicte Roullier. Je n'ai pas de chiffre précis et c'est lié à la question de la compétence numérique. Nous considérons que la compétence numérique peut, dans une petite entreprise, être interne ou externe. Il ne faut surtout pas considérer qu'elle doit être interne. Je pense que les deux cas de figure existent sans que nous ayons de statistique sur l'ensemble de la cible.

M. Philippe Latombe, rapporteur. Même si le chef d'entreprise a une compétence et qu'il est convaincu de la nécessité d'avoir un site marchand pour montrer ce qu'il propose, a-t-il le réflexe de penser que son temps est plus précieux consacré à d'autres activités et de faire appel à quelqu'un d'extérieur pour le faire ? Veut-il au contraire absolument maîtriser l'intégralité de la démarche ?

M. Aurélien Palix. Nous n'avons malheureusement pas suffisamment de données car les enquêtes que nous avons menées ne sont pas entrées dans ce degré de détail. Toutefois, l'initiative France Num consiste justement à référencer des activateurs qui peuvent être des offreurs de solutions ou des consultants numériques. Ceux-ci peuvent accompagner les entreprises dans cette démarche et pourraient faire le travail « à la place » du chef d'entreprise, en bonne intelligence évidemment, car il ne s'agit pas de livrer une solution sans consulter le chef d'entreprise. Si le chef d'entreprise souhaite avoir le conseil ou l'appui d'un professionnel, il peut se tourner vers un activateur France Num référencé avec une certaine garantie de qualité.

Mme Bénédicte Roullier. Certaines des offres à destination des TPE incluent une assistance à la mise en ligne du contenu. Certaines de ces offres sont françaises et il est essentiel pour la souveraineté de stimuler par cet accompagnement la qualité de l'offre française, donc la qualité de la relation client des offreurs de solutions. L'offre ne doit pas se réduire à un outil vide. Ces accompagnements sont, dans certains cas, inclus dans les abonnements.

M. Aurélien Palix. Nous en avons discuté avec certaines plateformes. Le volet accompagnement est un de leurs arguments de vente auprès des TPE.

M. Philippe Latombe, rapporteur. Qu'en est-il par rapport aux pays voisins ? Les autres pays qui sont à peu près au même niveau que nous ont-ils une démarche identique ou différente ?

Mme Bénédicte Roullier. Les politiques d'accompagnement des TPE et PME existent depuis longtemps, dans d'autres pays comme en France. Les sujets souvent traités portent sur la gestion des aides aux entreprises. Les positionnements vis-à-vis des questions de souveraineté sont différents suivant les pays. Que ce soit sur Internet en général, les démarches en ligne ou la transformation numérique des TPE et PME, les pays du Nord sont plutôt en avance, la France est au milieu et les pays du Sud ont tendance à être derrière, mais cela dépend des pays. Cela varie aussi avec l'organisation administrative, selon que les pays sont plus ou moins centralisés ou régionalisés, mais je ne peux pas être plus précise.

M. Philippe Latombe, rapporteur. Vous êtes-vous inspirés de pratiques d'autres pays ? Échangez-vous avec des homologues ou des collègues étrangers ?

Mme Bénédicte Roullier. Oui, les actions de France Num ont été définies au sein du conseil national du numérique et nous travaillons encore avec ce conseil en faisant des comparaisons internationales. Les actions de France Num n'ont pas été définies par la DGE sans lien avec le contexte. En outre, nous avons de nombreux d'échanges sur le plan européen. Il faut malgré tout penser que les TPE ne constituent pas un public unique pour lequel un levier unique fonctionnera. C'est pourquoi nous avons réalisé une segmentation.

Nous discutons aussi de la façon d'atteindre les TPE et de les faire passer au numérique avec des prestataires privés qui nous contactent parce qu'ils sont sur le marché de l'équipement numérique des TPE, au niveau européen, voire mondial. J'avais partagé avec l'une de ces sociétés le chiffre de 68 % de TPE et PME convaincues des bénéfices concrets du numérique pour leur activité. J'ai obtenu comme réponse que ce chiffre était relativement élevé.

M. Philippe Latombe, rapporteur. Lorsque vous parvenez à convaincre une entreprise, vous interroge-t-elle sur la cybersécurité ? Prenez-vous l'initiative de lui en parler ? Est-ce un sujet qu'elle découvre *a posteriori* ? Est-ce une source de craintes ? Nous savons que les TPE et PME sont assez facilement attaquables par des rançongiciels. Elles sont dans une situation de vulnérabilité.

Mme Bénédicte Roullier. Nous avons posé cette question dans l'étude effectuée début 2020 et nous aurons bientôt une actualisation. 36 % des entreprises ont peur de perdre leurs données. Cela fait donc effectivement partie des craintes. Le basculement vers le numérique se joue sur la confiance et le choix.

M. Philippe Latombe, rapporteur. Ne les accompagnez-vous pas *a priori* dans ce domaine ? Lorsque vous leur parlez du numérique comme axe de développement commercial ou de gestion, leur parlez-vous aussi de cybersécurité ?

Mme Bénédicte Roullier. La priorité de France Num est effectivement de les convaincre des enjeux, même si la cybersécurité est un sujet pour nous.

M. Aurélien Palix. Si nous les encourageons tout en leur faisant miroiter en même temps tous les risques, nous risquons de ne pas « embarquer » les TPE et PME. Nous suivons de très près le sujet de la cybersécurité et, dans le plan de relance, une stratégie sur la cybersécurité a été lancée dans le quatrième plan d'investissements d'avenir (PIA 4). Cela a été annoncé par le président de la République en février dernier.

Cette stratégie comporte un volet sur la diffusion de la cybersécurité, en particulier dans les collectivités locales. L'agence nationale de la sécurité des systèmes d'information (ANSSI) a été dotée, dans le plan de relance, de 136 millions d'euros pour sécuriser les collectivités locales.

Aucun budget propre n'est encore identifié pour sécuriser les TPE et PME mais, en revanche, des actions sont en cours. Typiquement, nous avons élaboré avec l'ANSSI, les chambres de commerce et d'industrie (CCI), les chambres de métiers et de l'artisanat (CMA) et le groupement d'intérêt public contre la cyber malveillance (GIP ACYMA) un guide très simple à destination des TPE et des PME qui leur donne en quelque sorte le premiers gestes d'hygiène en matière de cybersécurité. La cybersécurité consiste parfois en des habitudes très simples telles que changer son mot de passe régulièrement, faire attention de ne pas utiliser une clé USB provenant de l'extérieur sans précaution… Ce guide d'hygiène va de points très simples à des aspects plus compliqués.

Nous discutons actuellement avec les CCI, les CMA et Bpifrance qui mène des actions sur la cybersécurité, notamment des diagnostics. Nous regardons qui fait quoi pour savoir comment passer à l'échelle et essayer de sensibiliser de manière large l'ensemble des TPE et PME.

En revanche, ce n'est pas un argument que nous mettons particulièrement en valeur lorsque nous essayons de convaincre une TPE ou PME. Bien évidemment, lorsqu'elle a entrepris sa démarche, il est important de lui faire prendre conscience des risques mais, pour lui faire faire ses premiers pas numériques, parfois sans même qu'elle le sache puisque certaines sont référencées sur Google sans le savoir, nous essayons de mettre en exergue les avantages de la numérisation en termes de retour sur investissement plutôt que les risques.

M. Philippe Latombe, rapporteur. Je comprends votre réponse mais les experts de la cybersécurité nous disent qu'il faudrait commencer à penser cyber dès le départ, dès la numérisation pour avoir un process complet. Je me demandais donc si les chefs d'entreprise se posent cette question dès qu'ils commencent à se numériser ou si cela vient plus tard et comment, dans ce cas, leur donner ces gestes d'hygiène élémentaire sur les changements de mot de passe, les clés USB…

M. Aurélien Palix. Plus la question est posée en amont, mieux nous sommes préparés. En plus de ce guide, nous réfléchissons à lancer des diagnostics, même si nous ne pourrons évidemment pas diagnostiquer toutes les TPE et PME de France et de Navarre.

Un autre sujet qui nous paraît important est de proposer des solutions clés en main sur la cybersécurité. Plutôt que France Num, cela concerne ma sous-direction qui travaille sur les technologies. Il faut que l'entrepreneur se demande comment assurer sa transition numérique de manière sécurisée et, idéalement, il faut qu'il bénéficie d'une offre globale sur la cybersécurité ce qui n'est pas évident aujourd'hui parmi les offres existantes.

M. Philippe Latombe, rapporteur. Ne travaillez-vous pas en commun avec Cybermalveillance sur ce sujet ?

Mme Bénédicte Roullier. Cybermalveillance est partenaire de France Num et nous travaillons effectivement avec eux.

M. Aurélien Palix. Il existe une double relation puisque le GIP Cybermalveillance est partenaire de France Num et que la DGE siège au conseil d'administration du GIP. Le guide a été élaboré en partenariat avec eux.

Mme Bénédicte Roullier. Nous pensons également organiser une action intermédiaire consistant à former les activateurs France Num. Ce sont eux les contacts de terrain avec les TPE. Les former est un enjeu important.

M. Philippe Latombe, rapporteur. Comment voyez-vous aujourd'hui l'évolution de la numérisation des TPE et PME ? Est-ce de plus en plus facile ? Se produira-t-il un effet « boule de neige » et d'entraînement, parce que chaque entreprise a un pair qui a déjà fait le « grand saut » ? Verrons-nous une accélération de la numérisation ou cela interviendra-t-il de façon assez linéaire ? Je ne vous demande pas de prévoir l'avenir mais avez-vous des objectifs ? Comment les suivez-vous ?

Mme Bénédicte Roullier. Nous avons des objectifs mais certains sont des objectifs de moyens, dans le plan de relance, les réformes prioritaires et le programme budgétaire.

Dans le plan de relance, nous avons l'objectif d'accompagner 300 000 entreprises au titre de France Num d'ici le 31 décembre 2022. Cela ne comprend pas les objectifs de l'émission *Connecte ta boîte* pour laquelle nous avons de gros retours d'audience. Nous avons un impact assez massif lié à l'exposition. Nous avons par ailleurs traduit la vision qu'a France Num de la transformation numérique en indicateurs compatibles avec les indicateurs européens : la visibilité, la vente en ligne ou la transaction en ligne, la gestion.

Le chemin est malgré tout long et nous sommes probablement sur une accélération assez légère, dans une logique linéaire. Il faut attendre les résultats pour conclure. Je pense que l'accélération en pourcentage d'entreprises qui passent au numérique est plus complexe qu'en volume du côté des consommateurs où nous constatons une explosion des actes numériques

Nous insistons aussi toujours sur le fait qu'il s'agit d'une politique économique. C'est le résultat économique qui compte. L'important est l'avantage économique qu'en tire l'entreprise et le numérique n'est qu'un moyen. Il est fréquent que le sujet se détourne sur des chiffres. Les petites entreprises, notamment dans le secteur de l'hôtellerie, y sont très sensibles. Être sur un plateforme en se faisant capter 40 % de la valeur leur fait se poser des questions.

Pour nous, il reste important d'insister sur l'intérêt de l'activité économique. Le numérique n'est pas un but en soi mais un moyen au service de l'activité. Le programme *Connecte ta boîte* a été conçu ainsi, comme les témoignages et les actions liés à France Num. C'est la caractéristique de France Num et cela nous semble être le levier principal.

Il ne faut pas oublier que le numérique peut être perçu comme une charge par les entreprises. Les logiciels induisent une complexité et il faut resituer l'ensemble dans une politique économique.

M. Philippe Latombe, rapporteur. En termes d'équipements et non seulement de numérique pour faire de la vente sur une plateforme, les entreprises s'équipent-elles plus et sont-elles sensibles à la modernité de leurs outils informatiques ?

Mme Bénédicte Roullier. En ce qui concerne l'équipement, la question du financement peut constituer un sujet mais cela dépasse notre périmètre. Nous avons des chiffres d'équipement mais nous ne savons pas forcément si l'équipement est perçu comme obsolète.

M. Philippe Latombe, rapporteur. Souhaitez-vous attirer notre attention sur un sujet particulier ? Existe-t-il un frein pour lequel nous auriez besoin d'un coup de pouce du législateur ? S'agit-il au contraire de problèmes de financement plutôt que de problèmes législatifs ?

M. Aurélien Palix. Je ne pense pas que nous ayons de sujet réglementaire spécifique. Nous ne souhaitons pas que la numérisation soit subie comme une obligation mais plutôt qu'il s'agisse d'une démarche volontaire de la part des entreprises. Elles doivent comprendre qu'elles ont tout intérêt à se numériser pour augmenter leur activité.

Mme Bénédicte Roullier. Il me semble qu'une priorité nationale relative aux compétences numériques, y compris dans nos organisations, est nécessaire. Je ne sais pas dans quelle mesure cela concerne le législateur.

Audition, ouverte à la presse, de M. Paul-François Fournier, directeur exécutif en charge de l'innovation de Bpifrance
(15 avril 2021)

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. L'audition de M. Paul-François Fournier, directeur exécutif en charge de l'innovation de la banque publique d'investissement Bpifrance, doit nous permettre d'évoquer le financement des entreprises technologiques qui est évidemment un levier essentiel pour la création de licornes et pour la protection de la souveraineté numérique française et européenne.

Je pense que notre rapporteur sera également très intéressé par la façon dont Bpifrance soutient l'innovation dans le plan d'investissements d'avenir (PIA) et par son expérience durant la crise sanitaire. Comment ces financements ont-ils continué à se mobiliser ?

M. Philippe Latombe, rapporteur. Je souhaite vous interroger sur trois sujets. Le premier concerne votre approche de la notion de souveraineté numérique. Il s'agit d'une question rituelle lors de nos auditions qui provient de la grande diversité des définitions de cette notion. Comment définissez-vous cette notion et, surtout, comment est-elle prise en compte dans votre action de soutien et de financement des entreprises ? Je voudrais que vous nous fassiez part des différents instruments mobilisés ou gérés par Bpifrance, dont le fonds « French Tech Souveraineté ».

Ma deuxième question porte sur le plan Deeptech dont Bpifrance est l'un des principaux artisans. Je voudrais faire avec vous un bilan de sa mise en œuvre, notamment dans la crise sanitaire, et vous entendre sur les difficultés que peuvent rencontrer les entreprises technologiques pour se financer. Plusieurs interlocuteurs ont en effet mentionné lors des précédents échanges la nécessité de passer par le marché américain pour se financer faute de l'habitude, de la part des investisseurs français, de composer un portefeuille comportant des actifs au contenu technologique important. Je voudrais savoir si nous avons, selon vous, une véritable difficulté pour garder nos pépites comme cela nous est assez souvent indiqué.

Enfin, je ne peux pas ne pas revenir sur la polémique qui a concerné Bpifrance au sujet de son usage du *cloud* d'Amazon pour héberger les données du prêt garanti par l'État (PGE). Au-delà des critiques dans lesquelles je ne veux pas que nous rentrions, je voudrais savoir quelle analyse vous faites *a posteriori* de ce choix et comment vous voyez les géants du Web (GAFAM) dans l'environnement des *start-up* et des entreprises du numérique.

M. Paul-François Fournier, directeur exécutif en charge de l'innovation de Bpifrance. La souveraineté est une problématique qui revient assez fortement dans le débat public depuis quelques mois et quelques années, en particulier avec la crise, mais qui était déjà présente auparavant et revêt, selon les interlocuteurs, des caractéristiques assez diverses. De façon générale, il s'agit de maîtriser un certain nombre d'outils ou d'éléments de production.

Notre vision de ce sujet est résolument offensive. Depuis la création de Bpifrance, nous sommes convaincus qu'innovation et souveraineté sont intimement liées et que, pour être souverain, il faut avoir une logique de puissance technologique, donc des écosystèmes aussi efficaces et puissants que possible dans la technologie.

Suite à ce constat et avec le soutien de l'État, nous avons pris avec M. Nicolas Dufourcq une option très forte au moment de la création de Bpifrance en constatant que

l'innovation a beaucoup changé en France depuis une vingtaine d'années. Nous avons vécu une période très riche avec de grandes filières industrielles très innovantes dans les années 1970 et 1980. Nous avions de grands groupes, de grands centres de recherche et développement (R&D) qui avaient le monopole de l'innovation. Avec le digital, l'innovation a complètement changé et le modèle le plus créateur de valeur est maintenant celui des *start-up*. Même si les filières traditionnelles continuent à être innovantes, les *start-up* sont aujourd'hui l'outil de création de valeur au début du processus d'innovation. Nous avons donc mis en place, avec l'État, une action très volontariste pour le financement des *start-up* autour de deux axes.

Le premier axe consiste à faciliter la création de *start-up*. Nous mettons en place des financements très significatifs au travers de dispositifs tels que les bourses French Tech, des avances remboursables, des prêts « innovation » ou des prêts d'amorçage pour donner aux jeunes et moins jeunes entrepreneurs le signal que la puissance publique accompagne ce processus de création. Nous avons ainsi presque triplé depuis 2013-2014 le nombre de *start-up* que nous finançons, aujourd'hui proche de mille entreprises par an. Nous avons donc une politique de diffusion de la création de *start-up*. Un point important pour nous est le changement de regard des jeunes ingénieurs, chercheurs ou entrepreneurs dans les écoles d'ingénieurs ou de commerce qui, aujourd'hui, considèrent la voie de la création de *start-up* comme une voie importante.

Le deuxième axe, pour que ces entreprises ne restent pas une forêt de bonsaïs, nécessite que nous disposions d'un écosystème dynamique d'investissement de capital-risque, donc de fonds d'investissement dynamiques et puissants, pour accompagner la croissance de ces entreprises. Suivant l'exemple de Londres, nous pensons que la France doit devenir un grand pays de l'industrie du capital-risque au niveau européen. Depuis cinq ou six ans maintenant, nous avons mené avec l'écosystème des fonds une action volontariste de croissance et de développement de la taille des fonds pour leur permettre d'accompagner la croissance de ces entreprises avec des moyens significatifs, notamment grâce aux programmes d'investissements d'avenir.

La taille moyenne des fonds dans lesquels Bpifrance était investisseur en 2012-2013 était de 80 millions d'euros. Aujourd'hui, la taille moyenne des fonds dans lesquels nous investissons est de plus de 200 millions d'euros, proche de 250 millions d'euros. Cet écosystème grandit donc. Le capital-risque français est passé de deux milliards d'euros en 2013-2014 à plus de cinq milliards d'euros cette année et la France est l'un des rares pays à avoir été en croissance en 2020.

Ce capital-risque français est de plus en plus européen. Il compte des fonds de plus d'un milliard d'euros et nous avons bien l'intention de continuer. De plus, nous avons plus de dix milliards d'euros de *dry powder*, c'est-à-dire de capacité à investir dans les années à venir. Cela a permis en 2020, malgré la crise, de réaliser 80 levées de vingt millions d'euros, alors que nous n'en comptions qu'une quarantaine en 2016. Douze levées de plus de 100 millions d'euros ont eu lieu l'année dernière en pleine période de covid contre six en 2016. Nous voyons donc bien la dynamique et la maturité de cet écosystème.

Nous sommes convaincus d'être au début de cette dynamique, qu'il faut continuer. C'est un message important. Je fais souvent le parallèle avec Airbus : nous sommes en train de créer une nouvelle filière industrielle, comparable aux filières traditionnelles, mis à part que ce sont des filières de tech avec des entreprises jeunes qui deviennent des entreprises de taille intermédiaire (ETI) de technologie. Nous avons parfois le sentiment qu'il a fallu pour créer Airbus et la filière aéronautique française une décision politique de quelques semaines entre la France et l'Allemagne. Cela a, en réalité, pris plutôt vingt ou trente ans. Nous

demandons une continuité de l'action publique. Même si, avec le digital, ce type de filière est plus rapide à créer, il faut du temps et nous sommes au début du processus de création d'une grande filière de technologie avec des entreprises de plus en plus matures.

La croissance de cet écosystème nous semble nécessaire dans les années à venir pour qu'il donne sa pleine puissance. Il est encore jeune puisqu'il n'a que cinq ou six ans. Je rappelle que le capital-risque américain est né dans les années 1950, que la Silicon Valley est née dans les années 1950. Je ne dis pas qu'il faudra soixante-dix ans mais cinq ans n'est qu'un début dans ce type de dynamique et il faut persévérer.

Nous souhaitons ajouter deux sujets importants pour la souveraineté à cette dynamique. Nous sommes d'abord convaincus que nous allons vers une révolution de la *deep tech*, c'est-à-dire que les industries traditionnelles connaîtront la même rupture que le digital, avec des *start-up* venant disrupter les industries traditionnelles. Nous le voyons très bien dans le spatial que je pensais pourtant être une industrie de grands groupes. De multiples briques technologiques arrivent des *start-up*. C'est aussi le cas dans de nombreux domaines tels que la cybersécurité ou la santé. Ce sont souvent des sujets en rapport avec la question de la souveraineté.

Nous devons, avec l'État, accompagner cette nouvelle vague d'innovation. C'est la raison pour laquelle nous avons lancé voici deux ans un plan Deeptech qui vise à rapprocher notre écosystème de recherche de l'écosystème des entrepreneurs et investisseurs. Cet écosystème de recherche est de qualité au niveau mondial mais n'est pas suffisamment en connexion avec l'écosystème des entrepreneurs et des fonds d'investissement. D'une certaine façon, le jeune chercheur est comme le jeune ingénieur était voici cinq ans. Il faut qu'il considère la possibilité de valoriser le fruit de sa recherche par une *start-up*, sans en être forcément le patron, mais qu'il participe et réfléchisse avec l'écosystème des entrepreneurs.

Les priorités des années à venir sont ce changement culturel, l'accélération de la chaîne de financement, grâce aux sociétés d'accélération des transferts de technologie, l'adaptation des fonds de financement à ces sujets de *deep tech*, dont la nature est différente de celle des sujets du digital. Notre plan Deeptech a deux ans et des dynamiques commencent à émerger. Nous sommes au début d'un processus qui devrait nous permettre de créer de nouvelles entreprises, dans des domaines souvent souverains, souvent industriels. Nous espérons qu'ils nous permettront de créer de nouvelles entreprises françaises qui apporteront des solutions à ces problématiques d'avenir.

Il reste évidemment la question de la connexion avec les filières traditionnelles. Nous pensons que certaines de ces entreprises deviendront de grandes entreprises, comme cela est en train de se produire dans le digital. Certaines passent le cap des plusieurs milliards d'euros et, dans les années à venir, compte tenu de la dynamique en cours, nous pensons que des entreprises de la tech seront dans le CAC40 et vaudront huit ou dix milliards d'euros, qu'à un certain moment, certaines de ces entreprises pourront et devront être réintégrées dans les filières traditionnelles, car elles auront besoin de capacités de production, de savoir-faire de qualité d'usine ou de réseaux de distribution présents dans les filières traditionnelles ou parce qu'elles sont des briques de ces filières.

Nous avons donc annoncé, avec France Industrie, une plateforme nommée Tech In Fab qui vise à rapprocher les industries traditionnelles et ces pépites de la tech pour qu'elles fassent du commerce ensemble et, éventuellement, que ces grands groupes ou ces ETI les rachètent pour moderniser leurs entreprises.

Notre métier est d'apporter et de développer des opportunités afin que les filières françaises et l'État aient le maximum d'options pour choisir des solutions françaises. Pour que ces solutions soient efficaces, il faut souvent que ces entreprises deviennent internationales et, pour certaines d'entre elles, qu'elles s'attaquent au marché américain qui reste un marché extrêmement important et dynamique.

M. Philippe Latombe, rapporteur. Comment Bpifrance gère-t-elle le continuum de l'accompagnement de ces *start-up*, depuis le *sourcing* d'une entreprise propriétaire d'une technologie qu'elle souhaite développer jusqu'à ce que cette entreprise devienne incontournable pour cette technologie ? Comment intervenez-vous ? Comment sourcez-vous les entreprises ? Comment les accompagnez-vous, lors des premières phases, puis lorsqu'elles grandissent ?

M. Paul-François Fournier. Nous disposons de trois outils très complémentaires : le financement de l'innovation ou l'aide à l'innovation, l'investissement et l'accompagnement.

Le premier outil est à la base de notre métier en ce qui concerne le *sourcing*. L'État au travers des programmes d'investissements d'avenir ou l'Europe nous donnent des moyens nous permettant de proposer aux très jeunes entrepreneurs des outils de financement, le premier étant une bourse French Tech pour un entrepreneur au moment de la création de son entreprise. Il s'agit en fait d'une subvention pour lui permettre de commencer, de créer son entreprise et d'aller chercher les premiers financements dits des *friends and family*, ou des *family offices* et des gens autour de lui qui peuvent l'aider. Cette bourse peut aller jusqu'à 50 00 euros ou 90 000 euros dans le domaine de la *deep tech* en lien avec le monde de la recherche.

Nous avons ensuite des dispositifs de prêts, tels que le prêt d'amorçage ou le prêt innovation. Ils nous permettent, au fur et à mesure que l'entreprise grandit, de lui prendre du risque. C'est notre rôle et il est assez significatif pour ces prêts. C'est pourquoi ils sont garantis par l'État. Ils nous permettent de financer le début de la vie de l'entreprise pour qu'elle accoste le monde essentiel de l'investissement. C'est le deuxième pilier qui prendra alors le relais.

Cette première partie du financement est extrêmement importante et extrêmement territoriale. Je pense que c'est une des forces de Bpifrance, comparée à un certain nombre d'acteurs européens ou mondiaux dans le financement de l'innovation. Nous avons cinquante implantations régionales que vos collègues connaissent et côtoient je l'espère. Nous avons des équipes spécialisées d'ingénieurs, au plus près des écosystèmes d'incubateurs, des pôles de compétitivité. Nous sommes aux côtés des régions qui nous confient des moyens. Nos trois donneurs d'ordres sont en effet l'État, les régions et de plus en plus l'Europe.

Notre première étape est donc un accompagnement avec un financement dans lequel nous prenons un fort risque, assumé. Il s'agit en général au départ d'une petite subvention, puis de prêts pour aider l'entreprise à trouver les premiers fonds.

M. Philippe Latombe, rapporteur. Faites-vous du préfinancement de crédit impôt recherche ? C'est un outil plébiscité par l'ensemble des interlocuteurs que nous avons entendus. Ils disent qu'il ne faut pas y porter atteinte mais que le processus est un peu lent. Les banques classiques ne savent pas trop faire. Avez-vous cette expertise et cette compétence ?

M. Paul-François Fournier. Nous le faisons même si la mobilisation du crédit impôt recherche est un processus un peu long car il faut que l'État valide l'enveloppe. Nous essayons

de le faire de plus en plus, mais tous nos financements permettent justement d'avoir les moyens d'attendre le délai de remboursement du crédit impôt recherche.

De façon générale, tous nos moyens permettent de trouver des financements, que ce soit du montant du crédit impôt recherche lui-même ou que ce ne soit pas lié à ce crédit, ce qui simplifie la situation en nous permettant d'aller plus vite dans le financement de l'entreprise, sans entrer dans la logique administrative de la mobilisation du crédit impôt recherche. Inversement, notre conviction est qu'il faut regarder pourquoi nous ne pourrions pas aller plus vite. C'était une des demandes régulières des entrepreneurs : pouvoir mobiliser plus rapidement et avoir des remboursements plus rapides du crédit impôt recherche.

Après les premiers financements qui servent à lancer l'entreprise et à trouver des financements autour de soi, il faut que l'entreprise parvienne à convaincre un fonds d'investissement qui prendra la relève. Nous continuerons à aider au financement, mais le fonds est tout de même l'outil qui donnera les moyens. Il faut aussi reconnaître que c'est lui qui sélectionne les entreprises puisque le dispositif des *start-up* fonctionne avec une sélectivité progressive pour que les moyens soient donnés aux entreprises les plus prometteuses. Nous finançons massivement les fonds d'investissement et, tout d'abord, les fonds d'amorçage.

Quelques 36 fonds d'amorçage sont répartis sur l'ensemble du territoire français. Il s'agit d'une vraie richesse française, grâce aux programmes d'investissements d'avenir. Ces fonds d'amorçage sont extrêmement territorialisés : près de 60 % de leurs financements proviennent des territoires, en dehors de l'Ile-de-France. C'est la première validation tierce permettant de s'assurer que d'autres acteurs que nous sont convaincus de l'intérêt du projet.

Nous finançons au début mais nous jugeons qu'il faut ensuite que d'autres financent et c'est l'objet de l'amorçage : s'assurer que d'autres acteurs mettent des moyens. En l'absence d'autres acteurs, les règles européennes font que l'État ne peut pas continuer à financer seul au travers de Bpifrance une entreprise sur laquelle personne d'autre ne met un minimum de moyens de financement privés et c'est conforme à notre conviction.

Il existe aussi un réseau de fonds sectoriels thématiques, parfois régionalisés. Nous finançons cet écosystème de près de 120 fonds français qui devient de plus en plus puissant et important. Il peut de mieux en mieux accompagner les entreprises, en termes de développement mais aussi pour avoir les moyens d'aller à l'international ou de faire des acquisitions pour grandir

Nous travaillons avec Business France et des dispositifs de diagnostic d'innovation. Ce sont de petites missions de conseil, très concrètes, comme « Pitch&Win » pour apprendre à « pitcher », en anglais mais pas uniquement, c'est-à-dire pour savoir expliquer en dix minutes son entreprise. C'est un exercice absolument essentiel pour se faire comprendre. Nous faisons aussi des diagnostics sur la stratégie, sur l'industrialisation et nous avons beaucoup de missions d'accompagnement à l'international pour permettre aux entreprises d'accoster en Europe ou aux États-Unis. Dans certains domaines, c'est absolument essentiel.

Enfin, un enjeu important et complexe consiste à tisser le lien avec les filières traditionnelles pour faire travailler les grands groupes français, les ETI ou les PME avec cet écosystème de *start-up*. Il s'agit à la fois de faire en sorte que ces *start-up* aient des clients, qu'elles trouvent de vrais marchés et de vrais clients et, pour les grands groupes, d'avoir l'opportunité de travailler avec des *start-up* proches de chez eux, qui leur permettent d'accélérer leur digitalisation ou d'intégrer une nouvelle brique technologique et de rendre plus compétitive leur offre. Ce maillage est un grand enjeu des années à venir pour ré-innover dans ces filières.

Nous sommes donc très heureux que France Industrie parraine avec nous cette plateforme Tech In Fab et commence, dans la *deep tech*, à créer des liens de plus en plus étroits entre les *start-up* et les grands fleurons industriels. Ces *start-up* deviennent de véritables éléments de la filière et permettront de créer des solutions, de retrouver de nouveaux marchés. Elles pourront rester indépendantes ou intégrer des groupes ou des ETI ayant besoin de ces briques technologiques.

M. Philippe Latombe, rapporteur. Qui co-investit dans les fonds dans lesquels vous investissez ? S'agit-il de particuliers, de *family offices*, de fonds de fonds contenant des fonds étrangers ? Pensez-vous que le milieu bancaire et assuranciel est suffisamment présent dans ces fonds, qu'il a une culture de l'investissement dans les *start-up* et la *deep tech* ?

Les Français adorent l'assurance-vie, les fonds en euros qui sont constitués d'obligations d'État et d'immobilier. Les compagnies d'assurance ont-elles suffisamment intégré le virage technologique et la nécessité d'investir dans ces entreprises d'avenir ? En ce qui concerne les établissements bancaires avec leurs capitaux propres, jouent-ils le rôle d'investisseurs en capital et en risque, pas uniquement en prêts ?

M. Paul-François Fournier. Nous sommes un acteur important de ces fonds. Nous investissons une part minoritaire mais très importante dans ces fonds. Ce sont des sociétés de gestion qui captent des moyens financiers des acteurs du monde de l'assurance, de la banque, des *family offices*, des fonds de pensions, des banques publiques pour lever un fonds d'investissement. Leur première mission est de convaincre les investisseurs, souvent institutionnels ou *family offices*, d'investir dans leur fonds pour, ensuite, faire leur vrai métier : investir dans le capital des *start-up*.

Nous sommes un acteur important de cet écosystème puisque nous sommes volontaristes. Un de nos rôles consiste à être aux avant-postes pour aider à la transformation de l'écosystème, au travers des financements du programme d'investissements d'avenir. Nous avons incité les fonds à augmenter leur taille moyenne en investissant plus. Par exemple, nous leur demandons de passer leur fonds de 100 millions à 200 millions d'euros en les aidant à lever et en donnant le signal que nous sommes prêts à suivre. Nous investissons aussi plus dans des fonds d'amorçage, en particulier de la *deep tech*, car ce domaine est un peu plus risqué que la technologie. Nous mettons dans ces fonds régionaux ou ces fonds d'amorçage un peu plus que les 20 % que nous mettons en moyenne dans un fonds afin d'aider à monter les tours de table. Nous jouons un rôle « activiste » pour pousser l'écosystème à changer d'échelle.

Les co-investisseurs dans ces fonds sont rarement des personnes physiques. Cet écosystème est peu accessible aux personnes physiques et c'est la raison pour laquelle nous avons lancé une première initiative avec le fonds « Bpifrance Entreprises 1 ». Toutefois, ce sont plutôt des *family offices* – c'est-à-dire des gens qui ont des moyens très significatifs – qui investissent dans ces fonds, les tickets allant en général de 500 000 euros à un million d'euros. Les investisseurs sont aussi des institutionnels : les assureurs, les banques et les fonds de pension étrangers qui, de plus en plus, viennent investir dans des fonds français. Je crois qu'il faut s'en réjouir. Beaucoup de fonds étrangers de capital-risque viennent sur la place française et c'est une bonne nouvelle mais le mieux est qu'ils investissent directement dans les fonds français avec nos investisseurs et nos sociétés de gestion françaises afin de booster notre filière française de la finance et de la faire croître.

Un des gros enjeux consiste à attirer les fonds de pensions, en particulier américains, pour qu'ils investissent directement dans les fonds français. Nous commençons à y parvenir.

C'est un axe important pour faire croître notre écosystème de fonds français et l'aider à grandir.

La situation évolue bouge du côté des institutionnels, d'abord parce que l'État a joué un rôle d'incitation très significatif depuis quelques années. Vous avez déjà entendu parler de l'initiative de Philippe Tilly. Nous étions hier avec M. Nicolas Dufourcq et M. Philippe Tilly pour faire le point sur cette initiative. Il s'agit de pousser les principaux institutionnels français à investir beaucoup plus significativement dans les fonds importants, à 500 millions d'euros ou un milliard d'euros, pour accompagner les importantes levées de fonds en cours de développement en France. Ce processus est nouveau et la rentabilité n'était jusqu'à présent pas très bonne. Il est difficile de demander à quelqu'un, dont l'assurance-vie, avec une rentabilité maximale, est le métier, de prendre plus de risques dans un écosystème non encore mature.

La bonne nouvelle est que la mécanique mise en place collectivement produit ses effets. Chaque élément de l'écosystème nourrit l'autre et permet de faire grandir l'ensemble. Cette dynamique permet aux *start-up* de grandir, de lever plus de fonds et d'être plus rentables, donc plus attractives, en termes de retour sur investissement pour ces acteurs. La rentabilité de ces fonds est maintenant stable et aura tendance à s'accroître, puisque la technologie jouera un rôle de plus en plus important. Nous arrivons à une rentabilité qui permet d'attirer de plus en plus de capitaux français et étrangers pour parvenir, dans les années qui viennent, à un écosystème mature qui donne toute sa puissance.

La situation évolue. Il faut continuer car le mouvement est encore naissant mais les signaux sont plutôt positifs même s'il reste d'importants progrès à faire. Nous aurons besoin de beaucoup de capitaux dans l'avenir car notre potentiel de *start-up* est croissant. Nous avons de plus en plus de jeunes entreprises nées voici quelques années et, avec le plan Deeptech, nous en créerons de plus en plus. Elles auront massivement besoin de capitaux. Si tout fonctionne bien, nous aurons besoin de toujours plus de capitaux et ce sera plus facile si l'écosystème de la tech démontre qu'il crée de la valeur pour ces investisseurs institutionnels.

M. Philippe Latombe, rapporteur. Le fait que des fonds de pensions ou des fonds étrangers fassent partie des fonds ne serait-il pas, pour eux, une stratégie d'identification à moindre coût de pépites qu'ils pourraient ensuite acheter ? Participer à de tels fonds n'est-il pas, pour des fonds de pensions ou des fonds étrangers, un moyen assez facile de sourcer des pépites qu'ils pourraient acquérir ?

Par ailleurs, les entrepreneurs sont-ils aujourd'hui suffisamment ouverts à l'idée d'ouvrir leur capital à des fonds ? Cela signifie diluer leur capital, parfois décorréler la partie technique de la partie gestion financière. L'entrepreneur, dans une *start-up* ou une ETI de la tech, est-il suffisamment mature pour accepter ces investissements ?

Aux États-Unis, il a fallu du temps et cela fait maintenant partie de leur culture. Nos entrepreneurs ne préfèrent-ils pas plutôt avoir moins de fonds mais avec des personnes physiques qu'ils connaissent, faisant partie de leur environnement amical ou avec qui il existe un lien d'être humain à être humain ? Ce n'est pas tout à fait pareil avec un fonds.

M. Paul-François Fournier. Pour répondre à votre première question, je crois au contraire que les fonds de pensions, américains par exemple mais pas uniquement, constituent un formidable moyen d'aider notre écosystème français à grandir et à créer ces *start-up* sans que le risque soit avéré. Nous visitons ces fonds de pensions, une ou deux fois par an. Ce sont les fonds de retraites, des hôpitaux du Canada, du Québec ou de Pittsburg ou des pompiers d'Atlanta. Je les ai rencontrés et ils ne manifestent aucun intérêt pour l'avenir de l'entreprise.

Le seul et unique regard qu'ils ont est le retour sur investissement, puisque ce sont les retraites de ces pompiers ou personnels soignants. En passant par ces fonds, le lien est uniquement financier pour la majorité de ces investissements.

Pour les *corporate*, le risque peut exister et nécessite probablement une vigilance ponctuelle pour certains fonds très sectoriels. Sans rentrer dans les détails, cette vigilance existe. Elle permet parfois de se demander si le fait qu'un industriel de tel ou tel pays entre dans un fonds d'investissement pose une question d'accès à du savoir. Le niveau de risque est moins important que lorsqu'ils investissent directement dans l'entreprise mais il existe une vigilance, de notre part et de celle de l'État. Il est déjà arrivé quelquefois que des investissements ne se fassent pas pour des raisons de souveraineté sur certaines thématiques.

La difficulté provient de ce que nous ne croyons pas pouvoir construire un écosystème qui ne soit pas un minimum ouvert sur le reste du monde. C'est là toute la complexité de la souveraineté. Avoir des entreprises qui soient de vraies solutions technologiques pour moderniser des filières nécessite souvent qu'elles soient très innovantes donc puissantes et compétitives au niveau mondial. L'accès à des capitaux est essentiel pour les faire croître puisque, même si beaucoup d'argent dort dans les bas de laine, beaucoup d'argent se trouve aussi à l'international et permet de réduire notre déficit du commerce extérieur. Il ne s'agit pas seulement de pétrole, mais aussi d'argent investi dans nos *start-up*. Parfois, des fonds américains ou étrangers européens qui co-investissent dans des entreprises peuvent aussi donner à l'entreprise un accès à un réseau de compétences ou à un réseau de relations qui a de la valeur.

Pour nous, il faut garder ce chemin de crête entre un écosystème de fonds français puissants que nous développons, qui soient connectés à des fonds étrangers équilibrés pour permettre aux entreprises de se développer sur les marchés internationaux et de devenir de grandes entreprises innovantes, concurrentielles par rapport à leurs homologues internationaux. Cet équilibre est compliqué. Nous y travaillons tous les jours mais nous ne croyons pas qu'un écosystème français uniquement financé sur les fonds français soit pérenne. Nous pensons que ces entreprises doivent s'ouvrir à l'international pour être puissantes et apporter des réponses efficaces à notre écosystème.

En ce qui concerne la culture, nous avons beaucoup progressé. Je comprends l'impatience sur ces sujets de souveraineté technologique : nous sommes sur la bonne voie. Il faut reconnaître que nous avons pris un peu de retard durant ces quinze ou vingt dernières années mais nous sommes sur une dynamique plutôt positive.

Dans la tech traditionnelle, dans le digital, nous avons maintenant plusieurs générations – ce qui participe à la qualité de l'écosystème – avec des entrepreneurs qui ont réussi et réinvestissent dans les *start-up* ou recréent des *start-up*. Il nous semble que cet ensemble est à un niveau tout à fait conforme aux références internationales. Cet actif a été bâti collectivement depuis une dizaine d'années.

Lorsqu'un entrepreneur dit ne pas vouloir des fonds, c'est en général un souci d'ambition ou de modèle, mais l'ensemble des entrepreneurs considèrent qu'intégrer un investisseur est un moyen considérable de grandir et nous les accompagnons dans cette logique. Nous poussons aussi les fonds d'investissement à avoir une culture de l'accompagnement, c'est-à-dire à ne pas seulement regarder l'argent mais à créer un écosystème avec des talents, des *managing partners*. Ce sont souvent d'anciens entrepreneurs qui accompagnent l'entrepreneur pour lui permettre d'accélérer et de capitaliser sur les succès et les échecs de ses prédécesseurs.

Dans la *deep tech*, nous sommes au début du changement culturel. Nous avons annoncé voici deux jours un rapport avec le Boston Consulting Group (BCG), Bio-Up et France Biotech. Notre écosystème d'entreprises de biotechnologie est important mais la crise a montré un certain nombre de limites. C'est l'occasion de faire croître notre ambition. Un axe important concerne les talents. Pour ces entreprises de *deep tech*, les marchés sont plus complexes et l'accès aux marchés est souvent plus complexe parce que la science elle-même est plus complexe que dans le digital. Le financement est parfois plus long parce qu'il faut plus de capitaux.

Nous avons encore du travail pour l'acculturation des uns et des autres, y compris des fonds d'investissement, des accompagnateurs, des chercheurs qui envisagent l'entreprenariat. Il faut savoir comment attirer des talents. Nous avons appris ces dernières années que la solution est en général dans la constitution d'une équipe de co-fondateurs, des binômes ou des trinômes où chacun a des éléments de compétences complémentaires pour couvrir le spectre des besoins de ces entreprises. Cela nous a été confirmé par notre rapport sur la biotech qui est en quelque sorte la partie émergée de ce monde des entreprises de technologie.

M. Philippe Latombe, rapporteur. Lors des auditions précédentes, nombre d'entrepreneurs ont dit ne pas souhaiter des subventions – même si elles sont utiles au départ – mais avoir surtout besoin de clients. Ils jugent une relation de client à fournisseur plus intéressante que des subventions. Le client a des exigences auxquelles il faut savoir répondre ; il faut savoir négocier un contrat…

Bpifrance a un remarquable carnet d'adresses d'entreprises innovantes. Comment êtes-vous prescripteur de ces entreprises auprès des grands comptes ? Vous avez parlé des grandes entreprises et dit que vous les mettiez en relation mais vous faites, indirectement, partie de l'État. Comment arrivez-vous à devenir prescripteur de ces entreprises auprès de l'État ?

Je donne un exemple : nous avons entendu une entreprise très innovante dans le domaine de la sécurisation des cartes du type cartes d'identité, soutenue par vous, retenue par des pays étrangers mais pas par la France. Pourtant, c'est une pépite française que vous avez identifiée, qui a été identifiée par tous, qui a eu des prix d'innovation. Cela pose des questions sur la suite, sur « l'après-BPI ».

M. Paul-François Fournier. C'est une question au cœur de nos sujets actuels. Vous avez raison et nous sommes de ce point de vue très clairs : nous pensons qu'un euro de client vaut plus qu'un euro d'investissement ou de financement de Bpifrance. Nous ne minimisons pas notre action, mais notre enjeu est d'aider l'entreprise, de créer des conditions permettant qu'un écosystème de capital-risque les fasse croître. Mais, à la fin, une entreprise vit de ses clients et de sa capacité à se développer. Comme les fonds, nous sommes convaincus que notre écosystème doit être propice à ce développement.

Je pense que nous n'avons jusqu'à présent pas complètement réussi à réaliser ce tissage entre l'écosystème du digital et l'écosystème des entreprises françaises. Nous y mettons beaucoup d'énergie. Nous nous appliquons à nous-mêmes cette logique. Vous avez certes parlé du PGE mais nous travaillons avec cent *start-up* françaises. C'est parfois difficile car, même si nous ne sommes pas une très grande entreprise, nous avons nos contraintes, nos modes de fonctionnement. Nous sommes bien conscients de l'importance de ce sujet. Nous avons créé voici cinq ans le hub avec la conviction que le moment viendrait un jour de connecter l'écosystème. Nous avons relancé voici quelques jours la plateforme Tech In Fab. Nous déployons tous nos efforts pour que les filières et les grands groupes s'intéressent aux *start-up*.

Je pense que nous franchissons actuellement une étape, que nous passons en fait la troisième étape de la maturité de l'écosystème des *start-up* et de ses rapports avec les grandes entreprises. La première étape fut de l'ordre de l'amusement, chacun créant son incubateur tandis que les grands groupes invitaient les *start-up* un peu comme on invite un pauvre pour l'aider. Lors de la deuxième étape, nous avons vu plus de scepticisme sur la capacité de ces entreprises à intégrer du business, le sentiment étant que nous en faisions trop sur les *start-up*. Je pense que les grandes entreprises sont maintenant convaincues que ces *start-up* deviennent de vraies entreprises et ne sont plus une mode, mais de véritables solutions. La meilleure preuve en est le partenariat que nous avons signé avec France Industrie. Il est assez symbolique, très important et a été suivi par une trentaine de grands groupes industriels, ce qui montre que la situation évolue.

Des dizaines d'entreprises valent déjà entre 500 millions et un milliard d'euros, ont plusieurs millions de chiffre d'affaires et des dizaines d'autres suivront, je vous le promets. Ce ne sont plus de petites *start-up*, mais des entreprises capables de résoudre les problèmes industriels de très grandes entreprises et d'apporter des solutions industrielles. Leur puissance financière et leur exposition internationale leur permettent de trouver des solutions.

Il reste un énorme travail d'acculturation. C'est parfois une de nos inquiétudes mais nous essayons de faire évoluer les mentalités avec ces plateformes, avec des partenariats, par de la communication au travers de nos évènements à l'occasion desquels nous mettons en valeur les succès de ces entreprises.

Je souhaite revenir sur un point important pour la souveraineté : les acquisitions de *start-up* par l'étranger. Notre ambition, en tant que financeur, est que des entreprises deviennent de très grandes entreprises et recréent des usines comme Ynsect à Amiens ou Aledia à Grenoble. Ces *start-up* recréent donc de l'industrialisation et nous espérons que certaines d'entre elles seront au CAC 40 dans cinq ou dix ans. Toutefois, une bonne part d'entre elles arriveront – c'est la règle du jeu – à une limite en capacité de réseau de distribution ou seront une vraie opportunité pour ces filières. L'enjeu est alors qu'elles puissent être rachetées. Il s'agit que les filières traditionnelles rachètent ces entreprises pour les intégrer et leur donner toute leur puissance grâce à leur propre réseau de distribution ou à leur savoir-faire industriel.

Nous regardons cet enjeu par le prisme des acquisitions étrangères de ces *start-up*, ce qui nous interpelle à chaque fois. L'État et nous-mêmes sommes vigilants sur ces sujets, en particulier sur des sujets souverains. Pourtant, nous oublions parfois de nous demander pourquoi nos filières traditionnelles ne choisissent pas d'acquérir ces *start-up*. Lorsque nous regardons les chiffres de nos fonds d'investissement, les acquisitions de *start-up* en 2019 par des fonds dans lesquels nous sommes investisseurs se font pour 60 % auprès d'investisseurs français. La grosse majorité des sorties se font donc avec des investisseurs français. 12 % des sorties se font auprès d'investisseurs européens donc près des trois quarts sont des acquisitions par des investisseurs européens. 17 % des sorties sont des acquisitions par des investisseurs américains. C'est beaucoup mais ce n'est que 17 %. Par contre, parmi les 60 % acquises par des investisseurs français, la moyenne de la valorisation est le tiers de la valorisation faite par les acquisitions des investisseurs américains.

Nous devons nous interroger sur le fait que ces entreprises sont rachetées aux États-Unis, mais nous avons aussi besoin d'avoir en France des opportunités d'acquérir ces entreprises. Il faut faire en sorte que les moyens soient mis pour consolider ces acteurs en France. Le fait que nous ayons des acteurs importants qui nous permettent de devenir des consolidateurs est probablement un des moyens pour le digital. Pour la *deep tech*, il faudra

également que nos grands groupes rachètent ces belles entreprises, en particulier les plus belles d'entre elles, pas uniquement les moins valorisées.

M. Philippe Latombe, rapporteur. Vous avez en partie répondu à ma question. Je me permets de demander à nouveau comment vous pouvez prescrire auprès de l'État et des collectivités territoriales. La commande publique est un formidable levier de financement par la relation client. Comment ces entreprises qui pourraient mettre leurs technologies au service de l'État peuvent-elle être référencées à ce niveau ? Quand l'État a envie d'investir dans une solution informatique, il préfère de grands acteurs parce que c'est plus simple, qu'il suffit de passer un seul marché public et une seule commande publique. Or, il faut faire émerger des acteurs de taille beaucoup plus petite. Comment Bpifrance est-elle un prescripteur de ces entreprises auprès de l'État pour qu'elles aient accès à la commande publique ?

M. Paul-François Fournier. Nos plateformes telles que Tech In Fab ou la plateforme du hub qui porte sur une dimension plus *deep tech* nous permettent de travailler avec l'union des groupements d'achats publics (UGAP) ou avec l'État et les acheteurs de l'État. Il m'est arrivé plusieurs fois d'intervenir auprès des acheteurs de l'UGAP pour leur expliquer la dynamique des *start-up* et comment faire.

Il faut reconnaître que la commande publique n'est probablement pas le meilleur moyen de faire de l'innovation. Les politiques d'achat sont parfois contradictoires avec la capacité d'innovation et il faut trouver des moyens de traiter le sujet de l'innovation, souvent différent de l'achat de produits matures. Sur des sujets de souveraineté ou de développement de l'innovation, il faut avoir les moyens de sortir de la seule logique à court terme des moyens pour donner sa chance à une *start-up*.

Plus globalement, nous faisons tout ce que nous pouvons, mais, à un moment, nous arrivons au bout de nos capacités. Notre métier est de financer les entreprises. Nous le faisons le mieux que nous pouvons, mais nous avons nos propres enjeux d'efficacité. Notre rôle est de donner de la visibilité à ces *start-up*, mais je ne crois pas raisonnable que nous devenions l'agent de transformation de l'État dans sa commande publique. Nous sommes un opérateur résolument centré sur la culture de l'entreprise pour apporter à l'État une proximité avec l'entreprise et une capacité à déployer des moyens simples de financement. Je ne nous sens pas devenir une agence de transformation de l'État.

Nous militons pour un modèle qui a commencé à donner ses fruits, celui de l'agence de l'innovation de la défense. Elle est notre interlocuteur potentiel vis-à-vis de la défense. Dans la santé, nous avons proposé avec le Boston Consulting Group et France Biotech la création d'une agence de l'innovation de la santé.

Ces agences doivent être l'aiguilleur, l'agent de la transformation et le parti pris des *start-up*, dans l'écosystème de la santé ou de la défense. Quel que soit son nom, nous avons besoin d'une structure qui nous donne des priorités dans le domaine de la santé et qui puisse accompagner les entreprises, être leur avocat pour simplifier les processus administratifs. Cette structure doit aussi être un acheteur de produits innovants, ici des produits de santé, mais c'est valable dans de nombreux autres domaines. Son regard doit être innovant et probablement plus souverain. Nous avons de plus en plus besoin de ce type d'interlocuteur qui soit la voix de l'État client et la voix des entreprises françaises à l'intérieur de l'administration, en particulier des entreprises innovantes qui sont plus fragiles et ne disposent pas forcément de lobbyistes pour leur permettre de comprendre les méandres des cabinets et des administrations. Une telle agence, en plus de guider les entreprises, pourrait leur donner un vrai modèle économique, puisqu'elles ont besoin de plus de visibilité qu'une structure traditionnelle.

M. Philippe Latombe, rapporteur. Souhaitez-vous aborder un autre sujet ?

M. Paul-François Fournier. J'insiste sur notre conviction que la souveraineté est aussi un acte très offensif consistant à continuer à développer nos écosystèmes d'innovation pour multiplier les opportunités en ayant de plus en plus de très belles entreprises de tech internationales, dans le digital et, demain, dans la santé ou la *deep tech*. Les acheteurs et les partenaires des filières traditionnelles auront alors de plus en plus d'opportunités de trouver des solutions efficaces à intégrer dans leur propre filière. Nous bâtirons ainsi ce cercle vertueux de la puissance qui permettra de rayonner et de créer de la valeur en France.

Audition, ouverte à la presse, de Mme Martine Garnier, responsable du département « Numérique et mathématiques appliquées », et de M. Frédéric Precioso, responsable scientifique « Intelligence artificielle », de l'Agence nationale de la recherche (ANR)

(15 avril 2021)

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. Nous recevons Mme Martine Garnier, responsable du département « Numérique et mathématiques appliquées » au sein de l'agence nationale de la recherche (ANR), accompagnée de M. Frédéric Precioso, responsable scientifique « Intelligence artificielle ».

L'agence nationale de la recherche est un établissement public à caractère administratif, placé sous la tutelle du ministère de l'enseignement supérieur, de la recherche et de l'innovation (MESRI). Nous avons souhaité organiser cette audition au regard du fort contenu technologique de la notion de souveraineté numérique. L'audition d'aujourd'hui devrait nous permettre d'aborder le rôle de l'agence en matière de soutien à la recherche dans le domaine numérique et plus particulièrement les sujets ayant trait à l'intelligence artificielle. Votre agence est en effet chargée du pilotage de la stratégie nationale « Intelligence artificielle ».

M. Philippe Latombe, rapporteur. Je souhaite évoquer avec vous trois sujets. Le premier concerne votre approche de la notion de souveraineté numérique. Il s'agit d'une question rituelle lors de nos auditions qui provient de la grande diversité des définitions de cette notion. Comment définissez-vous cette notion et comment est-elle prise en compte dans vos actions de soutien à la recherche. Je voudrais que vous nous parliez des partenariats de l'ANR avec les autres acteurs de la recherche française dans le domaine des technologies numériques.

Ma deuxième question porte sur la stratégie nationale de recherche en Intelligence artificielle qui prend appui sur le rapport de M. Cédric Villani de 2018 et a conduit à la mise en place en France de quatre instituts interdisciplinaires d'Intelligence artificielle, dits instituts 3IA. J'aimerais faire avec vous un bilan de la mise en œuvre de cette stratégie et du rôle de l'ANR en son sein. La crise sanitaire a-t-elle ralenti cette dynamique ? Aurons-nous besoin d'un nouveau coup d'accélérateur ? Je voudrais aussi savoir comment nous nous positionnons sur ce sujet par rapport aux autres pays européens et vous entendre sur les usages de l'Intelligence artificielle, notamment dans l'industrie.

Pour conclure, je souhaite aborder un sujet qui vous concerne fortement, celui de la formation. Aucune recherche efficace n'est possible sans formation adaptée et sans attractivité. De ce point de vue, comment jugez-vous notre système de formation ? La recherche est-elle suffisamment attractive pour les talents dans des domaines où les rémunérations dans le secteur privé sont parfois beaucoup plus importantes que dans la recherche publique ? Je pense notamment aux grands acteurs type géants du Web (GAFAM).

Enfin, comment faire pour que nous restions dans la course en termes d'innovation ?

Mme Martine Garnier, responsable du département Numérique et mathématiques appliquées de l'agence nationale de la recherche (ANR). L'agence nationale de la recherche est un établissement public à caractère administratif placé sous la

tutelle du ministère de l'enseignement supérieur, de la recherche et de l'innovation. Le rôle de l'agence est de mettre en œuvre le financement de la recherche sur projets pour les opérateurs publics, qu'il s'agisse d'opérations entre eux ou avec des entreprises.

L'ANR a été créée en 2005 pour promouvoir la recherche sur projets, mais aussi pour stimuler l'innovation en favorisant l'émergence de projets collaboratifs pluridisciplinaires et en encourageant les collaborations entre public et privé. Son rôle est également de renforcer le positionnement de la recherche française aux niveaux européen et mondial. Les missions de l'agence, définies dans le décret du 1er août 2006 et révisées le 24 mars 2014, sont les suivantes :

– financer et promouvoir le développement des recherches fondamentale et finalisée, l'innovation technique et le transfert de technologies ainsi que les partenariats entre le secteur public et le secteur privé ;

– mettre en œuvre la programmation arrêtée par le ministre chargé de la recherche qui recueille l'avis des ministres exerçant la tutelle d'organismes de recherche ou d'établissements publics d'enseignement supérieur ;

– gérer de grands programmes d'investissement de l'État dans le champ de l'enseignement supérieur et de la recherche et suivre leur mise en œuvre ;

– renforcer les coopérations scientifiques aux plans européen et international en articulant sa programmation avec des initiatives européennes et internationales ;

– analyser l'évolution de l'offre de recherche et mesurer l'impact des financements alloués par l'agence sur la production scientifique nationale.

Ainsi, l'action de l'ANR vise à soutenir l'excellence de la recherche française à des degrés variés de maturité technologique, à soutenir la recherche fondamentale, à encourager les partenariats scientifiques académiques et public-privé et à favoriser des coopérations européennes et internationales.

L'ANR propose pour cela des appels à projets compétitifs et met en œuvre des processus de sélection rigoureux basés sur l'évaluation par les pairs. Ces processus respectent les principes internationaux en la matière : impartialité, équité de traitement, confidentialité, déontologie, intégrité scientifique et transparence.

Le plan d'action et la feuille de route programmatique de l'ANR définissent, pour une année budgétaire donnée, les principales actions de l'agence et les priorités de recherche. Ils détaillent les appels à projets et les instruments disponibles, offrant une vue d'ensemble de l'offre de financement de l'agence. Le plan d'action de l'ANR permet d'exprimer les efforts de recherche menés par la France pour accompagner notre société face aux grands enjeux auxquels elle est confrontée, en lien avec les défis sociétaux, les nouvelles missions et les partenariats pour le nouveau programme-cadre Horizon Europe, mais aussi les mégatendances de l'organisation de coopération et de développement économiques (OCDE) ou les objectifs de développement durable des Nations unies. Ce plan favorise ainsi la lisibilité des efforts de financement public de la recherche vers les citoyens, la promotion de la culture scientifique et permet un suivi quantifié de l'action de l'État.

Depuis 2010, l'agence est également opérateur de l'État pour la gestion des programmes d'investissements d'avenir – les PIA 1, 2, 3 et maintenant 4 – dans le champ de l'enseignement supérieur et de la recherche. L'agence assure à ce titre la mise en œuvre des

appels à projets, l'organisation de la sélection, de la contractualisation, du financement, du suivi, de l'évaluation de l'impact du projet et des actions du programme qui relèvent de ce champ. Chaque programme des investissements d'avenir fait l'objet d'une convention entre l'État et l'ANR qui définit notamment les objectifs et la gouvernance.

Le fait majeur de l'année 2020 demeure bien entendu la crise sanitaire de la covid-19 qui a conduit l'agence à s'adapter pour assurer complètement ses missions, finaliser l'ensemble des appels à projets programmés et réduire au maximum l'impact de la situation sanitaire sur l'activité de recherche de la communauté scientifique française.

Des actions spécifiques importantes liées à la covid-19 ont été prises, en particulier des mesures d'urgence mises en place dès le début de l'année 2020. Sans les détailler complètement car elles sont nombreuses, dès le début de l'épidémie, en articulation avec notre ministère de tutelle et avec le réseau *REsearch and ACTion targeting emerging infectious diseases* (REACTing), l'ANR a décidé d'accompagner l'effort national de recherche pour endiguer l'épidémie, avec un certain nombre d'appels à projets dédiés à la crise sanitaire et au soutien aux recherches.

La crise sanitaire a considérablement modifié le fonctionnement de l'agence et des laboratoires. L'ensemble des personnels de l'agence, mis en télétravail, se sont totalement mobilisés pour assurer la continuité de la mise en œuvre du plan d'action 2020. Cette mobilisation a conduit à adopter, dès l'annonce du premier confinement, des mesures exceptionnelles pour minimiser l'impact de la crise sanitaire sur l'activité des laboratoires et les processus de sélection. Nous avons fait évoluer le calendrier des appels, prolongé systématiquement de six mois les projets, reporté la tenue des comités d'évaluation qui se sont finalement tenus en septembre en format à distance. Nous avons, pour un conventionnement plus rapide, annoncé les résultats au fil de l'eau et nous avons décalé l'ouverture de l'appel à projets générique, le grand appel annuel de l'ANR, ainsi que l'ANR Tour.

Depuis le début de la crise, l'agence n'a pas raisonné en termes d'évolution organisationnelle mais plutôt en termes de capacité d'adaptation avec une mise en mode « projets » et le lancement d'actions spécifiques en cas de besoin. L'ANR a montré sa capacité à répondre aux grands enjeux sociétaux avec différents appels : le Flash Covid-19, la recherche-action Covid-19, l'appel Résilience. L'ANR a également mobilisé ses compétences en développant de nouveaux partenariats financiers pour ces appels avec différents opérateurs publics, des fondations, des régions dont la région Grand Est et d'autres établissements publics. L'ANR a ainsi démontré son agilité pour assurer complètement ses missions en matière thérapeutique, notamment avec les mesures d'urgence et les actions scientifiques spécifiques.

En dehors de la crise sanitaire, l'actualité 2020 de l'agence a été portée par l'élaboration du prochain contrat d'objectifs et de performance 2020-2025 qui fait suite à celui de 2016-2019 et à l'évaluation du Haut conseil de l'évaluation de la recherche et de l'enseignement supérieur (Hcéres). La signature avec la tutelle est prévue le 26 avril.

La loi de programmation de la recherche promulguée le 24 décembre 2020 et le plan de relance renforceront considérablement les moyens de l'ANR dès 2021.

M. Philippe Latombe, rapporteur. La programmation prévue au départ a-t-elle été modifiée ? Comment rattrapez-vous l'éventuel retard provoqué par la crise ?

Mme Martine Garnier. L'ANR a réagi très rapidement et redéfini un calendrier de façon à ne pas impacter le cycle annuel de son appel générique et de son plan d'action de façon

générale. Cette adaptation a permis de conserver et de suivre le plan d'action tel qu'il était prévu.

M. Philippe Latombe, rapporteur. Où en sommes-nous sur l'Intelligence artificielle par rapport au rapport de M. Cédric Villani de 2018 ?

Mme Martine Garnier. L'Intelligence artificielle est un enjeu majeur dont Frédéric Precioso est le responsable scientifique à l'ANR, aussi bien en ce qui concerne les grands programmes d'investissement de l'État que sur les autres actions menées au titre du budget d'intervention.

M. Frédéric Precioso, responsable scientifique « Intelligence artificielle » à l'agence nationale de la recherche (ANR). Le programme des instituts 3IA est financé sur le PIA3. En avril 2019, un jury international a sélectionné quatre sites candidats à être labellisés « institut 3IA ». Ces établissements se sont immédiatement mis au travail puisque, en septembre 2019, les quatre instituts 3IA étaient constitués et fonctionnaient. Il faut souligner que, du fait de la complexité de ces nouveaux instruments et de la diversité des consortiums impliqués, le conventionnement a été finalisé avec l'État en juillet 2020 ce qui n'a pas empêché les quatre instituts de fonctionner dès septembre 2019.

Nous arrivons à mi-parcours et, comme prévu dans le programme initial, les quatre instituts produiront à l'automne 2021 un document de synthèse de leurs deux premières années d'activité. À la rentrée 2022, le même jury international se réunira pour évaluer les réalisations accomplies et ce, malgré la crise.

Le budget actuellement alloué aux quatre instituts se monte environ à 75 millions d'euros et une dotation supplémentaire pourra être accordée si le jury international considère que les objectifs ont été atteints.

Je tiens à signaler que l'État et les différents organismes décideurs ont assoupli quelque peu certaines règles de constitution des 3IA du fait de la crise sanitaire et de la difficulté économique pour certains partenaires qui s'étaient initialement engagés. La crise modifie surtout les calendriers d'objectifs chiffrés mais n'impacte pas l'ampleur des 3IA. Les conséquences concernent par exemple l'exigence d'avoir atteint 33 % du budget financé par des industriels avec tel pourcentage d'apport en cash…

Les instituts 3IA sont financés à 33 % par l'État, à 33 % par des partenariats industriels et à 33 % par les établissements publics engagés et éventuellement les collectivités territoriales.

L'ANR, accompagnée de la mission IA constituée de l'institut national de recherche en informatique et en automatique (Inria) comme coordonnateur et de représentants du MESRI, est allée rendre visite physiquement à deux sites en septembre, entre deux périodes de confinement, puis virtuellement pour les deux derniers sites du fait de la deuxième phase de confinement. Nous avons pu constater les avancées réalisées malgré la crise, souvent même au-delà de ce qui était attendu. Le constat est donc très positif. En particulier, l'installation des instituts dans leur écosystème et le lancement de nombreux projets collaboratifs entre les établissements académiques et les partenaires privés sont effectifs.

Un des grands volets des 3IA est leur contribution à la formation. Vous mentionniez le rapport de M. Cédric Villani qui prévoyait, parmi ses objectifs, de doubler d'ici quatre ans le nombre de diplômés en IA. Les instituts 3IA se sont mis à l'œuvre et, en particulier, un certain

nombre de formations continues, en direction des partenaires industriels, sont déjà en place et actives. Du point de vue de la formation, les objectifs sont donc en passe d'être atteints.

Un autre objectif lors de la création des 3IA était de construire des hubs du maillage français en IA et que ces sites phares soient visibles à l'international et au niveau européen. C'est déjà le cas puisque, lors de l'appel à projets européen de 2020 pour la création de quatre centres d'excellence européens en IA, chacun des 3IA fait partie de l'un de ces quatre centres. Ils ont donc été immédiatement reconnus et sont bien visibles.

Notons que le modèle français a essaimé au niveau européen puisque, à la suite de la création des 3IA en France, l'Allemagne par exemple a créé cinq centres de *machine learning* ce qui couvre une partie de l'IA. Des discussions sont en cours avec l'Italie : nous avons rencontré en 2019 les instances du ministère italien de la recherche et ils mènent des réflexions pour créer quelques grands centres en IA selon le modèle français.

Plus largement, il existe d'autres structures financées dans des programmes nationaux, comme des chaires IA, et des programmes doctoraux. Les instituts 3IA s'appuient en effet, selon les instituts, sur une collectivité d'une trentaine ou d'une quarantaine de chaires d'excellence en IA. En plus de ces quatre grands centres, l'État a souhaité mailler plus précisément le territoire en finançant des chaires en IA. Ces chaires se construisent autour d'une personnalité et de son équipe. L'État finance également un programme de contrats doctoraux en IA. Sur 29 programmes doctoraux proposés, 22 ont été retenus qui maillent le territoire. Sur 170 candidatures en chaire IA, 43 ont été retenues, là aussi de façon à mailler le territoire. Le réseau des sites en IA se met donc en place et des actions des 3IA envers un certain nombre de thèses dans leur territoire commencent déjà. Le maillage voulu dans le rapport de M. Cédric Villani est donc en cours de réalisation, de façon efficace.

M. Philippe Latombe, rapporteur. Le fait d'avoir lancé ces actions permet-il une attractivité forte dans le domaine ? Cela permet-il d'attirer les talents plutôt que de les voir partir dans le privé ?

M. Frédéric Precioso. Une des actions immédiates des 3IA, qui perdure pendant leurs deux premières années d'existence, est l'attractivité à l'international, puisque chacun des quatre sites 3IA a réussi à attirer sur certains de ses postes des chercheurs internationaux. Nous avons donc fait revenir des gens des États-Unis ou d'autres pays européens. C'est un vrai succès, aussi bien en ce qui concerne la visibilité que le fait d'attirer des talents extérieurs.

Un certain nombre de talents vont toujours vers l'industrie, vers les grands acteurs des technologies en IA comme les GAFAM, mais pas seulement. Nombre des 43 chaires IA citées précédemment sont détachées, pour partie voire totalement, chez des industriels français tels que Safran, Valeo ou Criteo, donc nourrissent le tissu industriel français dans ce domaine.

En ce qui concerne l'aspect recherche, cette perméabilité entre le monde académique et le monde industriel n'est pas forcément négative et peut même être positive, puisque la plupart de ces collègues continuent à garder des liens forts avec leurs anciennes institutions académiques ou y restent à temps partiel. Ils continuent donc d'établir des collaborations de projets de recherche entre leur nouvelle entreprise et leur ancien employeur académique. Du point de vue de l'activité de recherche, retirer les trois cadres d'une équipe de recherche pour qu'ils aillent dans l'industrie oblige évidemment le reste de l'équipe à se réorganiser. Le coût est certes non nul pour l'établissement, mais cela ne coupe pas les liens. Pour la formation, c'est en revanche particulièrement impactant puisque ces collègues n'enseignent plus ou seulement très peu. Toutefois, les chaires IA hors institut ainsi que les chaires IA dans les instituts ont un volet d'enseignement associé à la chaire. Les titulaires de la chaire doivent

enseigner ce qui signifie que toutes les chaires d'excellence dans les 3IA ou hors 3IA qui n'étaient pas enseignants-chercheurs auparavant contribueront à la force d'enseignement.

Nous sommes très loin de pouvoir couvrir les besoins : la demande est forte puisque ce domaine attire énormément, que le milieu industriel est très intéressé par monter en compétences sur ces thématiques. L'objectif du rapport de M. Cédric Villani de doubler le nombre de diplômés en IA, tous publics confondus, à trois ou quatre ans est compliqué à atteindre sans l'accompagner de vraies créations de postes, d'un vrai soutien par des postes d'enseignants dans ces thématiques. Nous manquons cruellement d'enseignants-chercheurs en informatique et en mathématiques appliquées pour soutenir la demande très importante, croissante, sur la thématique de l'IA.

Je parle de l'IA parce que je suis à mi-temps responsable de l'IA à l'ANR mais j'effectue mon autre mi-temps comme professeur à l'université de Côte d'Azur. J'enseigne, je mène des projets de recherche, j'encadre des étudiants et je vois le besoin accru de recrutement d'enseignants. Je pense que mes remarques sont aussi valables pour le futur plan quantique en cours de mise en place.

Toutes ces grandes stratégies sont très positives et contribuent à la souveraineté nationale mais il faut, si nous voulons construire et renforcer un domaine scientifique, aussi bien pour le milieu industriel que pour le milieu académique, l'accompagner du soutien d'enseignants-chercheurs pour que des enseignants soient présents devant les étudiants.

Mme Martine Garnier. Dans les stratégies d'accélération, que ce soit sur la cybersécurité ou les technologies quantiques, le pilotage « programme et équipements prioritaires de recherche » (PEPR) contient un volet économique, un volet recherche, mais également un volet formation puisqu'il est indispensable que ce volet formation soit développé et soit totalement partie prenante de ces stratégies d'accélération.

Je signale aussi que, dans la formation aux compétences numériques, l'une des quatre stratégies d'accélération porte sur « Enseignement et numérique ». Le centre national de la recherche scientifique (CNRS), l'Inria et l'université d'Aix-Marseille (AMU) ont été désignés comme pilote de ce programme prioritaire de recherche avec une dotation de 77 millions d'euros.

L'ANR sera également opérateur d'un appel à manifestation d'intérêt sur des démonstrateurs numériques dans l'enseignement supérieur. Afin de soutenir cette transformation numérique, l'État a décidé d'accompagner un ensemble d'établissements représentatifs de la diversité de l'enseignement supérieur français dans toutes ses dimensions. Il s'agit d'expérimenter toutes les dimensions de la transformation numérique en vraie grandeur, dans une nouvelle approche globale. Cela concerne la transformation des cursus, les questions d'équipements, les questions de formation des enseignants et des étudiants, le renforcement des équipes d'appui et d'accompagnement des enseignants, la mise à disposition de ressources pédagogiques, de plateformes, d'outils ainsi que la politique de vie étudiante, l'amélioration des usages, la réussite des étudiants, le bien-être des enseignants… L'objectif de cet appel à manifestation d'intérêt est d'identifier et d'accompagner un certain nombre d'établissements d'enseignement supérieur qui seront prêts à devenir les démonstrateurs et les pilotes de cette transformation.

M. Philippe Latombe, rapporteur. Le processus est lancé depuis deux ans maintenant. Pensez-vous avoir identifié les angles morts de ce processus ou pensez-vous qu'il couvre bien, comme prévu au départ, la totalité du champ visé ? Faut-il procéder à des adaptations, au-delà des points dont vous avez parlé sur la formation ?

Mme Martine Garnier. Nous avons beaucoup parlé de l'enseignement supérieur mais il est important de couvrir l'ensemble de la chaîne en termes d'éducation et de formation. Même si nous sortons un peu du domaine de compétences de l'ANR, nous pouvons signaler que l'organisation des enseignements de la voie générale du lycée s'est profondément transformée récemment avec l'introduction des sciences du numérique et technologies (SNT) en classe de seconde.

Ce tronc commun permet de donner à l'ensemble des élèves des voies générale et technologique une introduction au monde numérique. L'objectif est vraiment important. Il s'agit de donner les clés et les principales composantes du numérique et de la technologie pour comprendre les enjeux fondamentaux et les problématiques actuelles. Nous revenons ainsi au thème de la souveraineté numérique. Je pense qu'elle passe aussi par la compréhension par les jeunes générations des enjeux du numérique et de leur identité numérique.

Parmi les thèmes abordés, beaucoup sont liés à ces questions de souveraineté numérique. Les ressources proposées dans Class'Code abordent Internet, le web, les réseaux sociaux, les données structurées et leur traitement, des questions de localisation, de cartographie et de mobilité. Une nécessaire sensibilisation est effectuée en mettant l'accent sur la dépendance de l'utilisateur à ces systèmes souvent assez opaques et hors du contrôle de l'utilisateur.

Cet enseignement se poursuit en première et terminale, sous le nom « Numérique et science informatique ». Les élèves doivent choisir trois spécialités parmi les douze offertes et cet enseignement propose aux lycéens de leur expliquer ce qu'il se passe dans leur smartphone, dans leur ordinateur, comment les données sont codées, transmises.

Il est important d'expliquer aux jeunes, dès le lycée, ces grands domaines du traitement et de la représentation des données, des algorithmes et langages de programmation, des machines, des systèmes d'exploitation. La mise en place de cet enseignement permettra aussi, je pense, de nourrir le vivier des étudiants de demain, avec de meilleures clés peut-être.

M. Frédéric Precioso. Le réseau créé par les quatre 3IA et le maillage des chaires IA hors institut couvrent assez bien non seulement le territoire mais aussi les thématiques. Les actions ciblées du type cybersécurité ou IA quantique qui feront partie du plan quantique viendront renforcer et densifier ce maillage. Il peut évidemment être intéressant d'avoir des appels vers d'autres chaires, de poursuivre cet effort, mais l'idée initiale est bien en train de se mettre en place et la diversité des activités de recherche sur le territoire français fait que nous parvenons à n'oublier aucun domaine. Nous discutons de ces questions au sein de l'ANR, lorsque l'État nous interroge sur nos idées quant aux différents soutiens que nous pourrions apporter, par exemple de l'IA vers les autres sciences, vers les sciences humaines et sociales…

L'idée initiale ne demande qu'à s'ancrer profondément dans le territoire et la dynamique créée autour des 3IA fait que certains sites qui n'avaient pas été sélectionnés ou même n'avaient pas concouru pour l'appel 3IA ont créé des instituts ou des centres de recherche en IA. Je pense au *Sorbonne center for artificial intelligence* (SCAI) par exemple autour de la Sorbonne à Paris, à l'institut DATAIA à Saclay, à un centre d'IA près de Strasbourg dans le plan IA Grand Est. Des intentions ont été annoncées autour de Marseille : le projet a pris un peu de retard à cause du covid mais un centre d'IA s'installera à Marseille. Bordeaux suit le même chemin. La volonté de l'État de lancer ce maillage en France essaime et fonctionne. Nous pouvons faire confiance à la communauté scientifique française pour s'organiser de façon à continuer dans ce sens. Je suis assez serein sur le fait qu'il n'existe pas particulièrement de zone d'ombre et qu'il soit éventuellement facile de combler les zones

d'ombre qui pourraient apparaître dans les années à venir par des appels ciblés comme l'ANR a l'habitude de le faire de façon très efficace.

Autant pour les chaires que pour les instituts, ce sont des programmes prévus pour quatre ans. Il sera utile de décider et d'annoncer relativement rapidement la prolongation de ces structures. Elles engagent beaucoup de partenaires industriels qui ont des objectifs et des visions à plus long terme que quatre ans. Nous sommes déjà à mi-parcours. Les partenaires industriels des sites 3IA souhaitent voir plus loin qu'à deux ans et il est important, lors de la construction d'un tel maillage, d'envoyer des signaux sur la pérennisation de cette structuration.

Je parle du plan IA qui est de mon ressort, mais il en sera de même pour le plan quantique. Il faut avoir une vision à moyen et long terme pour stabiliser les structures que nous avons fait émerger et accompagner leur pérennisation par une pérennisation du soutien.

M. Philippe Latombe, rapporteur. Votre optimisme me rassure et je prends volontiers l'idée de donner une visibilité à moyen et long terme, aussi bien sur l'IA que le quantique.

Au-delà de l'IA et du quantique, devons-nous investir d'autres sujets pour préparer notre souveraineté de demain ? Voyez-vous émerger d'autres domaines sur lesquels nous devons tout de suite nous pencher pour ne pas prendre de retard ? Nous avons un peu la fâcheuse habitude de prendre du retard et, ensuite, de « cavaler derrière le char ».

Mme Martine Garnier. Vous nous avez au début demandé notre vision de la notion de souveraineté numérique. En considérant de façon assez classique qu'il s'agit de la capacité d'un État à asseoir sa stratégie économique et industrielle, à protéger ses citoyens et sa population, à préserver son modèle social et ses valeurs par la maîtrise des technologies clés, la maîtrise des flux de données, des réseaux et des infrastructures critiques, nous avons à traiter le grand sujet de l'Intelligence artificielle mais aussi les technologies quantiques liées aussi aux notions de cybersécurité. L'ANR contribue par la diversité de ses actions de soutien au renforcement de l'écosystème et c'est vraiment là le point clé. Cet écosystème est essentiel à la souveraineté numérique.

Le plan d'action de l'ANR est structuré en quatre composantes :

– la composante recherche et innovation ;

– la composante d'actions spécifiques, telles que des défis, dont le challenge en cybersécurité ;

– la composante de la construction de l'espace européen de la recherche et l'attractivité internationale de la France ;

– la composante de l'impact économique de la recherche et de la compétitivité avec des instruments tels que des structures réunissant un laboratoire et une entreprise ou des chaires industrielles ou, en partenariat avec l'agence de l'innovation de défense, des programmes tels que le dispositif d'accompagnement spécifique des travaux de recherche et d'innovation de défense (ASTRID) et ASTRID maturation.

Les enjeux de la cybersécurité sont essentiels pour renforcer notre souveraineté numérique. L'enjeu est double au plan national : conserver notre liberté d'appréciation, de décision et d'action en cas de cyberattaque et préserver nos domaines de souveraineté

traditionnels. Cela passe par le développement d'une filière industrielle nationale ou européenne forte, compétitive dans le domaine des produits et services de cybersécurité, mais aussi par une recherche d'excellence pour préparer les futurs outils. L'anticipation est également essentielle dans la souveraineté numérique.

La cybersécurité a été identifiée comme une priorité claire du PIA 4, avec un certain nombre d'initiatives et notamment la stratégie d'accélération en cours de lancement. L'objectif de cette stratégie d'accélération est, en structurant cette filière, d'atteindre un chiffre d'affaires de 25 milliards d'euros d'ici 2025 et de doubler le nombre d'emplois.

Un PEPR est également prévu dans le PIA 4 pour un montant de 65 millions d'euros. Il permettra de financer des actions pour une période de six ans. L'enjeu est de renforcer la coordination des actions de recherche et d'innovation, d'éviter tout risque de travail « en silos ». Il ne s'agit pas d'éparpiller les moyens mais de les concentrer pour développer de nouveaux outils de cybersécurité sur toute la chaîne, c'est-à-dire aussi bien sur les aspects *hardware* que *software*, en mathématiques mais aussi en sciences humaines et sociales. Il s'agit de faire travailler l'ensemble des acteurs provenant de disciplines différentes sur des plateformes technologiques, en étroite collaboration avec les acteurs industriels et étatiques pour garantir la performance et la pertinence des outils développés.

Depuis 2006, l'ANR soutient de plus la recherche en cybersécurité de façon très interdisciplinaire par son budget d'intervention avec un programme dédié « Concepts, systèmes et outils pour la sécurité globale ». En 2014, une réorganisation du programme en cohérence avec la stratégie nationale de la recherche a pris en considération un ensemble de problèmes sociétaux avec le défi « Liberté et sécurité de l'Europe, de ses citoyens et résidents ». Les défis sociétaux ont maintenant été abandonnés dans la programmation ANR au profit d'une recherche plus exploratoire.

Dans notre appel à projets générique, l'axe « Sécurité globale, cybersécurité » demeure, avec une notion très régalienne de la sécurité. Les projets doivent se positionner par rapport à des thèmes tels que la liberté et la citoyenneté dans le cyberespace, la sécurisation des systèmes d'information, la lutte contre le cyberterrorisme. Cela sous-entend de mobiliser des domaines de recherche en lien avec la protection de dispositifs et des systèmes d'information, les réseaux physiques, les équipements et les objets. Le spectre sur lequel se positionnent les projets déposés au titre de cet axe est très large. Entre 2005 et 2020, nous avons financé dans le domaine de la cybersécurité une centaine de projets ayant un *technology readiness level* (TRL) compris entre 1 et 4 pour un montant de 55 millions d'euros environ, hors PIA.

M. Philippe Latombe, rapporteur. Vous financez donc des projets à la fois dans le PIA et hors PIA.

Mme Martine Garnier. Nous finançons des projets sur le budget d'intervention. En 2020, le budget d'intervention de l'ANR s'est monté à 781 millions d'euros, dont 620 millions d'euros dédiés aux quatre composantes du plan d'action que j'ai présentées précédemment et 471 millions d'euros pour le grand appel à projets générique constitué de 50 axes thématiques. Au titre de l'année 2020, l'ANR a financé sur l'ensemble du plan d'action 1712 projets soit une progression de 122 projets et une croissance budgétaire de 55 millions d'euros. Nous avons financé dans l'appel générique 1229 projets sur l'ensemble du spectre thématique de l'ANR. L'ANR est une agence généraliste, mais elle ne finance pas la recherche sur le spatial et la lutte contre le cancer.

M. Philippe Latombe, rapporteur. Comment nous positionnons-nous, à l'échelle européenne, par rapport à nos concurrents géostratégiques, Américains d'un côté, Chinois de l'autre, Russes ? Ce que nous mettons en place nous permettra-t-il de rester dans la course ou même d'être leaders ? Sommes-nous en train de nous faire distancer sur certains sujets ?

M. Frédéric Precioso. L'Europe est très active sur cette question de souveraineté européenne, en particulier autour du numérique et de l'IA. Elle se positionne comme une troisième voie par rapport à la Chine et aux États-Unis, avec une autre approche de la préservation de la confidentialité des données, de la vie privée. De ce point de vue, je pense que c'est une très bonne stratégie pour ne pas être en retard. En IA, en dehors de la Chine et des États-Unis, le Canada est un très bon concurrent qui se positionne sur les mêmes valeurs que l'Europe.

L'Europe met en place des infrastructures pour rester dans la course sur l'IA mais aussi sur la donnée, avec en particulier le projet Gaïa-X qui est une très importante action collective pour le partage des données au niveau européen et les supercalculateurs qui permettront de traiter ces données. En France, le supercalculateur Jean Zay opéré par le grand équipement national de calcul intensif (GENCI) est le deuxième supercalculateur en Europe.

Le choix de l'Europe est tout à fait pertinent pour se positionner sur un autre axe que la Chine et les États-Unis, ce qui nous permet de préserver la population européenne de certaines nuisances et certains défauts de ces technologies et, en même temps, de nous prémunir contre les concurrents qui ne joueraient pas le jeu. J'ai par exemple été membre du comité d'analyse des développements des dispositifs médicaux et de santé intégrant des technologies en IA, parmi les trente experts qui participaient à la création de règles de régulation et d'évaluation de ces dispositifs. C'est une façon de rester dans la course et de garantir que ce qui sera mis au service de nos concitoyens est conforme aux valeurs de l'Europe. Cette voie prise par l'Europe pour rester dans la course me paraît donc très efficace.

Lorsque vous voulez un système de reconnaissance faciale, vous pouvez refuser un modèle, si l'accord des millions de personnes utilisées pour construire le modèle ne vous est pas fourni avec le système, ce qui vous met à l'abri de solutions qui n'ont pas forcément respecté les valeurs que nous souhaitons défendre en Europe. De la même façon, dans le domaine médical, pouvoir refuser un système qui prédit la présence d'une maladie sans avoir obtenu l'accord des patients dont les données ont été utilisées pour construire l'algorithme, aussi pertinent soit-il, est une façon de se prémunir en Europe. C'est la voie choisie, en s'appuyant sur le Règlement général de protection des données (RGPD) pour mettre des régulations très strictes qui nous prémunissent dans la course et dans le type d'approche, dans les comportements d'utilisation de ces technologies.

M. Philippe Latombe, rapporteur. Ne craignez-vous pas que l'usage dans d'autres pays fasse tache d'huile et que nous importions ces systèmes, malgré ces barrières de protection ?

M. Frédéric Precioso. Les axes sur lesquels il faut être vigilant sont justement ceux qui ouvriraient des brèches dans cette stratégie. Par exemple, d'importantes avancées sont actuellement faites dans le domaine du traitement du langage et de l'analyse du langage naturel. De nouvelles solutions sont proposées chaque semaine, en particulier aux États-Unis. Le modèle qui est l'état de l'art actuel se trouve aux États-Unis et il est tellement conséquent qu'il est impossible de l'exporter. Il ne peut pas être téléchargé comme un logiciel pour être utilisé en France, car il nécessite tellement de ressources que la seule façon de l'utiliser est d'exporter les documents dans l'entreprise américaine qui a développé le système pour les

faire traduire ou analyser. Nous voyons donc tout de suite qu'un problème de souveraineté numérique européenne se pose.

Il faut que la France et l'Europe investissent cette thématique, puisque, sans autre solution que ce modèle, celui-ci deviendra l'unique solution pour analyser des documents ou les traduire dans des dizaines de langues. Microsoft a passé un contrat voici deux mois pour que ce logiciel soit le logiciel de traduction intégré à la panoplie de logiciels Microsoft. Cela signifie que, lorsque vous traduisez un document dans votre logiciel Microsoft préféré, il sera envoyé à l'entreprise américaine et la traduction vous sera renvoyée.

Cette régulation et cette approche basées sur des valeurs de protection des données et de protection du citoyen doivent être étudiées attentivement. Nous devons lancer des programmes ou des actions pour soutenir la recherche, dès qu'une avancée a lieu dans un pays qui ne partage pas ces valeurs sur le traitement de la donnée, afin pouvoir proposer des alternatives crédibles.

M. Philippe Latombe, rapporteur. C'est donc la question des valeurs qui fera la différence.

M. Frédéric Precioso. C'est la stratégie européenne et elle me semble bonne.

Mme Martine Garnier. L'Europe a des partenaires pour renforcer cette approche, comme le Canada déjà cité. Nous avons aussi des accords de collaboration avec le Japon, justement parce que nous partageons un certain nombre de valeurs, telles que le développement du lien de confiance en respectant la vie privée.

M. Philippe Latombe, rapporteur. Pensez-vous que cette vision est partagée par l'intégralité de la communauté, c'est-à-dire à la fois les scientifiques, les politiques, les dirigeants d'entreprise ? Est-ce partagé par tous les pays au sein de l'Europe ? Existe-t-il des personnes qui ne veulent pas de ces valeurs ou qui réclament plus de pragmatisme ?

M. Frédéric Precioso. Les valeurs sont partagées, mais il faut être attentif à ne pas laisser des brèches s'ouvrir, en soutenant et en proposant des alternatives. Si la France et l'Europe ne sont pas capables d'avancées sur des solutions de traitement de la langue, il sera compliqué d'imposer aux industriels européens de ne pas recourir à une solution et donc peut-être de réduire leur compétitivité par rapport à la concurrence internationale.

Mme Martine Garnier. Pour que l'ensemble de l'écosystème s'y retrouve, il faut un soutien qui arrive actuellement de l'Europe avec un cadre législatif indispensable en cours de mise en place. La Commission européenne a dévoilé sa proposition de Règlement sur la gouvernance européenne des données, le *Data Governance Act*. Ce texte garantit la confiance en donnant un cadre juridique européen au partage des données, mais doit aussi proposer une véritable base technologique, avec l'objectif d'encourager la circulation des données entre entreprises. Il faut que les entreprises et administrations publiques puissent avoir accès à un maximum de données.

L'initiative franco-allemande Gaïa-X est devenue un projet de *cloud* européen, mais il faut aussi un cadre législatif pour l'ensemble de la chaîne. Le *Data Governance Act* sera renforcé par le *Digital Services Act* et le *Digital Market Act*.

M. Philippe Latombe, rapporteur. Souhaitez-vous aborder un autre sujet ?

M. Frédéric Precioso. Vous aviez évoqué lors des échanges qui ont précédé cette audition la question de la féminisation. Ce problème est une vraie question pour nos législateurs et législatrices, dans le numérique et plus généralement dans le monde de la recherche, le monde académique et le monde industriel.

L'État et le ministère agissent et c'est donc un sujet dont l'État s'empare. Un très bon rapport de mars 2020 est présent sur le site du MESRI : il fait un état des lieux tout à fait réaliste et pertinent de la situation, sans langue de bois.

Mme Martine Garnier décrivait les actions faites dès le secondaire et parfois même plus tôt pour former les plus jeunes au numérique, pour leur donner le contrôle, la compréhension et la maîtrise du domaine. Dans ces filières toutes récentes, les chiffres de la féminisation sont déjà catastrophiques en seconde, première et terminale puisque 0,9 % de filles s'inscrivent dans ces domaines.

C'est une problématique internationale et c'est une préoccupation européenne dans les échanges que nous avons avec nos partenaires européens. Cela influera aussi sur les contributions de ces domaines technologiques, puisque, si vous excluez la moitié de la population de ces domaines, cela l'exclura aussi des produits et services qui émergeront.

M. Philippe Latombe, rapporteur. Je partage avec vous ce constat. En quoi est-ce du domaine législatif ? Faut-il que nous fassions comme pour la parité en politique ou dans les grandes entreprises ? Il s'agit d'un problème qui vient de la formation et il faut que nous ayons des politiques publiques de très long terme pour expliquer aux jeunes filles qu'elles ont la même capacité que les jeunes garçons à faire les mêmes études.

M. Frédéric Precioso. Expliquer aux jeunes filles n'est pas la bonne stratégie. Les études menées sur cette question montrent que recruter une enseignante dans une filière dans laquelle les filles ne s'inscrivaient pas fait augmenter considérablement le pourcentage de filles qui s'inscrivent dans cette filière. C'est l'effet d'exemple. Il faut travailler sur l'équilibrage des populations dans ces métiers, afin que des femmes servent d'exemple. Si vous êtes étudiante et que vous n'avez aucune professeure ou très peu de femmes dans les nouvelles filières créées pour la nouvelle agrégation d'informatique qui apparaîtra en 2022, les jeunes filles ne s'inscriront pas.

En ce qui concerne la recherche, le CNRS a, comme le ministère, publié un rapport qui est aussi très intéressant. Si une femme a moins de chances d'être promue dans sa carrière, la carrière est moins attractive. Lorsque des doctorantes finissent leur thèse et voient la place faite aux femmes au sein des laboratoires, elles préfèrent aller dans d'autres domaines où elles ont l'impression qu'elles auront une plus grande facilité à s'épanouir.

Le CNRS et en particulier l'institut des sciences de l'information et de leurs interactions (INS2I), qui concerne directement les sciences du numérique, a une page dédiée sur laquelle il indique l'index d'avantage masculin, c'est-à-dire une mesure de l'avantage qu'apporte le fait d'être un homme ou une femme dans la promotion de carrière. Cette métrique est intéressante à suivre. Les chiffres de 2020 montrent que l'index d'avantage masculin est de 1,33. Un homme a donc 33 % de chances de plus d'être promu qu'une femme. Il existe de telles métriques dont il faut s'emparer pour se donner des objectifs et améliorer la situation.

Mme Martine Garnier. L'ANR a mis en place un plan d'action « Égalité 2020-2023 », qui formalise un certain nombre d'engagements. D'après l'analyse réalisée sur la période 2015-2020, dont le titre est *Le genre dans les projets ANR*, les projets sont portés en

grande majorité – 70 % – par des hommes et, en mathématiques et sciences du numérique, le pourcentage de femmes tombe à environ 17 %, ce qui montre à quel point le chemin à parcourir est encore long. En mathématiques et sciences du numérique, les femmes sont vraiment beaucoup moins nombreuses, avec une représentation à moins de 20 %.

Nous avons mis en œuvre plusieurs actions, dont la recherche systématique de parité dans les comités d'évaluation scientifique, la formation des présidents et présidentes de comité. Nous avons aussi introduit le curriculum vitae narratif qui permet de renseigner les interruptions de carrière. Cette année, sur les dix comités d'évaluation opérés par le département « Mathématiques et numérique », cinq sont présidés par des femmes. La parité est donc totale.

M. Philippe Latombe, rapporteur. Je suis preneur des différents éléments chiffrés dont vous disposez car nous aurons une séquence sur la formation et l'égalité. Si vous voulez bien y contribuer en dehors de l'audition d'aujourd'hui, nous en prendrons connaissance avec plaisir.

Mme Martine Garnier. Bien sûr et nous avons à l'ANR une référente « Genre » qui participe notamment aux projets européens *Gender-Net et Gender-SMART*. Elle pourra vous donner des éléments complémentaires.

Je termine sur nos partenariats technologiques avec les États membres avec une coopération très importante qui comporte un volet souveraineté numérique : la coopération franco-allemande. À l'issue du sixième forum de la coopération franco-allemande en recherche en juin 2018, nos deux ministères ont signé une déclaration d'intentions commune dont l'un des objectifs est « la recherche et l'innovation au service de la souveraineté technologique dans un monde numérique ». Dans ce cadre, deux appels bilatéraux ont été lancés par les deux ministères. Ils sont opérés par l'ANR en France, par l'agence VDI/VDE-IT (association des ingénieurs et fédération des industries de l'électrotechnique, de l'électronique et de l'ingénierie de l'information) et par l'agence spatiale DLR (*Deustches Zentrum für Luft- und Raumfahrt*) en Allemagne. Le premier, lancé en 2019, porte sur la cybersécurité et l'autre, en Intelligence artificielle, est piloté par Frédéric Precioso.

L'appel conjoint sur la cybersécurité avait pour thème les technologies protectrices des données personnelles. Huit projets ont été retenus et financés pour un montant de trois millions d'euros pour les participants français. Cet appel réunit, de part et d'autre, une structure académique et une entreprise. Les partenaires sont donc systématiquement un académique et une entreprise français, un académique et une entreprise allemands.

L'appel en intelligence artificielle a lieu au titre de la déclaration d'intentions conjointe sur la création des réseaux de recherche et d'innovation en intelligence artificielle. Il visait à encourager les collaborations de recherche franco-allemandes, notamment dans les domaines applicatifs suivants : les transports et la mobilité, la logistique et les services, l'énergie et en particulier l'énergie renouvelable, l'environnement, les ressources, les technologies d'industrie et de production, la santé, la robotique.

L'appel portait sur deux types de projets. Le premier type est constitué de projets à quatre ans qui unissent deux établissements d'enseignement supérieur et de recherche, l'un en Allemagne et l'autre en France, pour renforcer la collaboration franco-allemande en matière de recherche en IA. Le deuxième type concerne des projets regroupant des partenaires industriels et académiques, français et allemands, pour la recherche et le développement dans des secteurs applicatifs cités précédemment.

Il faut souligner que ce dernier appel a suscité une très forte participation. 152 projets ont été déposés et, sur les 145 propositions éligibles, 21 ont pu être financées pour un montant global de 12 millions d'euros. Nous voyons donc le dynamisme de cette coopération franco-allemande. Une seconde édition de l'appel est en cours de discussion entre les deux ministères.

M. Frédéric Precioso. Il est important de souligner que les chiffres sur l'égalité entre femmes et hommes sont disponibles sur le site de l'INS2I, parce que cet institut s'est emparé de cette problématique, ce qui n'est pas le cas de tous les établissements de recherche en France. J'ai pu me référer à ces chiffres parce qu'ils les affichent et il faut le voir comme un effort louable plutôt que comme une critique.

M. Philippe Latombe, rapporteur. Je ne l'avais pas considéré comme une critique, mais la précision est importante.

Audition, ouverte à la presse, de Mme Raphaëlle Bertholon, secrétaire nationale à l'économie, l'industrie, le logement et le numérique, et de M. Nicolas Blanc, délégué national au numérique, de la confédération française de l'encadrement–confédération générale des cadres (CFE-CGC)

(20 avril 2021)

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. Chacun connaît la confédération française de l'encadrement-confédération générale des cadres (CFE-CGC), syndicat fondé en 1944, représentatif au niveau national interprofessionnel. Nous accueillons Mme Raphaëlle Bertholon, secrétaire nationale, chargée de l'économie, de l'industrie, du logement et du numérique, et M. Nicolas Blanc, délégué national au numérique, de ce syndicat.

Vous vous intéressez au sujet de la souveraineté numérique. Vous nous avez d'ailleurs adressé une contribution écrite au titre de la mission d'information, ce dont nous nous remercions, et à travers vous, les personnes de votre organisation qui y ont contribué.

Nous attendons de cette audition d'aborder, en particulier, les aspects socio-économiques de la souveraineté numérique : les enjeux de formation, de conditions de travail, de féminisation d'un secteur numérique qui reste aujourd'hui largement masculin. Nous sommes heureux de pouvoir vous entendre.

M. Philippe Latombe, rapporteur. À titre liminaire, je souhaiterais soulever trois sujets pour introduire notre échange.

Le premier concerne votre approche de la notion de souveraineté numérique, question véritablement rituelle lors de nos auditions, et qui procède de la grande diversité de définitions qui peuvent exister de ce concept. Comment la définissez-vous ? Quel regard portez-vous sur sa montée en puissance dans le débat public en France et en Europe ? De façon complémentaire, je souhaiterais que vous nous dressiez un état des lieux de nos forces et de nos faiblesses dans ce domaine afin que nous revenions ensemble sur les constats que vous avez posés dans votre contribution.

Le second sujet concerne la formation. Il nous intéresse au premier chef puisqu'il n'existe pas de souveraineté numérique sans compétences. Comment jugez-vous notre capacité à former les salariés à ces savoir-faire parfois très évolutifs ? Selon vous, ces compétences sont-elles suffisamment disponibles dans certaines filières, telles que les télécommunications ?

D'une façon générale, comment percevez-vous la numérisation rapide du travail qui est intervenue pendant la crise sanitaire, avec un recours massif au télétravail, lequel présente des avantages, certes, mais peut être aussi source de difficultés pour certains salariés ?

Enfin, quelles propositions formuleriez-vous au sujet de la souveraineté numérique ?

Afin de mener à bien cette mission d'information, nous avons fait le choix d'adopter une approche pragmatique et opérationnelle. C'est pourquoi il est important pour nous que vous nous indiquiez les points qui vous sembleraient les plus pertinents à traiter afin d'améliorer le cadre existant et de renforcer notre autonomie technologique.

Mme Raphaëlle Bertholon, secrétaire nationale de la CFE-CGC, chargée de l'économie, de l'industrie, du logement et du numérique, CFE-CGC Caisse d'Épargne Rhône Alpes. La CFE-CGC s'intéresse déjà depuis de nombreuses années à l'évolution de la numérisation dans le travail. Elle a d'ailleurs initié plusieurs conférences sur le thème de l'Intelligence artificielle. Nous avons rédigé une charte éthique et numérique « RH » afin d'accompagner les salariés sur l'ensemble des questions, notamment éthiques, liées à l'utilisation de leurs données personnelles. Au mois de juin 2020, nous avons postulé à un projet européen, « SéCoIA Deal : servir la Confiance dans l'Intelligence artificielle par le dialogue », qui a récemment démarré. Nous sommes le chef de file de ce projet, avec plusieurs partenaires syndicaux français, notamment l'U2P, et européens. La CFE-CGC est également partie prenante, aux côtés du Mouvement des entreprises de France (MEDEF), dans un engagement de développement de l'emploi et des compétences (EDEC). Tel est le cadre de nos préoccupations et de nos réflexions sur le thème du numérique.

Notre réflexion nous a conduits à véritablement voir le numérique comme un espace à conquérir et à façonner, un petit peu à l'image de la conquête spatiale. Cela signifie qu'il « embarque » l'ensemble des sujets traditionnels de régulation et de réorganisation territoriale. Il s'avère donc extrêmement important de garantir notre souveraineté numérique, c'est-à-dire d'assurer la pérennité de notre développement économique pour les années à venir. Le numérique représente un moteur indispensable à la croissance future. Ce constat renvoie à l'exigence d'assumer des choix politiques, dans le contexte actuel où nous ne sommes pas en situation de force sur le plan technologique.

M. Nicolas Blanc, délégué national au numérique de la CFE-CGC. Je vous remercie de nous avoir permis de porter nos propositions.

L'idée de conquête de territoire est essentielle. La CFE-CGC se positionne sur la notion d'une défense de nos intérêts, tant nationaux qu'européens, afin de protéger nos compétences, nos entreprises, etc. Il importe de conquérir ce territoire-là parce que, actuellement, d'autres acteurs captent cette valeur et il nous appartient de poser un constat clair de cette captation.

Une étude de BearingPoint, publiée dans « Médias et publicité en ligne », en 2018, a montré que ces nouveaux acteurs modifient et bouleversent les équilibres. À titre d'exemple, l'arrivée de la publicité en ligne a capté un transfert massif des investissements de cette nature. Les acteurs historiques, les producteurs de valeur, qui représentent 80 % des contenus, ne perçoivent plus que 25 % de la valeur de cette publicité en ligne. Un puissant déséquilibre s'est créé. En outre, sur la période comprise entre 2010 et 2017, les investissements dans la presse ont diminué de 50 %.

Le capitalisme de surveillance, qui a été mis en avant par Shoshana Zuboff, révèle une véritable bascule. Le monde qui a suivi les évènements du 11 septembre 2001 a généré une captation sans régulation des données, qui a permis de « profiler », au sens commercial. Cela a conféré à la publicité en ligne un avantage comparatif considérable par rapport à l'existant, aux médias traditionnels et à la publicité classique.

En vingt ans, on a laissé se créer sans régulation d'énormes mastodontes, tels que Google qui, en 2020, représentait 87 % des recherches sur Internet aux États-Unis et 92 % des recherches mondiales. Neuf produits de Google (dont les principaux sont Android, Chrome, Gmail et YouTube) comptabilisent plus d'un milliard d'utilisateurs. Ils ont généré en 2019 cent quatre-vingt-deux milliards de dollars de chiffre d'affaires, soit quarante milliards de bénéfice net, et une valorisation boursière de neuf cent quatre-vingt-treize milliards de dollars. Total, l'entreprise française qui a affiché le plus important bénéfice net en 2019, annonçait dix

milliards de dollars. Amazon représente entre 65 et 70 % du commerce en ligne aux États-Unis et déjà 20 % en France.

Mme Raphaëlle Bertholon. Ce partage de la valeur rebat complètement les cartes à la fois économiques et sociales. Dans le domaine de la construction automobile, l'arrivée des données répartira la valeur entre le constructeur automobile, la plateforme de données, le fournisseur des capteurs, voire l'assureur. Un nouvel écosystème s'est construit sur la base de ces données et il convient de répartir, de manière correcte, la valeur créée. Cette distribution de la valeur représente un véritable enjeu.

S'agissant de l'emploi, autre véritable enjeu, nous nous orientons vers une polarisation des emplois. La confédération française de l'encadrement souhaite que cette tendance génère des emplois hautement qualifiés. Nous vous avons transmis une note relative au constat que nous avons posé sur la filière télécoms qui, selon des données fournies par l'INSEE et la DARES, a perdu en dix ans 25 % de son poids relatif en effectifs salariés. Ce constat s'inscrit dans les faiblesses de nos secteurs d'activité.

M. Nicolas Blanc. La souveraineté numérique constitue un nouveau territoire à conquérir, c'est-à-dire qu'il est essentiel de disposer d'une infrastructure et des outils indispensables à l'occupation de cet espace numérique. Un déséquilibre s'est créé et il nous appartient de le corriger.

Afin d'acquérir cette nouvelle infrastructure et de maîtriser les données, la régulation européenne et la régulation française permettent de réglementer ce monde dans lequel toute donnée devient une valeur marchande alors qu'initialement elle est une propriété.

Il convient également d'assurer la sécurité. Les attaques cyber se multiplient dans l'ensemble de notre pays. Ce nouveau territoire à conquérir comporte des risques. Comme l'a récemment rappelé M. Guillaume Poupard, la virtualisation des réseaux favorise les risques de cyber attaques. Il nous appartient donc de créer, de gérer et d'assurer cette sécurité. L'Europe a proposé une régulation de la 5G dans laquelle il importe que nous nous inscrivions.

Force est de constater que la situation est très complexe. Nous sommes également acteurs dans le domaine de l'Intelligence artificielle, dans lequel l'Europe a initié une régulation qui commence à se décliner. Il convient également de progresser dans les domaines de la 5G, de la *blockchain* et de l'informatique quantique ou calcul quantique.

Le constat éclairé posé par la CFE-CGC montre que la France dispose d'atouts. La compétence des ingénieurs français est reconnue. En atteste d'ailleurs l'installation par Facebook d'un centre de recherche sur l'Intelligence artificielle en France. Nous comptons des entreprises du numérique de taille suffisante pour construire les infrastructures : OVH – qui a tenu un rôle important dans GAIA-X, Athos, Thales, etc. Nous disposons de véritables forces industrielles qui nous permettent de construire cette souveraineté, tant à l'échelle française qu'européenne, si ces constructions peuvent s'assembler avec d'autres entreprises.

Notre patrimoine de données est très riche. Le Health Data Hub contient des données de santé qu'il importerait de valoriser.

Notre épargne et notre écosystème financier sont suffisamment solides pour accompagner le développement de l'économie du numérique. Il conviendrait de la valoriser et de la mobiliser pour cette souveraineté numérique qui nous concerne tous. La CFE-CGC estime qu'il est indispensable de sensibiliser l'ensemble des Français, à tous les niveaux, afin qu'ils comprennent l'importance que revêt cette souveraineté.

Nous accusons également des faiblesses. La souveraineté numérique représente un concept très protéiforme qui intègre différents intérêts d'autonomie stratégique au niveau de l'État. Cependant, au niveau interministériel, force est de constater que les logiques de souveraineté diffèrent et plus encore au niveau européen, car chaque pays développe son propre concept de souveraineté numérique. Nous espérons qu'à l'occasion de sa présidence de l'Union européenne, début 2022, la France se posera en acteur dans ce domaine, mais actuellement, il n'existe aucune vision commune européenne de la souveraineté numérique.

Les décideurs publics ne sont pas suffisamment sensibilisés aux forts enjeux économiques nationaux et collectifs de la perte de souveraineté. La puissance publique doit être exemplaire. Nous ne comprenons pas la posture de la banque publique d'investissement (Bpifrance) face au Health Data Hub, à l'hébergement des prêts garantis par l'État (PGE) par Amazon, etc. La souveraineté numérique impose un équilibre.

S'agissant des télécoms, nous constatons un défaut de soutien efficace au développement dans nos territoires.

Les règles de concurrence ne sont pas très claires, notamment vis-à-vis des États-Unis.

Notre puissance financière est très faible en regard des moyens financiers apportés par l'État américain où la *Defense Advanced Research Projects Agency (DARPA)* est omniprésente. L'Europe s'organise sur l'innovation de rupture, mais nous sommes toujours en rattrapage.

Mme Raphaëlle Bertholon. Forts de ce diagnostic, nous avons formulé un certain nombre de propositions. La première consisterait à sensibiliser les décideurs à ces enjeux par la pédagogie centrée, non seulement sur des conséquences économiques et sociales, que nous avons précédemment mentionnées, de notre perte de souveraineté, mais également sur les évolutions du monde, afin de mieux le comprendre. Par exemple, le fonctionnement des algorithmes modifie considérablement le jeu concurrentiel et il s'avère indispensable de communiquer quant à ces enjeux.

Afin de pallier l'absence de cohérence, il est important également de mettre en œuvre un pilotage et nous proposons de recréer le Commissariat au Plan et de construire un véritable plan de conquête de l'espace numérique et de notre souveraineté numérique, à l'instar de la démarche initiée dans le passé afin d'assurer l'autonomie du pays en matière de techniques d'information (Plan Calcul).

Nous suggérons également de créer un cadre cohérent, avec une régulation adaptée, en organisant un écosystème propice à une mutualisation des technologies, en construisant une infrastructure qui permette de comprendre le fonctionnement des algorithmes, en élaborant une politique de données d'intérêt général efficace qui placera la création de valeur au niveau de l'analyse des données et non plus au niveau de leur détention. Cet enjeu est très important dans les réflexions en cours à Bruxelles relativement aux données extra-financières, à la construction de ce pilier de l'analyse et de la comptabilisation extra-financière, afin d'assurer notre souveraineté. Nous défendons l'idée d'un *European Cloud Act*, sur le modèle du *Small Business Act*, afin de pouvoir assurer et garantir non seulement la protection des données de chaque citoyen, mais également la protection de nos start-up, mais en cohérence avec une épargne drainée qui accompagnerait le développement des entreprises. En effet, les quelques maillons existants méritent d'être renforcés.

Il serait souhaitable de dresser un bilan des mesures de protection déjà mises en place.

Nous suggérons de nous appuyer sur nos atouts, en les gardant à l'esprit, et de nous émanciper d'un environnement technologique qui ne nous est pas favorable, puisque 90 % des données personnelles sont stockées dans un *cloud* étranger. Nous préconisons que nos décideurs publics deviennent les porte-étendards de nouveaux choix assumés qui s'appuieraient sur des entreprises françaises ou européennes et proposeraient des solutions technologiques alternatives aux GAFAM. Il importe de donner de la visibilité à des solutions technologiques numériques françaises. L'exemple de Dassault Systèmes est intéressant parce que, grâce à une acquisition, cette entreprise a créé une plateforme sur laquelle ont été développés plus de la moitié des essais thérapeutiques liés aux vaccins. Nous disposons d'atouts. Il importe de nous appuyer dessus et de les disséminer.

S'agissant de l'épargne, nous avançons une proposition visant à reconstruire une forme de nouveau capitalisme français, mais en drainant l'épargne et en associant la garantie de l'État pour les apports en fonds propres, telle que l'a d'ailleurs proposée le rapport de France Stratégie sur la compétitivité des entreprises.

S'agissant de nos compétences, il nous semble très important de les protéger afin d'éviter que le cas de Nokia ne se renouvelle. Notre compétence existe et il convient de la préserver.

Nous envisageons la formation et l'accompagnement à ces transformations de compétences comme une hybridation. Cela signifie qu'il importe de conserver la compétence de cœur de métier à laquelle s'ajoutera la compétence de la donnée à différents niveaux, entre la culture *data* et un niveau beaucoup plus important.

M. Nicolas Blanc. S'agissant de Nokia, nous constatons une mutation d'un réseau purement télécoms vers un réseau virtuel. Cette évolution requiert de nouvelles compétences dans le *upskilling*, qui consiste pour les ingénieurs déjà en poste à acquérir de nouvelles compétences, et dans le *reskilling*, qui vise à former les nouveaux ingénieurs du futur sur les réseaux 5G totalement virtualisés. Ces compétences nouvelles constituent un véritable enjeu. Le centre de recherche et développement et le centre de cyber sécurité de Nokia sont simultanément impactés. La cyber sécurité s'avère essentielle afin que nous soyons en capacité de « tuiler » ces compétences et, surtout, de les préserver. Des actions ont été initiées dans ce sens, mais le maintien de ces compétences s'avère complexe. Je pense notamment à Qualcomm, une entreprise américaine, qui reprend une partie des capacités. Il convient de prendre conscience qu'à défaut de disposer d'une véritable filière télécoms, nos compétences nous échappent.

S'agissant de la cyber sécurité, Alcide, entreprise française, est en passe d'être rachetée par des capitaux étrangers. Il convient de se donner les capacités de réagir. Le décret Montebourg et ses extensions existent, certes, mais les levées de fonds présentent des risques, car elles ne font pas obligatoirement l'objet de contrôles. Des entreprises nous échappent lors d'importantes levées de fonds. Dataiku est passée sous pavillon américain et elle est dorénavant domiciliée aux États-Unis alors qu'initialement, cette entreprise a été incubée et innovée en France. Dataiku représente malgré tout un échec français.

La souveraineté numérique n'a pas de sens si elle ne s'inscrit pas dans une dimension européenne. Certaines initiatives françaises sont reprises au niveau européen. En matière de données, la France a une influence normative. En effet, la République des données de 2016 a repris la notion de donnée à forte valeur ajoutée dans le *Data Governance Act*. Le constat selon lequel nos propositions pertinentes remontent au niveau européen est donc positif. Le rapport de M. Éric Bothorel contient également des éléments très intéressants. L'Open data France

nous a permis de prendre une avance réglementaire. Certains éléments sont repris dans la norme européenne.

La communication de la Commission européenne *Shaping Europe's Digital Future* constitue malgré tout un cadre européen très complet. Il conviendrait que nous l'intégrions et le déclinions au niveau local. La *Toolbox 5G* de l'Union européenne représente un cadre de réglementation très intéressant qui permettra de disposer d'un réseau sécurisé et d'une norme européenne respectée. Le *cybersecurity package* européen, décliné en 2017-2019, a été étendu avec la *new strategy* cyber européenne. Une logique intéressante s'inscrit également dans la stratégie française cyber avec le développement d'une filière française, l'investissement d'un milliard d'euros et le développement d'une véritable culture cyber dans les entreprises. L'enjeu d'acculturation aux risques cyber est également intéressant.

Sur le plan des compétences, le *Digital Skills and Jobs Coalition* mène une réflexion globale sur les modalités d'acquisition des compétences numériques. Il en existe une déclinaison française, pilotée par le MEDEF, qui se matérialise par « Perspectives IA » qui représente une appropriation générale de l'Intelligence artificielle. En outre, la participation à un engagement de développement de l'emploi et des compétences (EDEC) nous permet d'essayer de structurer la filière de l'Intelligence artificielle en France.

M. Philippe Latombe, rapporteur. Vous avez dressé un constat sur l'état actuel de la situation. Vous avez notamment évoqué Amazon qui représente actuellement au moins 65 % du commerce aux États-Unis, mais uniquement 20 % en France.

Ne pensez-vous pas que cette évolution semble tellement inévitable que s'y opposer serait peine perdue ? Ne serait-il pas préférable d'accompagner cette transformation plutôt que de s'y opposer et de quelle manière pourrions-nous l'accompagner ? À titre d'exemple, la pandémie a montré qu'Uber avait révolutionné non seulement le domaine de la livraison, mais également le monde du travail. La justice a repris la main en requalifiant, dans différents pays, les travailleurs d'Uber comme salariés.

Du point de vue de la centrale syndicale que vous représentez, est-il impératif de combattre cette évolution, d'ériger des murs, ou est-il préférable de l'accompagner ? Comment pouvons-nous la réguler ? Quelles protections pourrions-nous ériger et nous y tenir ?

Mme Raphaëlle Bertholon. Il serait souhaitable de formuler des propositions alternatives, telles qu'une régulation économique. La mise en place d'audits, l'identification de sanctions, l'exigence d'une transparence des algorithmes permettraient d'atteindre au cœur de l'impact du jeu concurrentiel. À titre d'exemple, Uber ne tire aucun bénéfice des taxis. Il existe un jeu de concurrence qui, selon nous, est faussé. Autoriser un audit et obtenir une transparence des algorithmes constitueraient un élément-clé qui permettrait de comprendre le modèle économique, son fonctionnement et la répartition de la richesse. Dès lors, il devient possible de comparer le modèle salarial à celui de type Uber. Uber n'acquitte aucun impôt et n'est pas rentable. Il constitue un prédateur économique.

M. Nicolas Blanc. La part de marché prise par Amazon n'est pas dérangeante, mais l'abus de position dominante l'est. Le problème réside dans le droit de la concurrence. En effet, nous constatons un abus de dépendance économique parce que les entreprises qui occupent sa *market place* sont dépendantes d'une augmentation d'Amazon qui décide de plus ou moins ponctionner les revenus. Il s'agit donc bien d'un abus de dépendance économique. L'abus de position dominante constitue une référence à la souveraineté économique (marché primaire/marché secondaire). Quand Amazon propose l'Amazon premium, il se positionne obligatoirement comme dominant, c'est-à-dire qu'il utilise son pouvoir de marché pour

influencer un autre marché, à savoir celui de la vidéo à la demande (VOD). Seule une régulation permettrait de supprimer ces distorsions de concurrence. À défaut, c'est impossible. La régulation s'impose à nous.

En outre, les aspects liés au code du travail sont très opaques. Nous rencontrons des difficultés à entrer dans ce périmètre afin de le réglementer. La réglementation doit intervenir non seulement au niveau concurrentiel, mais également au niveau du code du travail. Il est essentiel que ces entreprises respectent la réglementation en place.

M. Philippe Latombe, rapporteur. Comment une centrale syndicale approche-t-elle ces évolutions du marché du travail, les opportunités d'emploi, l'accompagnement des publics éloignés du numérique qui, à la suite d'incidents professionnels, sont contraints de retrouver du travail, etc. ? Comment appréhendez-vous la situation actuelle ? Quel type de formation continue pourrions-nous mettre en œuvre ? Comment une centrale syndicale accompagne-t-elle les salariés ? Quels conseils leur prodigue-t-elle ? Comment appréhendez-vous la situation actuelle dans votre participation aux différents organismes de formation professionnelle ?

Mme Raphaëlle Bertholon. J'ai évoqué précédemment la notion d'hybridation. Nous évoluons d'un territoire vers un autre. Les compétences des ingénieurs doivent être préservées, mais il convient de les compléter par hybridation de sorte que leurs compétences initiales puissent s'exercer pleinement dans le territoire numérique. Nos collègues de Nokia et de la métallurgie, dans leur plan de sauvegarde d'activité avaient proposé une initiative intéressante qui consistait à conserver les compétences « cœur de métier » acquises, à procéder à un tuilage de deux ou trois ans, dans le cadre d'un groupement d'intérêt public qui aurait regroupé plusieurs entreprises, et à accompagner la mise en place de la 5G, notamment dans l'industrie, puisque la croissance s'y annonce forte. Ce projet, proposé par la CFE-CGC, n'a malheureusement pas été retenu. Dès lors, ces ingénieurs qui sont des spécialistes de la 5G devront se reconvertir, probablement dans le *big data*, aux frais du contribuable. Ils perdront une partie de leurs compétences, alors que nous proposions une alternative. Nous estimons qu'il est essentiel de garantir cette continuité de passage vers ce nouveau territoire. Il nous semble indispensable de préserver les compétences numériques qui permettent d'évoluer dans les secteurs un peu brouillés de l'espace numérique.

M. Nicolas Blanc. J'ai évoqué la notion d'acculturation qui consiste également à comprendre la réalité. L'arrivée de l'Intelligence artificielle a été abordée comme susceptible de générer potentiellement la disparition de l'emploi, etc. L'impact sur les salariés a été puissant. Dès lors, nous avons initié des cycles sur l'Intelligence artificielle et rédigé une charte éthique et numérique afin de, non seulement nous approprier ces sujets, les comprendre, mais également être capables de les expliquer. Nous nous positionnons dans une logique de transmission et de sensibilisation des salariés, puis d'accompagnement dans les formations.

Nous nous attachons à identifier les impacts sur l'emploi. L'Intelligence artificielle se concentrant sur le travail à faible valeur ajoutée, cela permet de développer de nouvelles compétences que nous accompagnons.

La charte que nous avons mise en place vise également à sensibiliser les directions des ressources humaines (DRH). En effet, il convient d'accompagner non seulement les salariés, mais également les DRH vers les nouvelles gestions prévisionnelles des emplois et des compétences. Nous disposons de modèles plus agiles et nous les accompagnons dans la mise en place d'un numérique au service de tous.

Cette acculturation permet de circonscrire un terrain propice à la formation au numérique et d'éviter que la peur conduise à l'incompréhension des sujets.

Mme Raphaëlle Bertholon. Le numérique ne nous fait pas peur. Nous essayons de le comprendre et nous observons qu'il génère de prodigieux gains de productivité. Notre projet européen vise à identifier ces gains de productivité afin de le poser en véritable moteur de l'accompagnement de la transformation et des compétences. Les nouveaux modèles économiques partagent différemment la valeur ajoutée et ils deviennent ensuite un moteur d'identification de l'ensemble des transformations.

Différents observatoires de métier ont mené des études relatives à l'impact de l'Intelligence artificielle sur les métiers (banque, commerce, télécoms). Les résultats sont parfois surprenants. Les transformations ne sont pas toujours aussi importantes qu'attendu, parce que les compétences « métier » demeurent. Lorsque les impacts sont identifiés, il convient d'harmoniser les aspects économiques, l'accompagnement et le dialogue social.

M. Philippe Latombe, rapporteur. Les entreprises, notamment les TPE-PME, sont-elles suffisamment numérisées ou conscientes de la nécessité qui s'imposera à elles d'entrer dans la numérisation ?

La nécessité absolue d'accompagnement des salariés vers le numérique est-elle bien intégrée dans les entreprises, qu'il s'agisse d'acquérir des compétences en interne ou d'assurer leur éventuelle employabilité future ?

Le numérique ne représente-t-il pas un moyen pour des entreprises de trouver des compétences dont elles ne disposaient pas auparavant et qu'elles ne trouveraient pas obligatoirement sur le marché, du fait du déficit de compétences incluses dans la formation initiale des salariés ?

Mme Raphaëlle Bertholon. La plupart des grandes entreprises sont conscientes des enjeux. S'agissant des petites et moyennes entreprises, nous constatons des chaînes de valeur totalement déséquilibrées. En effet, les donneurs d'ordres exercent un véritable pouvoir sur les PME et les contraignent. À titre d'exemple, General Electric a demandé à l'ensemble de ses sous-traitants de réduire leur facture de 20 %. Cet exemple est représentatif de la réalité économique du tissu des PME. Dès lors, si les PME sont conscientes qu'il est indispensable de progresser vers le numérique, elles n'en ont pas obligatoirement les moyens. Il appartient à l'État d'aborder le sujet en écosystème afin de permettre aux petites entreprises d'en profiter et de ne pas être complètement étouffées. Je rappelle que les PME représentent le plus important pourvoyeur d'emplois en France.

M. Nicolas Blanc. Les PME sont les laissées pour compte de la souveraineté numérique. Il n'existe actuellement aucune logique d'organisation. Les PME s'orientent vers des outils gratuits et elles se numérisent comme elles peuvent.

En revanche, les grands groupes ont pris la mesure de la transformation numérique, de la transformation digitale. La difficulté réside dans le choix entre une numérisation progressive et une bascule radicale vers des modèles plus orientés sur l'Intelligence artificielle. La gestion prévisionnelle des emplois et des compétences (GEPC) n'est pas encore généralisée. Il est complexe de mesurer l'impact sur les emplois et les GPEC sont construites à horizon de deux ou trois ans. Or nous avons besoin d'une plus grande agilité afin d'être très réactifs. Il conviendrait de mesurer l'impact de l'Intelligence artificielle sur chaque emploi et chaque année, ce qui représente également une transformation technologique complexe.

Je suis très critique des écoles de l'Intelligence artificielle de Microsoft. Si le secteur public n'agit pas, le secteur privé agit. Or les certifications de ces écoles de l'Intelligence artificielle sont uniquement des certifications Microsoft. Nous formerons donc des Data

Scientists de Microsoft. L'université de la Sorbonne propose un master Microsoft Learning. Il convient de prendre conscience que Microsoft pénètre tous les niveaux en France, y compris le secteur de la formation. Le logiciel utilisé pour l'école à la maison, Blackboard, est américain et il est hébergé par Amazon Web Services. Ce constat relève de la problématique de souveraineté. Nous sommes acteurs de la mise en place de la formation pour les enjeux numériques.

M. Philippe Latombe, rapporteur. Selon vous, quel est le périmètre du rôle de l'État ? Vous avez évoqué le rachat d'entreprises de haute technologie et des start-up françaises par des Américains. Vous avez également évoqué l'éducation, Blackboard, Microsoft, AWS, etc. Jusqu'où l'État peut-il intervenir ?

Mme Raphaëlle Bertholon. Nous disposons d'une épargne importante, ce qui représente un atout formidable. Cependant, la réglementation bancaire est extrêmement contraignante. Il n'est pas possible de vendre un produit extrêmement risqué à un client qui n'a pas démontré qu'il comprenait et acceptait le risque. Nous pensons que l'État doit pouvoir accompagner en posant sa garantie et ce serait un moyen de drainer cette épargne et de lui donner du sens au service de notre souveraineté numérique. Il conviendrait d'étudier l'ensemble des étapes du financement des entreprises afin d'identifier des possibilités d'action. Le rôle de l'État consiste à assurer une cohérence globale et à faire en sorte que nous disposions de tous les outils à tous les niveaux, *via* Bpifrance. Cet exemple pourrait être dupliqué.

M. Nicolas Blanc. Nous considérons qu'il appartient à l'État de protéger les compétences. L'exemple de Nokia montre que cette perte de compétence en matière de recherche et développement en 5G et de cyber sécurité est malgré tout très frustrante, alors que la cyber sécurité devient un enjeu de société majeur. Nokia affiche la volonté de créer un centre de cyber sécurité, mais il n'a pas communiqué d'échéance.

Il revient également à l'État d'harmoniser les secteurs, d'agir dans une logique intégrée. Nous disposons de compétences éparses, mais d'aucune véritable filière 5G.

En outre, la situation actuelle est susceptible de générer de nouveaux plans sociaux chez Nokia, qui progresse dans toute l'Europe et qui fonctionne selon une logique mondiale, dépassant notre souveraineté nationale.

La force de l'État réside dans sa capacité à gérer les compétences au niveau national et au niveau local. La consolidation des résultats de l'EDEC par filière et par secteur nous permettra d'obtenir une vision complète de la situation. En effet, il s'avère complexe pour les entreprises de se projeter à cinq ou dix ans en matière de nouvelles compétences liées à l'Intelligence artificielle ou pour ce qui concerne les besoins qui seront les leurs à l'arrivée de jeunes salariés. Il convient donc de trouver cet équilibre entre le travail initial de prospective, mené par les organisations syndicales et patronales dans l'EDEC, et les propositions de formations aux nouvelles compétences.

Mme Raphaëlle Bertholon. Il appartient à l'État d'édicter une feuille de route et d'assurer la cohérence d'un ensemble qui se présente actuellement en « silos » afin de gagner en efficacité.

M. Philippe Latombe, rapporteur. Pensez-vous que l'État se structure autour du numérique ou bien estimez-vous qu'il fait preuve d'une trop grande dispersion ?

Sur quelles trajectoires jugeriez-vous souhaitable d'agréger l'ensemble de l'État ?

Mme Raphaëlle Bertholon. Certaines actions ont été initiées, mais nous n'avons pas le sentiment qu'il existe une véritable feuille de route qui coordonne l'ensemble. Nombreux sont ceux qui s'émeuvent que nos données de santé soient hébergées par Microsoft *via* le Health Data Hub ou Doctolib. Pour autant, le droit ne s'y oppose pas. L'évolution de cette situation relève d'un choix politique complexe qui mérite des explications. Ce choix n'ayant pas été véritablement affirmé, la commission nationale de l'informatique et des libertés (CNIL) et le Conseil d'État ont pris position, puis la caisse nationale de l'assurance maladie (CNAM) a finalement refusé de transmettre les données de santé pour un hébergement par Microsoft. Force est donc de constater que nous ne disposons d'aucune vision claire et assumée. L'état des lieux est ce qu'il est et il convient de l'assumer.

M. Nicolas Blanc. S'agissant de l'Intelligence artificielle ou de la cyber sécurité, les logiques européennes ont évolué, en regard des importants enjeux liés à la souveraineté. La France intègre ces logiques, en cohérence avec le cadre européen, et ce constat est positif pour nos partenaires. L'*open data* s'inscrit vraiment dans le *Data Governance Act*. Nous investissons dans l'interopérabilité et la cyber sécurité et nous construisons progressivement une véritable doctrine. Néanmoins, l'urgence ne peut pas constituer une priorité absolue et il importe de tenir compte des enjeux de souveraineté et de proposer une solution à décliner selon un calendrier déterminé. Il est incompréhensible que l'État, *via* Bpifrance, et sous couvert d'accélérateur numérique, propose à des PME d'héberger leurs données sur Amazon Web Services et qu'elles se retrouvent finalement sur la *market place* d'Amazon.

Il est regrettable que, d'une part, nous construisions une véritable doctrine cohérente, la notion de souveraineté numérique étant prégnante et la puissance publique s'engageant dans cette dimension, avec une volonté de sensibilisation et d'investissements à tous les niveaux, et que, d'autre part, nous encouragions le Health Data Hub. C'est choquant.

M. Philippe Latombe, rapporteur. Les outils législatifs résultent de choix sociaux, culturels, historiques, etc. Vous avez évoqué les acteurs américains du numérique, mais il existe également des acteurs dans d'autres pays, tels que la Chine, qui proposent des approches différentes. Que proposez-vous afin d'harmoniser ces approches ? Est-il souhaitable d'harmoniser l'ensemble de ces visions ou bien est-il préférable que nous tracions notre propre voie ? Quelles modalités de régulation suggèreriez-vous ? Les projets vous semblent-ils suffisants ? Selon vous, quelle serait la meilleure échelle ?

Mme Raphaëlle Bertholon. Il convient de cesser de nourrir des illusions. Il ne sera pas possible de construire une régulation impliquant les deux blocs que vous avez évoqués, la Chine et les États-Unis. La meilleure échelle serait européenne.

Trois textes permettent une forme de régulation : le *Data Governance Act*, le *Digital Services Act* et le *Digital Markets Act*. Le *Digital Governance Act* est assimilable, pour l'économie, au Règlement général sur la protection des données (RGPD) applicable à la vie privée. Il devrait permettre d'établir une véritable économie de la donnée. Ensuite, il conviendrait de pouvoir accéder aux algorithmes et de construire une autorité de régulation intermédiaire entre l'autorité de la régulation de la concurrence et la CNIL. Le travail d'une telle autorité permettrait de comprendre l'ensemble des effets des algorithmes, notamment sur le jeu concurrentiel, le nerf de la guerre.

S'agissant des données, il convient de mener une politique d'*open data* correctement ciblée qui permette de déplacer le niveau de création de valeur de la détention de la donnée, puisque les données sont alors ouvertes, vers l'analyse de la donnée. Cela constituerait un moyen pour les Européens de combler leur retard.

M. Nicolas Blanc. Il importe que nous nous inscrivions dans un cadre de régulation au niveau européen, car cela permettrait d'établir un véritable rapport de force. La déclinaison de la réglementation actuelle est complexe à opérer au niveau local. Toutefois, dans son rapport, M. Éric Bothorel s'inscrit au-delà de ce qui est proposé par le *Data Governance Act* pour l'Europe. La France est en avance sur certains points et elle dispose d'une force normative. À titre d'exemple, la loi pour une République numérique, promulguée en 2016, s'est avérée pertinente et elle est devenue normative au niveau européen. Bien qu'il fasse l'objet de nombreuses critiques, le projet GAIA-X, initié par l'Europe, propose une alternative vraiment intéressante, une troisième voie européenne. L'Europe propose des services et met en place un cahier des charges exigeant, notamment dans le domaine du stockage des données, dans la logique du *cloud* de confiance que nous avons essayé de mettre en place en France. La France a un rôle à jouer au niveau européen pour influencer les doctrines.

M. Philippe Latombe, rapporteur. Cela signifie-t-il que nous devions mettre des valeurs dans cette fameuse troisième voie européenne ? Trouverons-nous cette troisième voie grâce à la transcription des valeurs européennes dans le cadre réglementaire et législatif ? Vous avez évoqué l'exemple de la donnée. En ce qui concerne les valeurs, nous n'avons pas la même conception que les Américains qui considèrent que la donnée appartient à celui qui l'a collectée. À l'inverse, les Chinois estiment que la donnée appartient à l'État. L'Europe pose que la donnée appartient soit à la personne et non pas à celui qui l'a collectée, soit à un collectif, c'est-à-dire à celui qui l'a collectée mais de manière à l'intégrer à un ensemble qui sera exploité dans l'intérêt général.

Au-delà de la donnée, ces exemples peuvent-ils être déclinés sur d'autres sujets du numérique tels que l'Intelligence artificielle, le quantique, les réseaux sociaux, etc. ? Est-ce la bonne voie ?

Mme Raphaëlle Bertholon. C'est clairement la bonne voie. En ce qui concerne la donnée, le RGPD a posé les bases en reconnaissant la propriété de la personne. Ce postulat nous différencie du modèle chinois, basé sur le crédit social et donc l'appartenance des données à l'État, ou du modèle américain dans lequel la donnée appartient à son collecteur.

Notre organisation syndicale CFE-CGC est convaincue du pouvoir du collectif de la donnée. Ce thème constitue l'orientation à long terme des réflexions de notre syndicat. C'est pourquoi nous réfléchissons à cette valeur économique et à cette redistribution, au partage des richesses.

M. Philippe Latombe, rapporteur. Discutez-vous de ce positionnement de la CFE-CGC avec les autres centrales syndicales françaises et européennes ? Quelle est la position de vos homologues des autres centrales ?

Mme Raphaëlle Bertholon. Nous échangeons avec nos homologues des autres centrales syndicales. Cependant, s'agissant de la donnée, nous affichons notre spécificité parce que nous nous y sommes intéressés très tôt. Nous avons élaboré un projet avec nos homologues syndicaux, y compris européens. Nous sommes également partenaires de la chaire « Gouverner l'organisation du numérique » à Nanterre où nous sommes aux côtés de l'Union générale des ingénieurs, cadres et techniciens CGT (UGICT). Néanmoins chaque organisation syndicale a une perception un peu différente du numérique.

M. Nicolas Blanc. Le Conseil économique, social et environnemental (CESE) a organisé des discussions, notamment sur l'Intelligence artificielle.

Il existe une différence de maturité entre nous. À travers notre charte éthique et numérique, nous souhaitons impacter la notion de valeurs. Le RGPD a vraiment ouvert la troisième voie et il est devenu un avantage concurrentiel. Certaines entreprises mettent le RGPD en avant. La troisième voie existe et il faut poursuivre dans cette direction pour l'Intelligence artificielle, une Intelligence artificielle de confiance, parce que cela a du sens. La confiance est essentielle et c'est pourquoi nous souhaitons accompagner ces grandes mutations au sein des entreprises et les expliquer aux salariés. À titre d'exemple, la confiance constitue la base du télétravail.

Telles sont les valeurs que nous souhaitons mettre en œuvre. Dans tous les domaines, la troisième voie permettra, par la régulation, de circonscrire un cadre dans lequel se développera une confiance régulatoire afin de progresser.

M. Philippe Latombe, rapporteur. La pandémie a mis en exergue les difficultés à fonctionner, rencontrées par certaines entreprises ou administrations. Le télétravail a été mis en œuvre dans l'urgence pour pallier ces difficultés. Quelles conséquences en tirez-vous, bien que la pandémie ne soit pas terminée ? Quelle est votre vision de l'avenir relativement au travail *via* le numérique ? Dans une entreprise normale, comment fonctionnent le télétravail, le distanciel, le management ? Qu'attendez-vous des pouvoirs publics à ce sujet ?

Mme Raphaëlle Bertholon. La CFE-CGC considère que le télétravail, tel qu'il a été mis en place à l'occasion de la pandémie, constitue un télétravail contraint. À titre d'exemple, dans mon entreprise, nous n'avons pas appliqué l'accord relatif au télétravail, mais le plan de continuité d'activité, c'est-à-dire la poursuite de l'activité à domicile. Cette distinction est importante, car le télétravail n'a pas été déployé, lors de la pandémie, dans les conditions dans lesquelles la CFE-CGC souhaite qu'il s'applique. En effet, nous estimons que, pour rester efficace, le télétravail peut être autorisé pour deux jours par semaine, ainsi que le démontrent la plupart des études menées à ce sujet. Nous ne sommes pas favorables à un télétravail à temps plein, parce que nous considérons que le présentiel est important.

Des défaillances majeures ont été enregistrées. Je me souviens notamment de la fameuse fusée américaine qui a explosé et la recherche des causes a montré que l'accident avait trouvé son origine lors d'une réunion tenue en conférence téléphonique au cours de laquelle, malheureusement, les intervenants n'avaient pas identifié l'ensemble des signaux faibles. Cet évènement démontre toute l'importance d'une présence physique aux réunions au cours de laquelle des échanges sont initiés.

Pour ce qui concerne l'avenir, je pense que seront mis en œuvre des modes de travail que nous qualifierons d'« hybrides ». En effet, un total retour en arrière n'est pas envisageable et un certain nombre de réunions se dérouleront à distance afin d'éviter les déplacements. Il serait néanmoins essentiel de préserver le présentiel.

M. Nicolas Blanc. La mise en place du télétravail a été laborieuse, car elle s'est déroulée sur la base de préconisations. Les choix n'ont pas été très clairs alors que dans certaines régions, telles que la région parisienne, l'intérêt sanitaire aurait pu conduire à imposer le télétravail.

Toutefois, le télétravail produit un impact à long terme : perte du collectif, isolement, etc. La difficulté réside dans la gestion du télétravail dans la durée. En outre, la représentation syndicale est complexifiée par la perte du collectif.

Enfin, des négociations d'accords étaient en cours et nous pouvions supposer que les employeurs avaient pris conscience d'un certain nombre de points. Pourtant, le ticket

restaurant a dû faire l'objet de jurisprudences afin de déterminer les droits de chacun. Le télétravail est basé sur la confiance, mais il demeure essentiel que le salarié soit autorisé à discuter sereinement de son accompagnement.

Le télétravail comporte des aspects ergonomiques et de conditions de travail. Il est important de le mettre en œuvre dans de bonnes conditions, sachant que nous venons de subir les pires modalités du télétravail. Le télétravail nécessite non seulement un accompagnement dans la durée, mais également un accompagnement financier, qui doit être négocié et faire l'objet d'un accord. Nous sommes au cœur des discussions et nous constatons une certaine frilosité.

Quoi qu'il en soit, le télétravail se développera, y compris pour des emplois jugés initialement non télétravaillables. Finalement, avec de l'agilité, le télétravail a été ouvert à de nombreux emplois. Il convient dorénavant de lui construire un nouveau cadre plus réglementaire.

M. Philippe Latombe, rapporteur. Lors du premier confinement, le télétravail était obligatoire. Lors du deuxième confinement, le nombre de télétravailleurs a diminué. Cela signifie que certaines entreprises avaient demandé à leurs salariés de travailler en présentiel. Le gouvernement a imposé un télétravail obligatoire, dès lors qu'il s'avérait possible, lors du troisième confinement. Le télétravail a-t-il un avenir ou bien, culturellement, la France y serait-elle un peu réfractaire ?

Au-delà des problématiques d'accords, les entreprises sont-elles prêtes pour le télétravail ?

M. Nicolas Blanc. La mutation avait débuté avant la crise sanitaire. Il existe désormais non seulement une véritable culture du télétravail, mais également une réelle demande. Nous avons passé un cap.

Cependant, le cadre demeure très important. Un accord relatif au télétravail permet de limiter le nombre de jours de télétravail. Les réflexions doivent être menées en bonne intelligence afin de fixer un cadre dans lequel chacun établira ensuite un auto-diagnostic et choisira autant que faire se peut son fonctionnement.

Mme Raphaëlle Bertholon. Le nécessité du présentiel s'est également exprimée. La pandémie nous a surpris et a conduit les entreprises à organiser des plans de continuité d'activité. La banque, par exemple, a été considérée comme une organisation d'importance vitale (OIV) parce qu'il était important d'assurer une présence sur les sites. Ce choix s'est révélé salutaire pour les salariés, parce que certains ne parvenaient plus à déconnecter. L'être humain ressent le besoin quasiment physique d'entretenir des interactions sociales qui n'existent malheureusement pas *via* la vidéo et qui, malgré tout, représentent un gage d'efficacité.

M. Nicolas Blanc. Le télétravail a été rendu possible par les outils utilisés dans les entreprises et force est de constater que l'omniprésence de Microsoft a permis le déploiement de Teams qui s'est développé de façon spectaculaire.

Cependant, la situation nous a rendus encore plus dépendants à l'égard de ces outils. Il conviendrait que nous soyons capables de développer des alternatives. Actuellement, l'écosystème Microsoft est mis en place dans les grandes entreprises et il fournit l'ensemble des outils. Certes, c'est très fluide. Teams permet de créer sa gestion de projet, Outlook gère

les boîtes e-mail, etc. Nous sommes accompagnés dans cette logique, mais notre dépendance est considérable.

M. Philippe Latombe, rapporteur. Souhaitez-vous que nous traitions d'autres sujets que nous n'avons pas encore soulevés ?

Mme Raphaëlle Bertholon. Je souhaiterais aborder la féminisation des métiers à laquelle nous sommes d'autant plus attentifs qu'elle a régressé dans les métiers du numérique. Les femmes étaient plus nombreuses dans le passé dans ces métiers. Il est important de retrouver cet équilibre. Un univers uniquement masculin ne porte pas le même regard et cela impactera l'Intelligence artificielle. L'équilibre contribuera à sensibiliser aux enjeux du numérique. Le secteur du numérique n'enferme pas. Au contraire, il ouvre de nombreuses opportunités. Il convient de développer une pédagogie qui attirera le public féminin vers ces métiers du numérique dans son ensemble.

M. Nicolas Blanc. Je souhaiterais mettre en avant l'écosystème *open source* en France. L'*open source* a été identifié comme une véritable stratégie de souveraineté. Le conseil national du logiciel libre (CNLL), union des entreprises du logiciel libre et du numérique ouvert, est l'organisation représentative en France des entreprises de la filière *open source*. Il regroupe près de trois cents entreprises structurantes du domaine de l'*open source* et il importe de le valoriser. Ces entreprises sont également membres de l'association professionnelle européenne du logiciel libre (APELL). L'écosystème se structure et il importe de le souligner.

En France, certaines initiatives sont intéressantes. L'initiative « Libre », notamment, a mis en place une agrégation d'outils *open source* qui constituent une alternative intéressante aux GAFAM.

Il me semble essentiel de sensibiliser les grandes entreprises à notre dépendance aux grands outils, aux grands éditeurs, en priorité américains. J'espère que le dossier de GAIA-X génèrera une nouvelle confiance et conduira les entreprises à évoluer.

La souveraineté est l'affaire de tous.

Mme Raphaëlle Bertholon. Notre réflexion a progressé et nous avons enrichi la note que nous vous avions transmise. Nous vous transmettrons une note actualisée.

M. Philippe Latombe, rapporteur. Je vous remercie beaucoup pour ce temps que nous avons partagé. Il était important pour nous de connaître les réflexions de la CFE/CGC sur ce sujet.

Audition, ouverte à la presse, de M. Rémy Ozcan, président de la fédération française des professionnels de la *blockchain* (FFPB)
(22 avril 2021)

Présidence de M. Philippe Latombe, rapporteur.

M. Philippe Latombe, président et rapporteur. M. Rémy Ozcan, vous avez créé, en 2020, en tant que spécialiste de la technologie *blockchain* et cofondateur de Crypt4All, la fédération française des professionnels de la *blockchain* (FFPB) avec M. Jean-Michel Mis, député de la Loire et rapporteur, au même titre que Mme Laure de la Raudière, d'une mission d'information sur les usages des bloc-chaînes (ou *blockchains*) et autres technologies de certification de registres.

La FFPB rassemble les acteurs de l'écosystème français de la *blockchain* sous un seul et même étendard, autour de trois mots d'ordre : fédérer, professionnaliser et structurer. Ses membres appartiennent aussi bien au monde de l'entreprise qu'à celui de la formation ou encore de la recherche.

Nous nous réjouissons d'échanger avec vous sur l'état de l'écosystème de la *blockchain* en France et les moyens pour cette technologie de participer à la construction d'une souveraineté numérique nationale et européenne.

Je commencerai par ma question rituelle. Elle portera sur votre conception de la souveraineté numérique, dont existe une grande diversité de définitions. Comment approchez-vous personnellement cette notion ? En quoi pourrait-elle constituer un levier de souveraineté pour la France et l'Europe ? Je souhaiterais à ce propos que vous nous rappeliez brièvement les principes de la technologie *blockchain*, ses cas d'usage et son niveau de maturité.

Nous traiterons ensuite du développement en France d'un écosystème *blockchain* performant, notamment grâce à votre organisation, dont la mission consiste à fédérer et professionnaliser ce secteur en cours de construction. Comment jugez-vous l'action des pouvoirs publics dans ce domaine, alors même que le gouvernement a pris l'initiative, avec les acteurs de votre secteur, d'une stratégie nationale *blockchain* ? Comment, d'ailleurs, avance cette stratégie ? Qu'en attendez-vous ? Nous accueillerons volontiers toute proposition d'amélioration du cadre réglementaire en place.

Enfin, je souhaite aborder la dimension européenne de la *blockchain*. Comment la France se positionne-t-elle dans ce domaine par rapport à ses voisins européens ? Que pensez-vous de l'action de l'Union Européenne ? Nous en profiterons pour évoquer l'enjeu juridique de la force probante de la *blockchain*.

M. Rémy Ozcan, président de la fédération française des professionnels de la *blockchain* (FFPB). Je tenais tout d'abord, M. le député, à vous remercier d'avoir instauré une mission d'information sur ce sujet d'une importance cruciale pour l'avenir de notre pays.

La FFPB vise à structurer et professionnaliser l'écosystème français de la *blockchain*, trop fragmenté jusqu'alors. Consciente que son utilisation dépasse largement la sphère des cryptoactifs, notre fédération a adopté une approche plurisectorielle afin de permettre à toute entreprise, quel que soit son secteur d'activité, d'identifier des cas d'usage concrets de la *blockchain*, pour en tirer parti.

Malgré sa récente création en juillet 2020, notre fédération regroupe déjà un grand nombre d'entreprises œuvrant dans plus d'une dizaine de secteurs, dont l'énergie, les télécommunications, l'économie circulaire, l'assurance et le luxe – preuve de la diversité des cas d'usage de la *blockchain*. La présence, parmi les membres de la FFPB, de grandes entreprises, telles qu'EDF, Orange ou Suez, intéressées par cette nouvelle technologie, atteste le dynamisme de notre industrie. Il me semble important d'en identifier les forces et les faiblesses pour proposer des recommandations à même d'accompagner son évolution, en lui assurant le soutien des pouvoirs publics.

L'usage de la *blockchain* concerne de nombreuses questions, dont celle de la valeur juridique en tant que preuve des informations inscrites dans un registre de *blockchain*, ou encore celle de la souveraineté numérique. Avant de saisir les spécificités de cette technologie, il apparaît indispensable d'en comprendre la nature, les cas d'usage, et en quoi elle nous offre une formidable opportunité de nous réapproprier notre souveraineté dans l'espace numérique, l'un de ceux où la souveraineté de notre nation doit justement le plus se manifester.

La technologie *blockchain* correspond à ce que l'on qualifie d'Internet de la valeur. Elle permet d'échanger des actifs d'un usager à un autre, comme Internet permet de transmettre des informations de pair à pair, indépendamment de la localisation géographique de chacun, sans passer par un intermédiaire de confiance. La *blockchain* autorise une forme de collaboration horizontale, *via* le partage d'informations en toute sécurité, sans que leur intégrité puisse être remise en cause. Bien que le degré de maturité de cette technologie rende dès aujourd'hui possible son utilisation massive, elle continuera de se développer jusqu'à ce qu'elle puisse se déployer à l'échelle mondiale en 2022. En somme, la *blockchain*, loin d'être encore contestée, fait aujourd'hui figure d'évidence dans un certain nombre de secteurs, comme nous le rappelle d'ailleurs régulièrement l'actualité.

Par rapport à d'autres technologies existantes, la *blockchain* présente l'avantage de garantir l'intégrité des données et des informations inscrites dans son registre, du fait de ses composantes intrinsèques : la cryptographie, la signature électronique, la distribution du registre et la décentralisation des validations. La Russie et Israël utilisent essentiellement la *blockchain* à des fins de cybersécurité.

La seule question qui se pose encore porte donc sur l'usage réservé à la *blockchain*. Dans quel objectif les entreprises et les pouvoirs publics français s'en saisiront-ils ? Certains pays y recourent par souci de traçabilité, d'autres, comme l'Australie ou les États-Unis, dans le secteur financier. La *blockchain* apparaît en tout cas comme le moyen le plus rapide, fiable et sécurisé de transférer des actifs ou des données partout dans le monde.

Il me semble essentiel de situer la discussion dans son contexte géopolitique. Depuis l'avènement d'Internet et l'émergence de technologies disruptives, les principales luttes d'influence politique et économique se déroulent dans l'espace numérique, largement dominé par les États-Unis et la Chine. En tant que technologie d'infrastructure, la *blockchain* offre une formidable opportunité de redistribuer les cartes en réaffirmant la souveraineté de notre nation à travers celle de l'Union européenne.

Nous reviendrons sans doute sur la façon concrète dont la *blockchain* permet aux entreprises et aux pouvoirs publics de récupérer cette souveraineté érodée au fil des ans, au fur et à mesure des virages technologiques que nous avons manqués, tels celui d'Internet ou du *cloud*.

Mon optimisme foncier me convainc que nos faillites passées ne nous condamnent pas forcément à un nouvel échec à l'approche du virage de la *blockchain*. Malgré la rapide

mobilisation des pouvoirs publics autour de cette nouvelle technologie, notre écosystème doit encore évoluer, si nous voulons qu'il atteigne son apogée.

J'aimerais évoquer les constats effectués par la FFPB. Nous avons tout d'abord procédé à un état des lieux de l'écosystème de la *blockchain* afin d'en identifier les forces et les faiblesses. Les conclusions de notre enquête nationale, close en octobre 2019, ont été remises au secrétaire d'État au numérique, M. Cédric O, qui a bien voulu assister à notre première réunion publique, le 29 octobre dernier, dans les locaux de l'Association française de normalisation (AFNOR), partenaire stratégique de la FFPB.

Cette enquête a d'abord mis en évidence l'intérêt prononcé des grands groupes pour la *blockchain*. Plus de 55 % des sociétés dont la cote entre dans le calcul de l'indice SBF 120 mènent en ce moment même des projets impliquant cette technologie. Récemment, le groupe LVMH a décidé d'y recourir, après trois années d'expérimentation.

Notre enquête a en outre révélé la commercialisation en bonne voie d'un nombre considérable de produits et de services mobilisant la technologie *blockchain*. Plus de 69 % des acteurs de l'écosystème français de la *blockchain* ont déjà développé des solutions commercialisables. Le chiffre d'affaires de près de la moitié d'entre eux dépasse les 500 000 euros.

Le marché de la *blockchain* se présente essentiellement comme un marché interentreprises (ou *B to B*). La plupart des sociétés, quand elles répondent par exemple à un appel d'offres, en sollicitent d'autres pour acquérir auprès d'elles des solutions. 90 % des sociétés de notre industrie proposent des services ou des produits à d'autres entreprises. Plus de 60 % de petites et moyennes entreprises (PME) fortes d'une remarquable expertise dans la technologie *blockchain* ont conclu, avec de grands groupes, un partenariat qui relève pour elles d'une impérieuse nécessité.

Les investisseurs manifestent un intérêt indéniable pour la *blockchain*. Plus de 53 millions d'euros, en montants cumulés, ont été, entre 2017 et 2019, investis dans les sociétés de notre industrie, en dehors de Ledger qui a collecté, à elle seule, plus de 69 millions d'euros. Entre 2017 et 2019, les investissements dans ce secteur, aux États-Unis, sont passés de 850 millions à plus de 4,5 milliards de dollars. Une telle croissance spectaculaire se poursuit à l'heure où la pandémie prouve, plus que jamais, la nécessite d'accélérer la numérisation de notre économie.

La France doit augmenter ses capacités d'investissement pour soutenir le développement des entreprises de la *blockchain*. Nous aurions pu penser que le contexte difficile inciterait celles-ci au pessimisme. Au contraire, 90 % d'entre elles jugent favorables leurs perspectives de développement, qu'elles souhaitent poursuivre en France à court terme. Deux tiers ont déclaré vouloir engager des experts de la technologie *blockchain*, d'où le besoin d'étendre les offres de formation, afin de niveler par le haut les compétences des futures recrues.

66 % des acteurs de la *blockchain* se sont déclarés favorables à une volonté de privilégier des *blockchains* françaises, c'est-à-dire à l'architecture mise au point en France, par une entreprise siégeant en France, grâce à des financements français.

En conclusion, la France dispose d'un écosystème *blockchain* hétérogène et dynamique, en bien meilleure santé que d'autres secteurs rudement éprouvés par la pandémie. C'est aujourd'hui même qu'il faut soutenir les entreprises françaises du secteur et non dans quelques années, quand des puissances étrangères auront investi le marché. Comprenons bien

qu'il ne s'agit pas d'un simple marché de niche comme d'aucuns ont pu le croire. Il représentera en effet plus de 25 milliards de dollars en 2025, selon les prévisions du Forum économique mondial en 2018. L'accélération de la numérisation de l'économie due à la pandémie invite d'ailleurs à revoir ce chiffre à la hausse.

Un immense marché s'étend devant nous. Nombre d'entreprises se mobilisent déjà pour saisir les opportunités liées à la *blockchain*.

Je voudrais attirer votre attention sur un point fondamental qu'il convient de garder à l'esprit. La technologie *blockchain* permet de proposer, depuis n'importe quel pays, des produits et des services liés à la traçabilité de produits alimentaires et pharmaceutiques, la certification documentaire, l'échange d'actifs, la numérisation d'œuvres d'art ou encore la création, l'émission et l'échange de cryptoactifs. Nous devons répondre à une question simple, quoique fondamentale pour l'avenir de notre industrie en France : pourquoi une entreprise désireuse de proposer des produits et des services basés sur la technologie *blockchain* s'établirait-elle en France plutôt qu'ailleurs ? Comment donner aux sociétés l'envie de choisir la France ?

M. Philippe Latombe, rapporteur. Pourriez-vous revenir brièvement sur le principe de fonctionnement de la *blockchain* et ses usages pratiques, pour éviter de la réduire aux cryptoactifs auxquels certains l'assimilent à tort ? Quelques exemples d'utilisation concrète permettraient à ceux qui nous écoutent de mieux comprendre en quoi elle peut constituer un outil de souveraineté numérique.

M. Rémy Ozcan. Une bonne part des utilisateurs quotidiens d'Internet ne comprend pas son fonctionnement. Mieux vaudrait donc se demander, face à une nouvelle technologie comme la *blockchain*, ce qu'elle peut apporter.

D'abord, elle garantit la traçabilité de produits de manière à lutter contre la fraude. Une *blockchain* attribue à chaque produit une empreinte numérique unique, inscrite dans le registre partagé par tous les membres validateurs du réseau, lequel sollicitera la totalité du registre à chaque inscription d'une nouvelle information. Le stockage des données réparties aux quatre coins du monde rend quasiment impossible l'identification d'un dépositaire du registre original et, partant, l'interception ou la modification des informations qu'il contient. La *blockchain* apparaît dès lors comme un gage de certification dans des secteurs aussi divers que l'agroalimentaire ou le luxe. L'inscription de données dans le registre d'une *blockchain* les rend non seulement immuables mais surtout consultables par tous ceux qui disposent d'un accès à ce registre. L'usage de la *blockchain* a été envisagé pour certifier des diplômes ou encore des factures d'électricité afin de lutter contre la recrudescence de documents frauduleux.

Dans le secteur de l'énergie, la *blockchain* permet aussi d'automatiser une redistribution de l'électricité plus efficiente dans un quartier donné. Elle autorise en outre la création et l'échange rapide et simple de valeurs sans nécessité de passer par un tiers de confiance. Dans une perspective de souveraineté, elle facilite enfin le stockage de données par leur répartition.

Le récent incendie d'OVH a mis en évidence l'extrême centralisation des données. Qu'elle soit le fait de Google, Amazon, Facebook, Apple ou Microsoft (les GAFAM) ou d'entreprises européennes, le moindre problème dans leur stockage rejaillit dans ces conditions sur l'ensemble des utilisateurs. La *blockchain* distribue au contraire l'enregistrement des données en les chiffrant pour les sécuriser. Autrement dit, chacun peut contribuer à leur stockage en leur réservant de la mémoire sur un appareil électronique. Une

fois découpés, les fichiers se répartissent entre les usagers. Le recours à la cryptographie ôte toute valeur à leurs fragments, pris indépendamment les uns des autres. En réalité, la *blockchain* agrège plusieurs technologies préexistantes, à l'instar de la cryptographie, d'Internet ou de la signature électronique. Ce n'est pas un hasard si notaires et huissiers, en tant que tiers de confiance, souhaitent l'utiliser pour automatiser leur travail et gagner en efficacité.

Dans la pandémie, certains assureurs n'ont étonnamment pas voulu indemniser une part des entreprises contraintes de déposer le bilan. La mise en place de contrats intelligents *via* une *blockchain* aurait pu donner lieu à une indemnisation automatisée des assurés sans que nul ne puisse remettre en cause la validité de leurs contrats.

En résumé, la *blockchain*, en plus de garantir l'intégrité de données, permet d'automatiser des tâches et d'échanger de la valeur dans n'importe quel secteur d'activité. Grâce à la *blockchain*, des entreprises se financent par des émissions d'actifs numériques (*Initial coin offering* ou *ICO*), désormais encadrées par la réglementation française. Ces *ICO* offrent aux PME une formidable opportunité de numériser leurs actions, dont l'échange, dès lors plus simple et rapide, répond au problème fréquent de liquidité des titres financiers non cotés.

M. Philippe Latombe, rapporteur. Revenons à la traçabilité des informations inscrites dans une *blockchain* et à l'utilisation de cette technologie par les notaires et les huissiers. Comment la *blockchain* s'inscrit-elle aujourd'hui dans notre droit ? Je songe bien sûr à l'enjeu de la force probante. Où nous situons-nous en France par rapport à d'autres pays ?

M. Rémy Ozcan. Une ordonnance d'avril 2016 a réglementé pour la première fois cette technologie en lui donnant d'ailleurs une ébauche de définition légale. Cette ordonnance a reconnu la force probante des transactions de minibons, c'est-à-dire de titres financiers non cotés, effectuées *via* un dispositif électronique d'enregistrement partagé : en l'occurrence, une *blockchain*.

Ensuite, la loi relative à la croissance et la transformation des entreprises (dite loi Pacte) a fourni un cadre légal à l'usage de la *blockchain* en matière de financement, via les *ICO*. Cette loi garantit une relative sécurité juridique aux investisseurs comme aux entreprises souhaitant se lancer dans de telles opérations.

Le code civil ne comporte aucune disposition expresse relative à la force probante des informations inscrites dans un registre *blockchain*, même si une réforme de ce code pourrait toutefois la consolider à court terme. Lors des travaux préparatoires de la loi Pacte, M. Jean-Michel Mis a déposé un amendement en ce sens, qui n'a malheureusement pas été adopté. Notre code civil doit évoluer pour rassurer les utilisateurs de cette technologie, quel que soit leur corps de métier ou leur secteur d'activité, les huissiers et les notaires y recourant au même titre que les professionnels de l'immobilier. Rappelons que la *blockchain* permet de « tokeniser » des actifs liquides, autrement dit de leur substituer un élément équivalent, quoique sans valeur intrinsèque, une fois sorti du système. N'importe qui peut dès lors investir depuis son ordinateur dans un bien immobilier à la propriété fractionnée. Là encore, il faudrait apporter une sécurité juridique aux acteurs, qui le réclament d'ailleurs. Il conviendrait d'inscrire dans le code civil que les informations figurant sur le registre d'une *blockchain*, publique ou privée, possèdent une force probante. Naturellement, il reste à s'accorder sur la nature de la présomption, irréfragable ou simple, qui en découlerait.

Je vois une opportunité à saisir dans la révision prochaine du Règlement sur l'identification électronique et les services de confiance (*electronic IDentification,*

Authentication and trust Services eIDAS). Elle pourrait déboucher sur une reconnaissance officielle de la fiabilité de la signature électronique et de l'horodatage sur une *blockchain*, sans nécessité qu'intervienne un tiers certificateur, comme c'est encore le cas actuellement.

M. Philippe Latombe, rapporteur. D'autres pays d'Europe ont-ils déjà reconnu la force probante de la blockchain ? Si oui, l'ont-ils fait de manière systématique ou ont-ils créé pour ce faire une profession spécifique ?

M. Rémy Ozcan. Certains pays ont avancé sur la question en adoptant une approche de type *sandbox*, qui permet de commercialiser services et produits pendant un certain nombre d'années, hors de la contrainte d'un cadre juridique. En somme, les entreprises disposent là d'un premier moyen d'embrasser la technologie *blockchain*.

Nos voisins européens ne se sont pas réellement penchés sur la question de la force probante. En revanche, Dubaï a reconnu la valeur de preuve de la *blockchain*, notamment pour la mise à jour du cadastre. En Suisse, l'échange de titres financiers *via* une *blockchain* fait foi autant qu'une constatation par un huissier ou un notaire. Certains pays hors de l'Union européenne ont donc démontré leur volonté de tirer les bénéfices de la technologie *blockchain*.

Nous devons selon moi adopter une attitude pionnière en la matière et ne pas nous montrer timorés. Cette technologie ne suscite-t-elle pas l'intérêt de beaucoup de tiers de confiance, y voyant un moyen de gagner en efficacité dans l'exécution de leurs tâches ? Les notaires et les huissiers souhaitent ainsi l'utiliser, convaincus qu'elle leur fournira un outil plus rapide pour user des prérogatives que leur confère la loi.

M. Philippe Latombe, rapporteur. Toute *blockchain*, privée ou publique, mérite-t-elle d'acquérir une force probante ? Certaines reposent sur un plus grand nombre d'utilisateurs que d'autres. La réglementation doit-elle prendre en compte les différentes catégories de *blockchains* ?

M. Rémy Ozcan. Le droit ne doit, à mon avis, pas se contenter d'appréhender ce qui lui préexiste, surtout au vu de l'extrême brièveté des cycles technologiques d'évolution de la *blockchain*. La réglementation ne parviendra jamais à s'adapter à toutes ses formes d'utilisation. Je préconise une approche souple et flexible.

Si nous voulons donner valeur de preuve aux informations d'une *blockchain*, il faut d'abord s'assurer de la fiabilité de son protocole et de l'impossibilité pratique de modifier les données du registre, ce qui implique de définir des critères d'architecture du protocole, à l'aune des caractéristiques de la technologie *blockchain* elle-même. Voilà pourquoi il faudrait créer une certification des *blockchains* attestant de la présence, dans leur architecture, des spécificités garantes de la robustesse du système. Nous en comptabilisons cinq : la cryptographie, la signature électronique, le registre distribué, l'utilisation d'Internet et un système de « tokenisation ». Il suffit que l'un de ces cinq éléments manque pour que rien ne garantisse plus l'incorruptibilité des données.

Le meilleur moyen d'opérer un tri dans les évolutions encore à venir de cette technologie me semble être de créer une certification, délivrée par une autorité légitime, attestant que l'on a bien affaire à un protocole *blockchain* plutôt qu'à un système d'information se présentant ainsi, à tort.

M. Philippe Latombe, rapporteur. À quel niveau, national ou européen, faudrait-il mettre en place une telle certification ?

M. Rémy Ozcan. Je suggère de s'en occuper d'abord au niveau national et ensuite seulement européen, puisqu'une certification à un échelon supranational prendra plus de temps à établir. Ce processus par étapes garantirait en outre que les entreprises étrangères désireuses d'aborder le marché français respectent un certain nombre de critères de qualité en matière d'infrastructure, sans pour autant préjuger de la qualité du produit ou du service finalement proposé.

M. Philippe Latombe, rapporteur. La France commerce beaucoup avec l'Allemagne. Des liens forts se sont tissés entre les entreprises de part et d'autre de la frontière. Ne vous paraîtrait-il pas utile d'instaurer d'abord une certification supranationale ? Elle faciliterait les échanges avec nos principaux partenaires à l'intérieur de l'espace européen de libre circulation, en évitant une sorte de balkanisation du droit de la *blockchain*, dont l'harmonisation ultérieure à l'échelle de l'Union européenne présenterait à coup sûr des difficultés.

M. Rémy Ozcan. Je partage entièrement votre conviction que nous devons concevoir nos ambitions à l'échelle supranationale européenne. Pourquoi, dès lors, ne pas réfléchir à une certification en concertation avec les Allemands ? Je préconise toutefois une approche pragmatique consistant à identifier les secteurs à même de bénéficier au plus vite d'une telle certification. Leur recours généralisé à la *blockchain* les amènerait ensuite à donner le la aux autres. Un travail pourrait s'effectuer à l'échelle de l'Union européenne, en mobilisant le droit mou, à savoir la normalisation. Rien n'empêche en effet de créer des normes européennes portant sur la souveraineté.

Une bataille se livre en ce moment autour de l'*European Telecommunications Standards Institute (ETSI)*, qui en a profité pour acquérir une position dominante dans l'élaboration de normes numériques à même d'orienter les usages futurs des nouvelles technologies.

Il faut également envisager la souveraineté sous l'angle régalien, en lien avec la gestion de l'identité ou la cybersécurité. Il me semblerait judicieux de se pencher sur ces questions à l'échelle européenne en protégeant notre marché et en donnant confiance aux investisseurs. Nombre d'entre eux, privés, souhaitent investir dans la technologie *blockchain*. Ils hésitent toutefois, faute de la certitude qu'ils se trouvent bien en présence d'une *blockchain*. Quoi qu'il en soit, il est indispensable de se saisir de ces questions au plus vite. Nous pourrions rapidement réfléchir à une certification nationale, que nous proposerions ensuite au reste de l'Union européenne.

M. Philippe Latombe, rapporteur. Je ne reviendrai pas sur les débuts de la *blockchain*. Le rapport de M. Jean-Michel Mis et Mme Laure de la Raudière en a déjà traité. Il me semble que les protocoles *blockchain* ont au départ beaucoup été utilisés aux États-Unis. Quelle place actuelle la France et l'Union européenne occupent-elles dans leur conception ? Disposons-nous de *blockchains* d'aussi bonne qualité, voire meilleures, que les plus connues ? Quelles sont nos perspectives de développement technique dans ce domaine ?

M. Rémy Ozcan. L'Union européenne a lancé une initiative à travers la *British Standards Institution (BSI)* en vue de l'utilisation d'une seule et même infrastructure commune aux pays de l'Union, ce qui leur garantirait une certaine indépendance technologique vis-à-vis de l'étranger. Il faut bien garder à l'esprit la nature *open source* de la technologie *blockchain*. Ainsi, n'importe qui peut en réutiliser le code pour concevoir son propre protocole. Bitcoin, la *blockchain* 1.0, a démontré sa robustesse à travers un premier cas d'usage, le transfert de valeurs. Ethereum a lancé la création d'applications décentralisées et de contrats intelligents

dans d'autres secteurs comme la finance, les assurances ou l'industrie traditionnelle, afin d'automatiser des processus.

Malgré le caractère *open source* de la technologie *blockchain*, des brevets – et c'est là un point fondamental dont il est trop rarement question – sont déposés, beaucoup plus par des entreprises de Chine ou des États-Unis que d'Europe et, *a fortiori*, de France. Nous ne nous sommes pas encore lancés dans la course aux brevets. Il n'existe pas, à ce jour, de protocole 100 % français. Faut-il pour autant en développer ? Notre enquête a révélé le souhait d'une grande majorité des acteurs d'utiliser une *blockchain* française, c'est-à-dire l'architecture mise au point en France, par une entreprise au siège social sis en France, et financée par des investissements français.

Favoriser des liens entre des entreprises disposant d'une expertise de pointe et des instituts de recherche, tels que le Commissariat à l'énergie atomique et aux énergies alternatives (CEA) ou l'Institut national de recherche en informatique et en automatique (Inria), présente un intérêt stratégique évident. Le rapport sur les verrous technologiques et techniques de la *blockchain*, établi à l'issue de la deuxième réunion de la taskforce *blockchain*, voici deux ans, l'a d'ailleurs mis en évidence. Il faut impliquer les entreprises, en plus des instituts de recherche, pour mettre au point des protocoles dont nous maîtrisons l'entière chaîne de valeur.

M. Philippe Latombe, rapporteur. L'écosystème a paru s'émouvoir des réglementations récemment adoptées au sujet des cryptoactifs. Pourquoi ? Quelles modifications conviendrait-il de leur apporter pour pallier les critiques, et pour quelle raison ? Comment expliquez-vous les réticences que les cryptoactifs suscitent en France et en Europe? Certains, dans les milieux de la finance ou dans l'appareil d'État, craignent qu'ils servent au blanchiment d'argent et s'en méfient, vu qu'il ne s'agit pas de véritables monnaies.

M. Rémy Ozcan. Ceux qui accusent les cryptoactifs de faciliter le blanchiment d'argent méconnaissent le fonctionnement de la technologie *blockchain*. Loin de garantir l'anonymat des individus à l'origine des transactions, elle ne leur fournit qu'un pseudonyme permettant de retracer les échanges, de bitcoins par exemple, entre différents portefeuilles. Un faisceau d'indices permet aujourd'hui d'identifier grand nombre de ceux qui utilisent ce type d'actifs.

L'ancien directeur de la CIA a dénoncé une méconnaissance de l'usage de la technologie *blockchain* et de son fonctionnement. Elle ne contribue que pour une faible part au financement du terrorisme et au blanchiment d'argent. La société Chainalysis, spécialiste de l'investigation dans ces domaines, a publié un rapport révélant un usage bien plus répandu du dollar que des cryptoactifs lors de transactions douteuses.

La cinquième directive de l'Union européenne de lutte contre le blanchiment des capitaux et le financement du terrorisme (LCB-FT) s'applique à l'ensemble des échanges. Les plateformes de négociation de cryptoactifs sont ainsi soumises à la même réglementation KYC-AML (*Know your customer* et *anti-money laundering*) que les établissements bancaires tenus de vérifier l'identité de leurs clients.

Enfin, toute technologie est par essence neutre. Il appartient à ses utilisateurs de se montrer responsables. Prenons l'exemple de la Chine, qui, à la différence des autres pays, se sert des nouvelles technologies pour affecter une notation à ses citoyens. N'accusons pas la technologie mais uniquement ceux qui l'utilisent à des fins criminelles. Heureusement, un tel usage demeure extrêmement marginal. Il me paraît important que chacun mène ses propres recherches sur la *blockchain* pour en cerner le fonctionnement réel. Que penser, par ailleurs,

du mandat cash ? Ce service offert par La Poste, une institution aux liens historiquement étroits avec l'État en France, donne lui aussi lieu à des utilisations répréhensibles. Rappelons qu'il est possible d'identifier les individus à l'origine de 99 % des transactions réalisées *via* une *blockchain*.

Les prestataires de services sur actifs numériques (PSAN) utilisent les cryptoactifs au même titre que les entreprises souhaitant lancer une *ICO (initial coin offering)*, d'où la nécessité d'harmoniser la définition juridique des actifs numériques et des contrats intelligents. La superposition des définitions actuelles, convoquant par exemple les notions de jeton et de cyberjeton, complexifie inutilement la pratique du droit. Une mise à jour me semblerait la bienvenue.

L'actuelle conception officielle des contrats intelligents par trop réductrice. Ces « automates exécuteurs de clauses » permettent en réalité d'automatiser des transactions sans intervention humaine ni recours à un tiers de confiance. Ils trouvent une application dans le secteur des assurances, où ils déclenchent une indemnisation automatique en cas de sinistre, mais aussi dans le cas d'*ICO*, puisqu'ils automatisent la création et la distribution de jetons aux investisseurs ainsi que la collecte des fonds. Autrement dit, un contrat intelligent réalise les tâches que propose aujourd'hui la société de financement participatif Kickstarter, à la différence que celle-ci prélève une commission. On comprend dès lors que les PME plébiscitent leur autofinancement *via* une *blockchain*.

Revenons au cadre réglementaire applicable aux PSAN, les prestataires de l'un des neuf services sur actifs numériques répertoriés par le code monétaire et financier. Pour opérer, ils doivent, obtenir l'agrément de l'Autorité des marchés financiers (AMF) ou s'enregistrer auprès d'elle. À l'égard de ces PSAN, le législateur a retenu la même approche qu'en ce qui concerne les prestataires de services sur investissement (PSI), imposant aux uns comme aux autres des obligations des plus contraignantes, comme celle de disposer d'un important capital social, d'une assurance responsabilité civile professionnelle, de ressources humaines à l'expertise avérée et, surtout, d'un système d'identification des clients et de repérage des transactions suspectes en vue de les reporter à Tracfin.

Suite aux demandes du Groupe d'action financière (GAFI), le gouvernement français a renforcé les obligations KYC-AML, en décembre 2020, en imposant à l'ensemble des prestataires de les appliquer dès le premier euro échangé. L'étendue d'un tel dispositif exclut *de facto*, compte tenu de son coût, un certain nombre d'acteurs du marché. L'approche choisie par la France la classe donc malheureusement parmi les pays les plus contraignants pour les prestataires de services financiers recourant à des *blockchains*.

Il conviendrait en outre de modifier la supervision et l'accueil réservé à ce type d'entrepreneurs par l'AMF. Sa réglementation des PSAN, aujourd'hui bien trop contraignante, implique de trop longs délais de réponse. Une telle inertie conduit nombre de sociétés françaises à partir vers des pays aux juridictions plus souples, comme la Suisse, Dubaï ou Singapour. L'instruction AMF DOC-2019-06 prévoit un délai de vingt jours ouvrés entre la date de dépôt d'un dossier d'*ICO* et la délivrance d'un visa. Dans la pratique, l'AMF se livre à une préinstruction des dossiers d'une durée de trois à six mois, alors qu'elle-même avait fixé ce délai de vingt jours par souci de se conformer à l'esprit de la loi Pacte, destinée à garantir la compétitivité de la place financière française. Les acteurs du secteur ne peuvent plus compter que sur les élus de la République pour remédier à la situation. Nous espérons un changement des pratiques de l'autorité française de supervision des marchés financiers.

D'autres aspects du droit pourraient eux aussi évoluer. Quand une entreprise souhaite se lancer dans une *ICO*, l'AMF lui applique le droit de la consommation. Or ce droit concerne

les relations entre consommateurs et vendeurs, deux dénominations ne convenant manifestement pas à un investisseur et à l'entreprise qu'il finance.

La situation paraît d'autant plus injuste que le droit de la consommation ne s'applique pas au financement participatif (ou *crowdfunding*), au capital-investissement (ou *private equity*), à l'introduction en bourse (IPO) ou encore à l'émission obligataire. Au nom de quoi réserver un traitement à part aux *ICO* ? L'aberration se manifeste avec encore plus d'éclat quand on songe qu'en vertu de la directive Prospectus, le droit de la consommation ne s'applique pas aux *Security token offerings (STO)*, consistant, selon la définition du code monétaire et financier, à numériser des actifs financiers alors même qu'ils reposent sur la même infrastructure et mobilisent les mêmes outils que l'*ICO*. Les *STO* disposent d'un cadre réglementaire adéquat, au même titre que les *ICO* suite à la loi Pacte.

L'application du droit de la consommation aux *ICO* entraîne un autre problème. Ce droit prévoit un délai de rétractation de quatorze jours, à l'issue duquel l'intégralité des sommes versées doit être remboursée à la demande du client. Toute transaction *via* une *blockchain* donne lieu au prélèvement de frais qui rémunèrent les acteurs chargés de sécuriser et valider les transactions. Un remboursement intégral s'apparente à une double peine pour l'entrepreneur, qui doit assumer lui-même les frais d'utilisation du réseau, alors qu'il n'a finalement pas bénéficié d'un investissement. En résumé, le droit de la consommation s'avère inapte à réguler la technologie de la *blockchain*, du fait de la nature spécifique des tokens et des modalités de leur offre. Là encore, le législateur doit intervenir pour mettre fin à l'application du droit de la consommation aux *ICO*.

M. Philippe Latombe, rapporteur. Comment établir un lien entre l'utilisation de la *blockchain* et la souveraineté numérique française ou européenne ? En quoi la *blockchain* peut-elle devenir un outil de souveraineté ? Comment l'utiliser pour rebâtir notre souveraineté numérique ? Autrement dit : quel potentiel lui voyez-vous et quel usage en préconisez-vous ?

M. Rémy Ozcan. La question de la souveraineté numérique revêt une importance fondamentale pour l'avenir de notre nation et de nos entreprises. La crise sanitaire a mis en lumière notre forte dépendance économique et technologique vis-à-vis des autres pays et des grandes entreprises étrangères. L'avènement d'Internet et des nouvelles technologies a converti l'espace numérique en l'un des principaux terrains de lutte d'influence économique et politique.

La *blockchain* peut constituer une arme d'émancipation par rapport aux autres puissances mondiales, dans la mesure où elle permet de créer et d'échanger de la valeur à l'échelle internationale en s'affranchissant du système monétaire de Bretton Woods, plaçant le dollar au cœur du système financier mondial. Ces quinze dernières années, les États-Unis ont manifesté la volonté d'utiliser leur devise pour imposer leur propre réglementation hors de leur territoire. L'Union européenne souhaite aujourd'hui s'émanciper autant que possible de la tutelle des États-Unis. Dans le même temps, le Brésil, la Russie, l'Inde, la Chine et l'Afrique du Sud (les pays BRICS) ont impulsé un mouvement de dédollarisation du système financier mondial.

La Chine a d'ailleurs résolu d'utiliser la technologie *blockchain*, en tant qu'arme géopolitique, pour accélérer la dédollarisation, qu'elle associe à l'émergence de la Route de la soie. La Russie et la Chine ont en effet établi, à la faveur des changements climatiques, une nouvelle Route de la soie qu'elles souhaitent rendre accessible aux entreprises de toute la planète. Lors du dernier sommet du Groupe des vingt (G20), le dirigeant chinois, Xi Jinping, a estimé nécessaire de soutenir le développement des monnaies numériques de banques centrales *(Central bank digital currency* : *CBDC)*. Le yuan numérique a dès à présent cours.

Les entreprises qui voudront utiliser la route de la soie se verront contraintes d'y recourir en tant que monnaie de règlement des échanges commerciaux internationaux.

Un nouvel ordre financier mondial s'annonce. La technologie *blockchain* en constituera à n'en pas douter un pilier. Plus de quatre-vingts banques centrales expérimentent actuellement la création de monnaies de banque centrale à l'aide de la technologie *blockchain*. De telles monnaies présentent l'avantage d'assurer la maîtrise des flux monétaires et de faciliter l'ajustement des politiques monétaires. La simplification de l'échange d'actifs grâce à la technologie *blockchain* améliore en outre l'efficience économique. Comme cette technologie garantit la traçabilité des transactions, elle contribue enfin à la lutte contre le financement du terrorisme et le blanchiment d'argent.

Cet été, la Banque centrale européenne (BCE) décidera très probablement de créer un euro numérique, qui devrait voir le jour au plus tard en 2025. La technologie *blockchain* apparaît donc comme une arme de redistribution des cartes du système monétaire et financier international.

La pandémie a entraîné une numérisation massive et rapide des services et des produits. Les prochaines guerres ne se livreront pas sur un terrain terrestre mais dans l'espace numérique. La *blockchain* permet de sécuriser les échanges et les données en préservant leur intégrité. Autrement dit, il ne suffit pas de les intercepter pour les exploiter. Il faut encore s'approprier leurs clés de lecture, sans lesquelles elles ne présentent aucune utilité. Certains pays l'ont déjà compris : Israël ou la Russie recourent à la technologie *blockchain* dans le domaine de la cybersécurité.

À l'échelle de l'Union européenne, je préconise la rapide mise en place d'un euro numérique. Il éviterait que nous soit une fois de plus imposée une monnaie étrangère dans le commerce international. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) devrait par ailleurs superviser un recours généralisé à la technologie *blockchain* pour protéger nos infrastructures et favoriser la commercialisation et le développement de nos produits et services français à l'étranger.

M. Philippe Latombe, rapporteur. Dans quel aspect de la technologie *blockchain* devons-nous aujourd'hui investir pour affirmer notre souveraineté ? Quel usage de cette technologie faut-il promouvoir en urgence ? Par où commencer ?

M. Rémy Ozcan. Je recommande une approche pragmatique. La souveraineté peut s'envisager sous plusieurs angles. Sous celui de la gestion des données, nous pourrions créer un *cloud* décentralisé, bien plus sécurisé qu'une base de données centralisée. Combien d'entreprises ont-elles déjà fait l'objet de cyberattaques ? Combien de brèches de sécurité ont-elles déjà entraîné des fuites de données ? Combien d'exemples de piratages faudra-t-il encore avant que nous admettions notre vulnérabilité ? La *blockchain* permet de mettre fin à la dépendance vis-à-vis des GAFAM en matière de traitement et de stockage des données. Certaines entreprises l'ont déjà compris.

En matière de gestion de l'identité digitale, la *blockchain* permet d'attribuer à chaque individu un identifiant unique à l'abri des contrefaçons. Le ministère de l'intérieur a lancé un groupe de travail auquel j'appartiens. Son livre blanc, dont la parution ne saurait tarder, ambitionne de mettre en évidence l'intérêt de la *blockchain* dans la gestion des identités, notamment en vue des Jeux olympiques et paralympiques de 2024. Face à un afflux massif de personnes sur notre territoire, nous devons disposer de bases de données mondiales pour démasquer les individus usurpant l'identité d'un tiers ou susceptibles de menacer la sécurité

de nos concitoyens. De telles informations peuvent s'échanger *via* une *blockchain* sans qu'elles soient révélées dans leur intégralité.

En résumé, les bénéfices les plus évidents du recours à la *blockchain* passent par la création d'un *cloud* décentralisé et d'une identité digitale sécurisée ainsi que par les échanges d'informations à l'abri des cyberattaques en vue de préserver l'intégrité du territoire et la sécurité de ses ressortissants.

M. Philippe Latombe, rapporteur. Quelle place la *blockchain* occupe-t-elle actuellement dans notre économie ? Je ne songe pas ici à sa valeur en termes de produit intérieur brut (PIB) mais à ses usages actuels. Quels projets sur le point d'aboutir pourraient apporter une visibilité à cette technologie auprès de nos concitoyens ? Nous avons beaucoup parlé jusqu'ici de l'État et des entreprises, moins, cependant, des apports de la *blockchain* à nos concitoyens dans leur quotidien. Or il est indispensable de les impliquer dans les enjeux de souveraineté.

M. Rémy Ozcan. Les pouvoirs publics assument un rôle majeur : ils montrent la voie. Entre autres caractéristiques, la *blockchain* présente celle de l'immuabilité. Les informations, une fois validées dans le registre, deviennent impossibles à effacer. La *blockchain* assure un gain de temps et d'efficacité à l'usager comme aux services publics.

Cette technologie permettrait d'accélérer la numérisation de l'administration par la dématérialisation des documents « papier ». Suez, membre de notre fédération, œuvre dans l'économie circulaire et recourt à la *blockchain* pour assurer un traçage plus efficace des déchets et une meilleure inclusion des acteurs du secteur. Dans le même esprit, la numérisation des bordereaux de suivi des déchets réduirait la charge administrative qui pèse autant sur les pouvoirs publics que sur le secteur privé.

La *blockchain* faciliterait en outre, en l'automatisant, la mise à jour de registres comme celui du cadastre ou des actionnaires des sociétés non cotées. 85 % de la richesse créée en Europe provient des PME. Pourtant, celles-ci souffrent de difficultés de financement. La *blockchain* leur apporterait une solution, *via* la diversification de leurs investisseurs.

La mise en place d'un système de vote traçable et transparent au moyen d'une *blockchain* favoriserait une meilleure inclusion des citoyens dans les processus démocratiques. Le mouvement des Gilets jaunes a révélé une fracture grandissante entre les élus et ceux qu'ils représentent. La technologie *blockchain* apparaît comme un formidable outil pour restaurer la confiance. Grâce à elle, chacun pourrait constater, sans nécessité de s'appuyer sur la garantie d'un tiers, que son vote a bien été comptabilisé, ce qui limiterait l'abstention, révélatrice d'un problème démocratique. La mise en place d'un tel système de vote ne prendrait que quelques mois. Notre fédération se montrerait ravie de vous prêter son concours.

Le respect du code des marchés publics se révèle aujourd'hui marginal. Une entreprise répondant à un appel d'offres, pour peu qu'elle sache à qui s'adresser, obtiendra connaissance des offres concurrentes. Nous ne disposons pour l'heure d'aucun moyen de garantir la transparence dans la passation des marchés publics, hormis la *blockchain*, qui éviterait aux PME de se retrouver défavorisées par rapport aux grandes entreprises au carnet d'adresses mieux garni.

La France pourrait transmettre ces propositions et bien d'autres encore à l'occasion de sa présidence du Conseil de l'Union européenne au premier semestre 2022. La qualité de vie de nos concitoyens s'en trouverait améliorée, de même qu'en sortirait renforcée la confiance dans les élus et les institutions, mise à mal par les crises sanitaire et économique actuelles.

M. Philippe Latombe, rapporteur. La technologie *blockchain* et ses usages vous semblent-ils à même de générer un écosystème qui contribue à la souveraineté et inclue, en son sein, des dispositifs, voire une filière de formation ? En somme, cet écosystème doit-il s'intégrer à ceux, déjà en place, des *start-up* ou des nouvelles technologies ? Constituera-t-il plutôt un écosystème à part ? Dans quel cadre dispenser des formations à la *blockchain*, au vu de la multiplicité de ses usages ?

M. Rémy Ozcan. Nous avons établi le constat, partagé par M. le député Jean-Michel Mis, d'une excessive fragmentation de l'écosystème de la *blockchain*. Ses usages actuels dépassent largement celui des cryptoactifs, sa première application historique.

Nous avons opté pour une approche plurisectorielle, puisque chaque secteur d'activité dispose de sa propre réglementation et que l'usage de la *blockchain* varie considérablement de l'un à l'autre. Ceci explique que notre fédération accueille des sociétés œuvrant dans des domaines aussi différents que ceux d'EDF, Suez ou Orange. Le meilleur moyen de favoriser l'utilisation et le développement de la *blockchain* reste encore de respecter les spécificités de chaque branche pour amener leurs acteurs à saisir en quoi cette technologie peut faciliter l'extension de leurs activités en les aidant à créer des produits et des services à même de leur en apporter les bénéfices.

Il n'existe à ce jour aucune formation certifiante, reconnue par l'État, qui atteste une expertise en matière de technologie *blockchain*. La Commission européenne a partagé ce constat. Elle a d'ailleurs commandé, par l'intermédiaire d'un consortium baptisé le projet CHAISE, auquel je participe en tant que directeur général de ma société Crypto4All, une étude visant à définir les besoins des acteurs de l'écosystème de la *blockchain* pour proposer des formations qui y répondent. L'étude menée par notre fédération, achevée en octobre dernier, a montré que près de 65 % des entreprises souhaitent recruter à court terme des experts des *blockchains*, aussi bien développeurs ou architectes que commerciaux ou analystes.

Il faut donc qu'évoluent les offres de formation des écoles de commerce et des universités afin que ces entreprises disposent d'une main-d'œuvre maîtrisant la technologie *blockchain*. Celle-ci ne survivra qu'à la condition que des individus continuent à l'utiliser, la comprendre et la commercialiser. Notre fédération associe les universitaires aux entrepreneurs en vue de la conception d'une offre de formation en adéquation avec les besoins du marché.

M. Philippe Latombe, rapporteur. Faut-il institutionnaliser ces formations dès le départ ? Les entreprises qui en ressentent le besoin ne devraient-elles pas plutôt les organiser elles-mêmes, dans un premier temps, quitte à se regrouper, en préalable à la création d'une filière spécifique ?

M. Rémy Ozcan. Je recommande la même approche pragmatique que celle du gouvernement lorsqu'il a modifié les enseignements du primaire, du collège et du lycée en vue d'une meilleure adéquation avec le marché du travail, tel qu'il est appelé à évoluer au cours des dix prochaines années. Le ministère de l'éducation devrait inciter écoles et universités à intégrer dans leur offre de formation des modules *blockchains*. Les entreprises ne demandent qu'à dispenser leur expertise en la matière dans un tel cadre.

Il conviendrait de délivrer des formations à tous les corps professionnels, aussi bien aux métiers du droit, à l'École nationale de la magistrature (ENM), qu'à ceux de l'immobilier. Comment avocats et juristes pourraient-ils conseiller les entreprises sans comprendre le fonctionnement de la *blockchain* ? Une approche par corps de métier donnerait lieu à une sensibilisation progressive à l'impact de la technologie *blockchain* pour chaque secteur. À la

seule condition de disséminer et d'augmenter la qualité de l'expertise dans ce domaine, nous réussirons à convertir la France en « *blockchain nation* ».

M. Philippe Latombe, rapporteur. Souhaitez-vous évoquer un point que nous aurions omis d'aborder ? Quelles préconisations du rapport de M. Jean-Michel Mis et Mme Laure de la Raudière n'ayant pas été adoptées, ou du moins pas à temps, ou pas complètement, faudrait-il de nouveau mettre en avant ? J'aimerais en quelque sorte établir un point d'étape pour nous rendre compte de ce qu'il reste à implémenter afin d'aller au bout de la démarche entamée.

M. Rémy Ozcan. Je conseillerais d'abord de reprendre l'amendement déposé à l'occasion des travaux préparatoires de la loi Pacte, en vue d'établir la force probante des informations inscrites dans une *blockchain*. Notre fédération se tient à votre disposition pour aider le législateur à déterminer les types de protocoles suffisamment fiables, ou même proposer une définition de la technologie *blockchain* plus complète que l'actuelle. L'ordonnance du 28 avril 2016 caractérise en effet cette technologie comme un dispositif d'enregistrement électronique partagé, sans prendre en compte l'étendue de ses cas d'usage. Ces deux mesures rassureraient un certain nombre d'acteurs.

Lors de son audition par Mme la députée Typhanie Degois, à l'occasion de l'examen du projet de loi de finances 2021, notre fédération avait en outre demandé à disposer de systèmes de financement dédiés aux acteurs de la *blockchain*. Leur mise en place indiquerait clairement aux investisseurs comme aux entrepreneurs le soutien des pouvoirs publics à la *blockchain*, indépendamment de la somme qu'ils lui consacreraient. L'éligibilité des projets *blockchain* à des dispositifs en faveur de l'innovation tels que le Programme d'investissements d'avenir (PIA) ne suffit pas. La confiance joue un rôle fondamental dans les affaires. Dès lors que les acteurs jugeront la technologie *blockchain* fiable, ils développeront grâce à elle de nouveaux produits et services favorables à la croissance de l'emploi.

La mise en place des trois éléments que je viens d'indiquer, associée à celle de formations adaptées, marquerait un grand pas en avant vers la professionnalisation de l'industrie de la *blockchain*.

M. Philippe Latombe, rapporteur. Nous accueillerons volontiers vos suggestions quant à la force probante. Nous y reviendrons lors d'autres auditions à venir.

Souhaitez-vous aborder un dernier point ?

M. Rémy Ozcan. J'aimerais revenir sur les moyens d'aider les entreprises de la *blockchain*.

D'abord, nous devons renforcer notre capacité de contribution à leur financement. Ensuite, il faudra instaurer un cadre réglementaire intelligible favorable à l'utilisation de cette technologie. Enfin, il serait bon qu'évoluent les pratiques de place des autorités de supervision. Si celles-ci persistent à ne pas traduire, dans la pratique, l'état d'esprit de la loi, le sentiment viendra qu'une fois de plus, la France ne se sera pas montrée à la hauteur de ses ambitions. Le gouvernement a manifesté à plusieurs reprises sa volonté, partagée par l'ensemble des acteurs, de faire de notre pays une « *blockchain nation* », ce pour quoi ils se sont mobilisés et structurés autour de la FFPB.

Celle-ci reste à la disposition des pouvoirs publics pour échanger en vue du développement d'un écosystème structuré, en voie de professionnalisation et en adéquation

avec l'évolution de notre économie. J'ai indiqué des actions à mener dans l'intérêt des entreprises. Cependant, la question mérite qu'on y réfléchisse du point de vue des particuliers.

Un abattement fiscal de 50 % du montant investi dans une *ICO* en cas de conservation des actifs pendant une durée de deux ans, le temps, pour une entreprise, de mener à terme un projet puis de le commercialiser, inciterait à investir dans les PME recourant à ce type d'opération pour se financer. Une mesure similaire porte déjà sur les actions émises par les PME.

L'imposition à taux unique des particuliers ayant investi dans les cryptoactifs avoisine les 30 %. Certes, ce taux frôlait auparavant les 50 %, mais il conviendrait que la France s'aligne sur les autres pays. Nos voisins européens s'en tiennent à des taux d'imposition bien plus faibles. Le calcul de la plus-value, d'une grande complexité, repose sur l'établissement de moyennes. Le formulaire n°2086 de déclaration des plus ou moins-values de cessions d'actifs numériques apparaît mal adapté à la réalité des mouvements de cryptoactifs. Il autorise à déclarer cinq opérations seulement, un nombre de transactions qu'il n'est pas rare d'opérer en l'espace d'une journée. Il reste en outre à éclaircir la notion d'activité occasionnelle et à titre habituel. Les plus-values réalisées à l'issue d'investissements dans des cryptoactifs, par le biais d'*ICO* ou de *PSAN* établis en France ou à l'étranger, pourraient être exonérées d'impôts à condition qu'elles soient consacrées à l'achat de biens ou de services, sur lesquels l'État prélève 20 % de taxe sur la valeur ajoutée (TVA). Une telle mesure favoriserait l'adoption des cryptoactifs par les commerçants. Rappelons que l'euro numérique verra le jour au plus tard en 2025. L'Allemagne elle-même a opté pour une telle approche pragmatique.

Un cadre réglementaire et fiscal adapté, ajouté à des pratiques de place en adéquation avec nos ambitions, ainsi qu'au soutien des pouvoirs publics et des investisseurs privés, permettrait à la France d'occuper une place majeure dans la compétition internationale déjà bien entamée dans le domaine de la technologie *blockchain*.

M. Philippe Latombe, rapporteur. Une collègue ayant dû quitter la réunion s'interrogeait sur l'empreinte carbone et la consommation d'énergie de la technologie *blockchain*. Existe-t-il des projets pour les limiter ? La technologie *blockchain* est-elle compatible avec la réduction des émissions de gaz à effet de serre ? Nous apprécierions une réponse écrite à ces questions, que le temps nous manque de traiter.

M. Rémy Ozcan. Je vous rassure, il existe une multiplicité de protocoles parfaitement compatibles avec le souci de l'écologie, à la différence du protocole bitcoin, encore que de récentes études aient démontré une surévaluation de sa consommation énergétique. Notre réponse vous parviendra par écrit ces jours prochains.

Audition, ouverte à la presse, de M. Sébastien Dupont, président co-fondateur d'UNIRIS et de M. le général d'armée Grégoire de Saint-Quentin, président du cabinet de conseil Petra advisors et ancien conseiller du gouvernement pour la défense
(22 avril 2021)

Présidence de M. Philippe Latombe, rapporteur.

M. Philippe Latombe, président et rapporteur. Nous auditionnons M. Sébastien Dupont, président co-fondateur d'UNIRIS, ainsi que M. le général d'armée Grégoire de Saint-Quentin, président du cabinet de conseil Petra advisors et ancien conseiller du gouvernement pour la défense.

Cette audition publique s'inscrit dans nos travaux sur les technologies numériques de pointe, dont la *blockchain* fait partie. UNIRIS est une *start-up* issue de l'incubateur de Paris-Saclay. Elle propose une solution biométrique, couplée à une *blockchain*, permettant de s'identifier sans *login* ni mot de passe. Son périmètre d'action inclut nombre de sujets qui nous intéressent, depuis l'identité numérique auto-souveraine au contrat intelligent en passant par le vote sécurisé à distance.

Je souhaite évoquer trois sujets à titre liminaire. D'abord, je vous poserai ma question rituelle : quelle est votre approche de la souveraineté numérique ? Il en existe une grande diversité de définitions. Quelle est la vôtre ? En quoi la *blockchain* peut-elle constituer un levier de souveraineté, autant pour la France que pour l'Europe ? J'aimerais à cette occasion que vous nous présentiez UNIRIS, votre *blockchain* et ses cas d'usage.

Mon second point portera sur le développement en France d'un écosystème *blockchain* performant. La création d'UNIRIS au sein de l'incubateur Paris-Saclay vous permet de porter un regard lucide sur la capacité de notre pays à soutenir et financer les entreprises technologiques. J'aimerais que vous évoquiez le parcours d'UNIRIS et les difficultés éventuelles que vous avez pu rencontrer. Comment jugez-vous l'action des pouvoirs publics dans ce domaine, alors que le gouvernement a pris l'initiative, avec les acteurs du secteur, d'une stratégie nationale *blockchain* ? Notre mission accueillera volontiers toute proposition de votre part en vue de soutenir le développement des entreprises technologiques spécialistes de la *blockchain*.

Enfin, je désire que nous échangions sur la *blockchain* d'un point de vue européen. D'une part, je me demande comment la France se situe dans ce domaine par rapport à ses voisins. D'autre part, je souhaite vous entendre à propos des actions de soutien à la *blockchain* menées par l'Union européenne, en vue notamment de réguler les cryptomonnaies. Nous aurons ainsi l'occasion d'évoquer l'enjeu crucial de la force probante de la *blockchain*.

M. Sébastien Dupont, président co-fondateur d'UNIRIS. J'assimile la souveraineté numérique à la capacité à contrôler ses données numériques, autrement dit, à un niveau politique, supra-individuel, national, au fait de ne pas dépendre du bon vouloir d'autres puissances économiques ou politiques dans l'usage des outils numériques. Concrètement, cette souveraineté consiste à disposer d'un endroit neutre où mettre en œuvre ces outils numériques.

M. le général d'armée Grégoire de Saint-Quentin, président du cabinet de conseil Petra advisors et ancien conseiller du gouvernement pour la défense. J'accompagne M. Sébastien Dupont, car je suis convaincu de l'impact réel de la *blockchain* sur la souveraineté

numérique. Nous devrions, grâce à son exposé, approcher d'une définition assez précise de cette notion.

M. Sébastien Dupont. À l'issue d'une formation d'ingénieur en cybersécurité, j'ai été en charge de l'identité numérique chez Thales et Orange avant de fonder UNIRIS, entreprise que je dirige actuellement. Sa création répond au besoin fondamental de rendre accessible au plus grand nombre une technologie sécurisée, *via* une identité numérique universelle inviolable, dans un environnement numérique de confiance à même de garantir la souveraineté des individus, des entreprises et des États.

Nous comptons, pour y parvenir, créer une fondation chargée de rendre notre technologie *open source*. UNIRIS détient douze brevets, dont certains déposés en France, et emploie quinze salariés. Nous travaillons en partenariat avec l'École polytechnique et le centre national de la recherche scientifique (CNRS), qui nous apportent une aide immense. Nous avons reçu, entre autres distinctions, le label du comité stratégique de filière « industries de sécurité » pour les Jeux olympiques de Paris de 2024. Notre financement actuel repose en grande part sur des investissements personnels, ou de particuliers impliqués dans la défense de la souveraineté.

Aujourd'hui, un simple accès à nos *e-mails* nous oblige à passer par une infinité d'intermédiaires que nous ne connaissons pas. Nous ne nous rendons plus compte du nombre de personnes ou de logiciels, hors de notre contrôle, disposant d'un accès à nos données. Les États-Unis et la Chine détiennent l'ensemble des intermédiaires. Chaque connexion au web, chaque transaction en ligne dépendent du bon vouloir des États-Unis. Même en Europe, nous sommes soumis à ces deux grandes puissances. Il n'est plus temps de créer des entreprises concurrentes de Google, Apple, Facebook, Amazon et Microsoft (les GAFAM), ce qui, de toute façon, ne résoudrait pas le problème sur le long terme. La seule solution à notre dépendance réside dans un environnement numérique neutre, autrement dit dans la *blockchain*.

Ce système entièrement décentralisé permet à chacun de regagner le contrôle. Depuis sa conception en 2009, il a fait ses preuves et ne cesse de s'améliorer. Citons, parmi ses caractéristiques, sa neutralité, qui le rend insensible à toute ingérence humaine. Des algorithmes mathématiques garantissent son incorruptibilité. La *blockchain* résiste en outre aux cyberattaques, puisque son principe fondateur, selon lequel le moindre de ses composants pourrait en théorie faillir, se traduit par une exigence de parfaite transparence. Les *blockchains* se comptent parmi les environnements numériques les plus sécurisés.

UNIRIS a amélioré la technologie de la *blockchain*, de façon à mieux l'adapter aux besoins actuels. La *blockchain* UNIRIS est ainsi en mesure de traiter un million de transactions par seconde, contre dix seulement pour la *blockchain* bitcoin. Notre travail avec le CNRS sur nos algorithmes mathématiques a augmenté notre sécurité, d'un niveau désormais égal au secteur de l'aviation. Notre consommation énergétique est trois milliards de fois moindre que celle de la *blockchain* bitcoin.

Nous avons travaillé sur l'accessibilité de la *blockchain* au plus grand nombre en recourant à la seule solution envisageable, la biométrie, qui évite le recours aux *logins* et mots de passe. Les solutions biométriques actuelles, du fait qu'elles impliquent le stockage de données en vue de la comparaison d'empreintes, s'avèrent incompatibles avec le Règlement général sur la protection des données (RGPD). La *blockchain* UNIRIS, elle, s'y conforme en tout point, puisqu'elle s'appuie sur les particularités du réseau veineux propre à chaque individu pour générer des clés cryptographiques uniques. Nous avons créé un portefeuille d'identités numériques universel à même de stocker une infinité d'identités numériques. La certification de l'une d'elles par l'État en France permettrait, par exemple, de remplacer le

passeport ou de procéder au règlement des impôts. Des services de santé pourraient aussi y recourir.

Les contrats intelligents impliquent de programmer une *blockchain* pour exécuter automatiquement certaines actions comme l'envoi, au moment du versement de salaires, d'informations à une caisse de retraite, à la sécurité sociale ou à l'Union de recouvrement des cotisations de sécurité sociale et d'allocations familiales (URSSAF). Il ne resterait plus ensuite à l'État qu'à vérifier ces informations. Un contrat intelligent permettrait aussi, au quotidien, de déclencher un chauffage en fonction de la température extérieure.

Notre *blockchain* publique verra le jour dans quelques semaines. Il est prévu de l'appliquer à la gestion de données de santé, de villes intelligentes ou d'événements sportifs. Nous nous concentrons pour l'heure sur les briques essentielles à la création d'un Internet de confiance, qui passe par l'identité numérique, l'hébergement de sites web et des *e-mails* sécurisés.

Le gouvernement indien a mandaté UNIRIS pour mettre au point une solution de traitement de transactions bancaires à même de remplacer Visa et Mastercard. Il n'existe pas, en dehors d'UNIRIS, de *blockchain* ou de réseau centralisé capable de gérer les transactions de plus d'un milliard de personnes.

Un réseau *blockchain* se constitue de dizaines de milliers de mineurs hébergés sur toute la planète chez des particuliers désireux de contribuer à la sécurité du réseau. La nécessité s'est fait jour de dédommager ces contributeurs sans préjudice pour l'autonomie du système. La cryptomonnaie n'a jamais eu pour vocation de concurrencer les devises existantes. Elle propose une alternative fondée sur la réalité du marché, indépendamment de toute décision humaine.

À l'instar des actions boursières, la cryptomonnaie joue un rôle complémentaire par rapport aux autres devises. Elle ne possède de valeur que dans le monde virtuel. Son usage dans le monde réel oblige à la convertir en une autre devise, tel l'euro. Elle ne sert en somme qu'à faciliter et sécuriser les échanges entre les mondes réel et virtuel. Loin de constituer une fin en soi, elle ne relève que d'une nécessité pour garantir le fonctionnement de ce bien commun numérique qu'est la *blockchain*.

La quasi-totalité des fonds d'UNIRIS provient de ses fondateurs et de particuliers ainsi que d'un prêt de la banque publique d'investissement (Bpifrance). Nous collaborons étroitement avec des dizaines d'entreprises et d'administrations. La lourdeur de la réglementation des marchés publics rend impossible tout autofinancement d'une jeune entreprise par des commandes.

Nous avons toutefois bénéficié de la disponibilité sans faille de l'Autorité des marchés financiers (AMF) et du ministère de l'économie, des finances et de la relance, notamment à propos de l'application aux cryptomonnaies de la taxe sur la valeur ajoutée (TVA). Un cadre réglementaire incertain fait peser sur les entreprises *blockchain* un risque constant, qui pénalise lourdement leur fonctionnement quotidien.

La dilution dans les administrations intermédiaires des fonds publics destinés aux *start-up* les empêche au final d'en profiter. Celles que financent des fonds d'investissement dotés par l'État se voient contraintes de négocier leur revente dans un délai de cinq ans, idéalement aux GAFAM, ce qui s'avère un comble.

Enfin, les entreprises *blockchain* doivent supporter le risque permanent d'une clôture ou d'un gel arbitraires de leurs comptes par les banques françaises. Les entreprises *blockchain* jouent cependant un rôle clé dans la protection, et la souveraineté nationale, des entreprises et des citoyens. Elles proposent une technologie capable d'optimiser l'administration en la rendant plus efficace. Cette technologie bouleverse les conceptions actuelles de la souveraineté et de la protection. Il n'est plus possible d'ignorer la révolution industrielle qu'elle opère à l'échelle mondiale.

En tant que technologie de confiance éprouvée, la *blockchain* entraînera, en effet, inévitablement, une révolution. Les géants actuels de la *blockchain* viennent, pour ne pas changer, d'Asie et des États-Unis. Coinbase est désormais cotée à Wall Street. La Chine détient des coopératives de mineurs bitcoin. En Corée du Sud, 80 % de la population utilise la cryptomonnaie. La France risque une fois de plus de voir sa technologie lui échapper au profit d'autres puissances, alors même que celle-ci pourrait lui permettre de reprendre la place qui lui revient sur la scène internationale.

La technologie de la *blockchain* apparaît d'autant plus stratégique qu'elle pourrait neutraliser notre dépendance aux outils numériques fournis par d'autres puissances. La France doit accueillir cette technologie pour rattraper le train en marche. Malgré l'enjeu stratégique, la majorité des investissements proviennent encore de particuliers. L'État doit s'impliquer davantage en soutenant les solutions stratégiques pour la protection et la souveraineté numériques. Il apparaît urgent que les banques françaises acceptent enfin les fonds provenant d'échanges sur des plateformes agréées par l'AMF. Des intermédiaires comme Bpifrance devraient passer des commandes plutôt que d'accorder des prêts ou des subventions. Faute de mesures concrètes, UNIRIS ne pourra plus, d'ici quelques mois, payer ses salariés, ce qui contraindra l'entreprise à se domicilier à l'étranger pour survivre.

M. Philippe Latombe, rapporteur. Vous avez consacré une part notable de votre présentation aux cryptomonnaies. Que préconisez-vous aujourd'hui, techniquement, sur le plan législatif ou réglementaire, pour lever les freins à leur usage ?

M. Sébastien Dupont. Il nous est pour l'heure impossible d'inscrire nos avoirs sous forme de cryptoactifs sur les comptes de notre société, sous peine de leur gel par les banques françaises. Une première mesure d'urgence consisterait à lever ce frein.

M. Philippe Latombe, rapporteur. Les banques adoptent là une position de principe. La loi ne les contraint pas à geler les comptes approvisionnés par des cryptoactifs.

M. Sébastien Dupont. Une partie de nos cryptoactifs a transité par PayPal, qui nous a accusés de violation de son contrat d'utilisation, alors que celui-ci ne contenait aucune disposition à ce sujet. PayPal a gelé la totalité de nos avoirs. Le risque existe qu'une banque, faute de savoir à quel texte réglementaire s'en tenir, décide de geler nos comptes par prudence, ce qui nous place dans une situation compliquée en termes de versement des salaires et de règlement des impôts.

M. Philippe Latombe, rapporteur. À quelle somme en euros correspond le flux de cryptoactifs que vous souhaiteriez convertir chaque mois ?

M. Sébastien Dupont. Il nous faudrait convertir, au moins pour payer nos salariés, une centaine de milliers d'euros chaque mois, soit une manne qui nous reste pour l'heure inaccessible.

M. Philippe Latombe, rapporteur. Comment interprétez-vous la vision des cryptoactifs que nourrissent l'État, et plus généralement les entités publiques ? Inspirent-ils de la défiance ? L'expliquez-vous par une méconnaissance de leur fonctionnement ?

M. Sébastien Dupont. La crise sanitaire que nous traversons met à mal le système traditionnel. La crainte existe d'une conversion en cryptomonnaie d'une part de l'épargne susceptible d'être réinjectée dans l'économie sous forme d'euros. En réalité, les cryptomonnaies fonctionnent comme toute autre devise. À ce titre, elles permettront, sans que l'État ait à débourser le moindre centime, de financer la révolution industrielle qui se prépare.

L'engagement de M. Bruno Le Maire à recourir à une *blockchain* à l'occasion des JO témoignait d'une volonté des pouvoirs publics de se saisir de cette technologie. La situation a toutefois changé depuis. Elle empire au point que tous les acteurs de la *blockchain* en France se tournent aujourd'hui vers l'étranger.

M. Philippe Latombe, rapporteur. Revenons à la commande publique. Plutôt que de recevoir des subventions, les entreprises préfèrent étendre leur clientèle, car elles y trouvent, outre un bénéfice financier, une occasion de se confronter au réel en adaptant leurs produits aux besoins des commandes. Comment créer un marché pour une technologie de rupture, telle que la *blockchain*, alors même que les besoins de l'État ou des collectivités territoriales restent à définir ? Comment susciter un besoin qui incite à recourir à UNIRIS ?

M. Sébastien Dupont. Les pratiques anglo-saxonnes en la matière font école aujourd'hui. Il faut commencer par écouter le client. Le plus délicat reste de trouver un interlocuteur valable, qui nous explique son problème. Lui fournir ensuite une solution à partir du protocole, assorti d'outils, mis au point par notre entreprise, ne présente pas tant de difficultés.

Aujourd'hui, les acheteurs des administrations ou des entreprises que nous rencontrons ignorent ce qu'il leur faut vraiment. Si les détenteurs de solutions potentielles pouvaient directement s'entretenir avec ceux qui ont cerné les difficultés, il ne manquerait plus qu'un acteur comme Bpifrance pour faciliter le financement. Imposer aux *start-up* un seuil de dispense de procédure pour la passation d'un marché public fixé à 25 000 euros place celles-ci dans l'obligation de dépenser la totalité de cette somme pour fournir une solution, ce qui ne leur permet que de survivre et non de se développer.

M. Philippe Latombe, rapporteur. Vous laissez entendre que Bpifrance, au-delà de son appui financier, devrait passer des commandes publiques. Or son statut de banque ne le lui permet pas, du fait de la législation européenne. Comment, dès lors, éduquer l'État aux nouvelles technologies ? Comment l'inciter à les utiliser dans sa transformation ?

M. Sébastien Dupont. Il manque une structure administrative intermédiaire. J'ai certes émis l'idée, plus tôt, que la quantité de structures existantes rend l'écosystème étouffant. Il faut discuter avec une dizaine d'entre elles avant d'obtenir la moindre commande. Néanmoins, il serait formidable que voie le jour une structure en mesure d'indiquer quels enjeux de souveraineté la *blockchain* pourrait résoudre et dans quel cadre procéder à des expérimentations avec les entreprises.

M. Philippe Latombe, rapporteur. Général, faut-il en conclure à la nécessité de modifier la structure de l'État en ce qui concerne le numérique ? Un secrétariat d'État à Bercy vous paraît-il suffisant ? La Direction interministérielle du numérique (DINUM) joue-t-elle bien son rôle ?

Gal Grégoire de Saint-Quentin. Je ne me considère pas comme le mieux à même de répondre à une telle question. Mon expérience au ministère des armées, à l'origine d'importantes commandes publiques, m'a permis de constater un manque d'agilité et de flexibilité par rapport à des cycles technologiques d'une extrême rapidité. La rigidité de l'établissement de trop nombreux budgets ne permet pas d'en réserver une part significative à des solutions de rupture. Or, pour passer des commandes, il faut de l'argent disponible. Les *start-up* progressent moins vite grâce aux subventions qu'aux commandes, car celles-ci donnent confiance aux investisseurs. Il conviendrait de flexibiliser le système.

M. Philippe Latombe, rapporteur. Que vous inspire la situation de l'identité numérique en France ?

M. Sébastien Dupont. Je la qualifierais de catastrophique. En tant que chef d'entreprise, je dois gérer des identités numériques professionnelles, en plus des personnelles, à n'en plus finir. À titre d'exemple, il m'a fallu plusieurs semaines pour trouver, après la perte d'un mot de passe, un interlocuteur qui me permette de récupérer la main sur celle que j'utilise pour le fisc. La situation pose un véritable problème. Déjà pénible pour l'utilisateur, elle oblige à utiliser des outils potentiellement minés par des failles de sécurité. L'identité numérique ne me semble pour l'heure pas du tout adaptée à la nature humaine. En effet, nous ne sommes pas des machines capables de stocker des quantités de *logins* et de mots de passe. L'être humain ne doit pas devenir esclave de la technologie. Il faut au contraire qu'il puisse s'en servir de manière indolore et sécurisée.

M. Philippe Latombe, rapporteur. Nous avons auditionné, voici peu, l'agence nationale des titres sécurisés (ANTS), la société IDEMIA et la directrice du programme interministériel France Identité numérique. Il existe une volonté forte d'accélération de la part de l'État dans ce domaine. La carte nationale d'identité électronique, annoncée par l'Imprimerie nationale comme le réceptacle d'identités numériques futures, devrait bientôt voir le jour. Comment vous inscrivez-vous dans ce processus ?

M. Sébastien Dupont. Nous menons un travail en lien avec l'Imprimerie nationale. Nous œuvrons dans la technologie profonde, redéveloppant toutes les couches réseaux et le *hardware*. Notre désir d'être présents sur tous les fronts en même temps consomme une part considérable de nos ressources. Malgré notre volonté de nous impliquer, nous ne pouvons pas siéger dans toutes les commissions.

M. Philippe Latombe, rapporteur. Le déploiement de la carte nationale d'identité électronique ne devrait plus tarder. Elle comportera une puce accueillant des données relatives à des identités numériques publiques ou privées. Comment, selon vous, s'articuleront les deux ? Reviendra-t-il au titulaire de la carte de décider quel type d'identité numérique il y stockera ? L'État imposera-t-il ses décisions, *via* des marchés publics auxquels vous devrez répondre par une offre ? Comment ce marché émergent de l'identité numérique vous apparaît-il ? Craignez-vous une préemption de la part d'acteurs semi-publics tels que l'Imprimerie nationale ?

M. Sébastien Dupont. Il me semble inévitable qu'une entité proche du gouvernement héberge la carte d'identité nationale. La question porte plutôt sur le moyen d'y accéder. Des solutions biométriques apparaissent valables et sensées. Les utiliser pour accéder aussi bien à la carte officielle délivrée par l'État qu'à d'autres identités numériques réconcilierait les secteurs public et privé.

M. Philippe Latombe, rapporteur. Vous répondriez donc à un appel d'offres ?

M. Sébastien Dupont. Les entreprises du secteur informatique travaillent beaucoup sur les architectures. Nous commençons en général par réunir un maximum de personnes pour réfléchir à l'interaction des différentes composantes d'un projet avant de le lancer. Dès lors qu'existent différents types de solutions, il est préférable d'envisager le moyen pour chacun de les mobiliser. Il pourrait être intéressant de participer à des groupes de travail consacrés à la rationalisation et à la sécurisation de ces différentes identités.

M. Philippe Latombe, rapporteur. UNIRIS recourt à la technologie *blockchain* encore peu utilisée par l'État. Certains la jugent absconse, d'autres la réduisent aux cryptoactifs. Comment une technologie encore aussi mal comprise peut-elle matériellement trouver sa place dans la carte nationale d'identité ?

M. Sébastien Dupont. Cette carte contiendra une clé privée cryptographique d'accès à tous les services imaginables. Héberger une telle clé dans l'environnement neutre et sécurisé d'une *blockchain* préserverait de toute ingérence humaine. La question du contrôle de l'outil par un pays donné ne se pose plus. Ainsi, les algorithmes se chargent seuls d'assurer le fonctionnement de la *blockchain*, que nul ne peut dès lors plus remettre en cause.

Prenons l'exemple d'un vote à l'échelle nationale : le recours à une *blockchain* désamorce toute contestation. La neutralité d'un tel système *open source* opérant en toute transparence garantit la conformité des procédures. Un changement de paradigme s'amorce. L'utilisateur du système en garantit lui-même la fiabilité, au lieu de devoir s'en remettre à des tiers.

M. Philippe Latombe, rapporteur. Encore faut-il que la *blockchain* ait une force probante, ce qui n'est pas le cas aujourd'hui en France.

M. Sébastien Dupont. Tout à fait. Nous collaborons avec une chercheuse, dont le prix de l'Académie des sciences a salué l'an dernier le travail sur les réseaux décentralisés de la *blockchain*, travail qu'elle mène en parallèle à d'autres travaux sur l'aviation. Nous avons diffusé des *white papers* et des *yellow papers* décrivant mathématiquement le projet mis en œuvre. Ils apportent la preuve mathématique de l'impossibilité de corrompre la moindre transaction passée *via* la *blockchain*.

M. Philippe Latombe, rapporteur. Mais comment transformer la certitude mathématique en preuve légale ? Faut-il modifier le droit et rendre la *blockchain* probante dans tous les cas ? Toutes les *blockchains* se valent-elles ? Faut-il recourir à des tiers de confiance ou des certificateurs ? Le cas échéant, pourrait-on se tourner vers des professions existantes ou conviendrait-il d'en créer de nouvelles ? Avez-vous étudié ce problème, français, au niveau européen ?

M. Sébastien Dupont. La valeur probante de la *blockchain* est d'ordre mathématique. La *blockchain* convoque la notion de « notaire ». Dès lors qu'une identité est certifiée, par la gendarmerie par exemple, il devient impossible de la remettre en cause. Le système judiciaire devra s'adapter pour le comprendre, peut-être en sollicitant des experts mathématiques. Quoi qu'il en soit, d'un point de vue technique, la valeur probante de la *blockchain* ne laisse aucune place au doute.

M. Philippe Latombe, rapporteur. Prenons un exemple : la conclusion d'un contrat de prêt bancaire implique le calcul d'un taux annuel effectif global (TAEG). Il a fallu une dizaine d'années de jurisprudence pour établir que ce taux ne faisait pas foi au-delà de deux chiffres après la virgule, alors que des conflits ont porté sur cinq à dix décimales. Compte tenu de la brève durée des cycles technologiques, il vaudrait mieux que le législateur vous fournisse

un cadre ne dépendant pas d'outils mathématiques. Comment y parvenir ? Dans le cas contraire, il faudra s'attendre à des batailles d'experts, car tous les tribunaux ne traiteront pas forcément de la même manière les contrats intelligents, d'où d'éventuelles saisies des cours d'appel, voire de la Cour de cassation.

Cette question doit intéresser vos investisseurs et vos clients, puisqu'elle rejoint celle de l'usage de la *blockchain* et, donc, des revenus qu'elle pourrait générer.

M. Sébastien Dupont. La *blockchain* pourrait confirmer l'identité d'une personne contractant un prêt. Du moins, nous pourrions techniquement en apporter la preuve, même si cette preuve n'a pas, pour l'heure, de valeur juridique. Dès lors que l'État manifesterait la volonté de s'atteler à ce chantier, en vue d'améliorer l'efficacité de son administration, nous serions heureux d'y participer. En tout cas, il faudra tôt ou tard confronter les mathématiques à la loi.

M. Philippe Latombe, rapporteur. Des solutions comparables à celles que propose UNIRIS existent-elles dans d'autres pays européens ?

M. Sébastien Dupont. Nous occupons une position particulière. Nous voulions répondre à deux défis : permettre à toute personne, même dépourvue de connaissances technologiques, de se connecter à une *blockchain*, et en créer une qui ne consomme pas trop d'énergie. L'amélioration de ces aspects a nécessité des années de travail.

La *blockchain* bitcoin présente le grand mérite de respecter les principes philosophiques qui fondent cette technologie. Il convient de saluer l'apport d'Ethereum en matière de contrats intelligents. Les autres *blockchains* ne se démarquent pas vraiment du lot. Seule UNIRIS s'est concentrée sur l'identité numérique, la sécurité et l'efficience énergétique.

M. Philippe Latombe, rapporteur. Décelez-vous l'émergence d'une filière *blockchain* française ou européenne aujourd'hui ? Existe-t-il des spécialistes de cette technologie en Europe ? Certaines écoles assurent-elles des formations spécifiques ? Des entreprises ou des administrations commencent-elles à s'y intéresser ? Comment aider l'écosystème actuel à se développer ? D'ailleurs, que représente-t-il au juste,?

M. Sébastien Dupont. Une filière française commence bel et bien à se structurer autour d'une petite communauté d'entreprises qui, curieusement, travaillent aussi bien avec des entités françaises que du reste du monde, en s'efforçant d'apporter une réponse honnête aux problèmes qui surgissent.

Nous avons participé au programme européen Horizon 2020. Nos candidatures à des appels d'offres n'ont pas été retenues pour des raisons de coût, que nous n'avons d'ailleurs pas très bien comprises. Le RGPD marque en tout cas une formidable avancée. Sinon, nous nous sentons aujourd'hui plus proches du reste du monde.

M. Philippe Latombe, rapporteur. Voyez-vous un atout dans le RGPD ?

M. Sébastien Dupont. Oui, car notre fer de lance n'est autre que la protection de la vie privée.

M. Philippe Latombe, rapporteur. Vous tenez le RGPD, en tant qu'outil de réglementation, pour un moyen de protéger notre souveraineté ?

M. Sébastien Dupont. Tout à fait. Il suffit que quelqu'un ait accès à nos données personnelles, où qu'il se trouve, pour que le reste de la planète parvienne également à y accéder. Le RGPD marque une énorme avancée en matière de souveraineté numérique.

M. Philippe Latombe, rapporteur. Dans vos discussions, les responsables indiens vous ont-ils laissé l'impression d'une plus grande réactivité par rapport à leurs homologues français ? Comment percevez-vous leur état d'esprit comparé au nôtre ?

M. Sébastien Dupont. Le simple fait que le gouvernement indien ait mandaté une petite *start-up* française pour réfléchir à une solution qui remplace Visa et Mastercard en matière de transactions électroniques me paraît extraordinaire. Les responsables indiens ne doutent pas de la nécessité de recourir à la technologie de la *blockchain* pour gérer les transactions de leur population de 1,4 milliard d'habitants. Ils se montrent en revanche beaucoup plus réticents vis-à-vis de la cryptomonnaie qui s'apparente davantage, à leurs yeux, à un système pyramidal. Ils craignent que son usage ne déstabilise la population.

M. Philippe Latombe, rapporteur. Il me semble que l'Inde a fourni un énorme travail en vue d'identifier sa population à l'aide de solutions biométriques. Êtes-vous sollicités dans ce domaine aussi ?

M. Sébastien Dupont. Oui. En revanche, ce n'est pas l'Inde qui a fait appel à nous en matière de solutions biométriques, mais l'ONU, pour la gestion des réfugiés. Nous disposions déjà, sur le papier, d'un moyen rapide d'identifier les individus, sans risque pour leurs données privées, ni création de doublons. La prochaine étape du projet consistera dans le déploiement de notre *blockchain* couplée à notre dispositif biométrique.

M. Philippe Latombe, rapporteur. Revenons à votre plan de développement. Vous consommez pour l'instant votre trésorerie. Quand pensez-vous atteindre un équilibre de vos comptes ?

M. Sébastien Dupont. La conversion de nos cryptoactifs en euros nous permettra simplement de survivre. Nous espérons nous développer à partir de 2022. La mise au point de dispositifs biométriques s'avère particulièrement onéreuse. Nous chiffrons son coût, incompressible, à cinq millions d'euros. Son financement, même par les cryptomonnaies, s'annonce compliqué.

M. Philippe Latombe, rapporteur. Faut-il en conclure à une certaine frilosité des investisseurs par rapport à des technologies comme la *blockchain* ? Peinerez-vous à réunir les fonds nécessaires en France ?

M. Sébastien Dupont. Pour ne rien vous cacher, nous ne pensions pas recourir à l'émission d'actifs numériques (*Initial coin offering* ou *ICO*) mais nous autofinancer par des commandes. Seulement, l'officialisation du passage de commandes prend trop de temps. Durant la crise sanitaire, nous avons donc utilisé des *ICO*. Mon équipe et moi-même nous interrogeons actuellement sur l'opportunité de poursuivre notre développement en France, au regard des risques que cela implique. Lancer une *ICO* pour financer notre projet biométrique semble possible, mais une épée de Damoclès demeure suspendue au-dessus de nos têtes.

M. Philippe Latombe, rapporteur. Les GAFAM ou des fonds américains se poseraient-ils selon vous moins de questions ?

M. Sébastien Dupont. Évidemment, ils n'hésiteraient pas un instant, à condition de pouvoir récupérer ensuite la technologie développée au travers de nos projets.

M. Philippe Latombe, rapporteur. Les GAFAM vous ont-ils fait des propositions ? Vous avez mis au point une technologie de rupture qui présente de grands avantages écologiques, à même de faire la différence dans des politiques publiques, d'où votre attractivité technologique indéniable. Comment les GAFAM vous approchent-elles ?

M. Sébastien Dupont. Curieusement, nous avons été en relation avec PayPal. Je n'y vois pas de lien avec le gel de nos avoirs. PayPal est une société tentaculaire. Le département qui nous a contactés s'occupait d'investissement, de stratégie et d'innovation. Je ne crois pas à une collusion avec le service chargé de la gestion quotidienne des fonds. Le remplacement d'une carte bancaire par une empreinte digitale suffirait à changer la donne d'un point de vue stratégique.

Nous avons toutefois dès le début annoncé que tous nos brevets finiraient dans le domaine public en tant que bien commun numérique, ce qui nous rend incompatibles avec les GAFAM, puisqu'elles cherchent au contraire à s'assurer la mainmise sur des brevets pour en extraire le plus de revenus possible.

M. Philippe Latombe, rapporteur. Malgré tout, leur capacité à imposer rapidement de nouveaux usages les place en situation de quasi-monopole. Vos solutions technologiques ne pourraient-elles pas les intéresser, au moins pour leur usage ?

Gal Grégoire de Saint-Quentin. J'ai le sentiment que la technologie révolutionnaire que propose UNIRIS ne correspond pas du tout à l'optique des GAFAM, puisque la *blockchain* d'UNIRIS, parfait instrument du RGPD, amène *in fine* chacun à récupérer sa souveraineté sur ses données.

M. Philippe Latombe, rapporteur. Il faut donc défendre UNIRIS à tout prix.

Gal Grégoire de Saint-Quentin. Je le crois. Deux conceptions de la souveraineté s'emboîtent dans la technologie développée par UNIRIS. L'Europe entend par la première protéger ses citoyens. L'autre menacerait les intérêts de certains acteurs actuels du numérique. UNIRIS devrait bientôt mettre au point l'ossature de son nouveau protocole, ou *Mainnet,* d'ici à la fin de l'année. La *blockchain* publique qui en résultera deviendra à terme un bien public. M. Sébastien Dupont abandonnera ses brevets à une fondation d'utilité publique. Une telle démarche s'oppose diamétralement à celle de certains des GAFAM. Des applications monétisables pourront être construites à partir de cette ossature. En revanche, les données personnelles ne seront quant à elles plus monnayables.

M. Philippe Latombe, président et rapporteur. Souhaitez-vous porter à notre attention certains points particuliers ? Des problématiques périphériques vous viennent-elles à l'esprit, sur lesquelles nous pourrions agir ?

M. Sébastien Dupont. Nous avons la chance en France de disposer d'un système de recherche fantastique, auquel collabore un personnel, certes rémunéré, mais qui n'hésite pas à consacrer une part de son temps libre à l'amélioration de solutions. UNIRIS a bénéficié de la conjonction de tous les investissements réalisés en matière de recherche et de formation en France. Nous parvenons aujourd'hui à la limite du système.

Les cryptomonnaies ne sont pas toujours bien vues. Tout l'écosystème français s'est mis en branle pour que ce type de solution voie le jour. Toutefois, les entreprises qui les ont mises au point risquent de mourir si elles restent en France. La situation s'explique par nos traditions et je dirais même, par la Déclaration des droits de l'Homme. Elle nous empêche en

tout cas de concrétiser pleinement nos solutions dans notre écosystème, pour des raisons parfois peu compréhensibles du point de vue des entrepreneurs.

Gal Grégoire de Saint-Quentin. Je pense qu'il faut sortir de cette sorte de triangle des Bermudes. Le législateur, comme vous l'avez dit tout à l'heure, doit se pencher sur les moyens de rapprocher l'aspect légal et juridique de la *blockchain* de son versant mathématique.

Je comprends que les cryptoactifs véhiculent une image de spéculation. Il faut néanmoins les considérer comme un élément indispensable à la vie d'une entreprise, à l'instar des actions pour les sociétés cotées. Un important travail reste à mener afin de faire comprendre que les cryptomonnaies n'ont pas pour vocation de rivaliser avec les devises nationales. Elles sont émises en quantité limitée, comme les actions. Leur valeur découle de la nécessité de rémunérer ceux qui participent à la *blockchain*. UNIRIS s'est attachée à développer une *blockchain* perméable aux critiques qu'a suscitées le bitcoin.

M. Philippe Latombe, rapporteur. La souveraineté concerne l'État et les entreprises, mais aussi les citoyens. Comment acculturer ces derniers aux nouvelles technologies telles que la *blockchain* ? Quels conseils donneriez-vous ?

M. Sébastien Dupont. Peut-être pourrait-on commencer par expliquer la différence entre les logiciels propriétaires et *open source*. Nous devons tous nous demander à qui profite notre travail. Gmail propose une messagerie électronique gratuite, mais à quel prix ? Google revend nos données personnelles, privées. Certes, les outils marketing y gagnent en pertinence, mais les utilisateurs le payent.

Il n'y a rien de gratuit sur Internet. Un acteur du numérique proposant un service qu'il ne facture pas se rémunérera par un autre biais, de façon détournée. Une transaction sur une *blockchain* d'UNIRIS coûte moins de 20 centimes. Cette somme paye les mineurs qui la stockent et contribuent à sa validation. Aucun tiers n'intervient dans l'équation. Si tout le monde avait en tête que, selon la formule célèbre : « si c'est gratuit, c'est toi le produit », sans doute les risques de fuite des données des citoyens diminueraient-ils.

Gal Grégoire de Saint-Quentin. L'occasion se présente à nous de mettre en place des solutions prometteuses en accord avec nos valeurs européennes, face à des systèmes plus commerciaux ou fermés. La révolution de la *blockchain* représente un véritable tour de force. Bien qu'il reste encore beaucoup à accomplir, j'y vois des solutions potentielles à nombre de nos problèmes actuels. Longtemps en charge de questions de sécurité, j'estime que toute solution en mesure de remédier au déséquilibre des rapports de force sur Internet, qui n'offre aujourd'hui plus du tout un espace neutre, bénéficiera à la stabilité et à la sécurité de tous.

Audition commune, ouverte à la presse, de MM. Francesco Bonfiglio, directeur général, et Pierre Gronlier, directeur des technologies, de l'association internationale sans but lucratif GAIA-X et de Mme Marine de Sury, coordinatrice du French GAIA-X Hub
(22 avril 2021)

Présidence de M. Philippe Latombe, rapporteur.

M. Philippe Latombe, président et rapporteur. Cette audition s'inscrit dans notre réflexion relative à la souveraineté des données et à la nécessité de construire un écosystème européen du *cloud* conforme aux valeurs de l'Europe *via* la promotion de solutions interopérables, réversibles et sécurisées.

GAIA-X est une initiative européenne lancée en 2020. Elle rassemble plus de cent quatre-vingts entreprises privées avec pour objectif de proposer aux Européens une infrastructure et un cadre d'architecture sécurisés permettant de garantir une circulation maîtrisée des données. Cette initiative doit être abordée en lien avec le *Data Governance Act* proposé par la Commission européenne à la fin de l'année 2020.

Je souhaite que nos débats permettent d'aborder trois sujets. Le premier concerne votre définition de la souveraineté numérique et la manière dont elle est prise en compte dans l'initiative GAIA-X.

Je voudrais également que vous nous présentiez l'initiative GAIA-X en détaillant sa genèse, sa gouvernance et son actualité. Très concrètement, nous aimerions prendre connaissance des objectifs de GAIA-X et des jalons fixés pour sa mise en œuvre, mais aussi évoquer la doctrine de ce projet et les raisons pour lesquelles les *hyperscalers*, tels Amazon et Google, ont été conviés à y participer en tant que partenaires.

Enfin, j'aimerais savoir comment GAIA-X s'articule avec la démarche initiée par la Commission européenne dans le *Data Governance Act.* J'aimerais donc connaître votre approche du marché européen de la donnée et vos propositions concernant la manière dont nous devons agir pour trouver un équilibre entre l'innovation et la protection des données. L'accès aux données est un sujet essentiel pour assurer le développement de nombreuses technologies d'avenir, dont beaucoup s'appuient sur l'Intelligence artificielle.

M. Francesco Bonfiglio, directeur général de l'association internationale sans but lucratif GAIA-X. Votre première question concerne notre définition de la souveraineté numérique. Il s'agit d'une question très pertinente, posée par tous les acteurs. Ceci signifie qu'il existe de nombreuses interprétations concernant cette notion. Les choses sont très claires nous concernant. Nous parlons de souveraineté digitale, c'est-à-dire, en premier lieu, de la capacité à contrôler le stockage de nos données et leur exploitation, par qui, pour quel usage et de quelle manière. Cette notion renvoie également à notre capacité à reconquérir notre souveraineté en matière d'économie des données, notamment en matière d'échange des données.

M. Pierre Gronlier, directeur des technologies, de l'association internationale sans but lucratif GAIA-X. Je suis un ingénieur français ayant suivi un parcours académique dans le domaine du traitement du signal mathématique. J'ai successivement travaillé au sein de Microsoft et d'OVH avant de rejoindre depuis quelques semaines le projet GAIA-X, au sein duquel j'occupe le poste de directeur technique.

Six éléments permettent de définir le projet GAIA-X. Il s'agit tout d'abord d'un système dans lequel les différents acteurs, c'est-à-dire les citoyens, les entreprises, les autorités publiques et les États, peuvent contrôler la manière dont leurs données sont utilisées – ce qui renvoie à la notion de souveraineté numérique – et vérifier comment ces données peuvent être partagées et monétisées à travers un système d'infrastructures informatisées et fédérées.

Nous travaillons avec différents acteurs européens afin de réutiliser les services qu'ils ont déjà mis en place dans le cadre de directives européennes, par exemple en matière d'identité numérique et de *blockchain*. Notre démarche vise également à garantir le respect des valeurs européennes, à savoir la liberté, la démocratie ou encore l'État de droit.

Le troisième élément permettant de caractériser GAIA-X est la transparence, un sujet essentiel afin de garantir la souveraineté numérique. En effet, il convient d'être en mesure de préciser si une réglementation extraterritoriale non européenne peut impacter des données, des infrastructures ou des services. Cette notion renvoie également à la capacité de s'informer et d'être en mesure de garantir l'origine de l'information, à travers des certifications et des labels.

Le quatrième point correspond à la sécurité. En ce qui concerne les infrastructures et les technologies, GAIA-X vise à fixer des règles et proposer des composants garantissant un certain niveau de sécurité et de confidentialité. Entrent dans cette catégorie le *federated learning*, c'est-à-dire la capacité d'apprentissage fédérée et décentralisée, le *confidential computing*, c'est-à-dire les calculs sécurisés dans des enclaves physiques de processeurs, ou encore les *blockchains*, c'est-à-dire les consensus décentralisés, un sujet présenté ce matin à votre mission d'information.

Le cinquième élément porte sur la protection des droits, ce qui correspond à la souveraineté des individus et des organisations. Le terme de souveraineté doit alors être entendu comme la capacité à garantir l'autonomie stratégique de ses ressources, mais aussi comme la capacité à redonner confiance dans les outils numériques.

Enfin, sur la base des principes et des valeurs précédemment énoncés, GAIA-X vise à favoriser la création et la croissance des écosystèmes numériques de partage et de monétisation de la donnée, tout en s'assurant de l'interopérabilité, de la sécurité et de la transparence du dispositif. Ceci implique de favoriser le passage d'une gouvernance humaine à une gouvernance numérique, dans laquelle les algorithmes viennent supporter – et non remplacer – la partie légale. Cet élément a donc un impact réglementaire. Je pourrai illustrer mon propos ultérieurement au moyen d'exemples utilisateurs au sein de GAIA-X.

L'écosystème de GAIA-X, qui couvre un volet relatif à la gestion des données et un volet relatif à l'infrastructure, constitue un système autonome, au sein duquel les différents acteurs maîtrisent leurs interactions et savent comment leurs données sont utilisées. La brique des *federated services* constitue le moteur de cet écosystème. C'est à ce niveau que les *job providers*, c'est-à-dire les acteurs de la partie infrastructure, européens ou non européens, et les fournisseurs de données, là encore européens ou non européens, échangent.

La présentation des membres de GAIA-X permettra de répondre à la question relative aux *hyperscalers*. En effet, 95 % des deux cent douze membres récemment admis sont européens, et 70 % des membres sont des PME.

L'association GAIA-X repose sur une structure classique comprenant un conseil d'administration élu par une assemblée générale, un comité technique directeur – composé de M. Francesco Bonfiglio, de moi-même et d'autres directeurs prochainement désignés – un comité en charge de la *road map* technique et un comité en charge de la réglementation et de

la régulation. Ces comités sont assistés par des groupes de travail ouverts aux membres de l'association et au sein desquels sont élaborés les « délivrables » de GAIA-X.

La structure de GAIA-X repose sur l'association internationale sans but lucratif de droit belge GAIA-X (GAIA-X AISBL) et sur les différents *hubs* nationaux de GAIA-X, qui sont des incubateurs à projet nationaux. Enfin, la communauté de GAIA-X est ouverte à tous les contributeurs souhaitant être informés, observer et apprendre des travaux menés.

L'association GAIA-X a pour mission de produire trois types de « délivrables ». Le premier type correspond aux spécifications techniques permettant d'assurer la régulation et la gouvernance attendue. Le deuxième type correspond aux règles de politiques figurant dans des *policy rules documents* et permettant de traduire juridiquement les notions de souveraineté, d'autonomie et d'interopérabilité. Enfin, le troisième type correspond à une version *open source* et libre d'usage des *federated services*, un développement soutenu par des financements nationaux, actuellement français et allemands.

Un certain nombre de « délivrables » ont déjà été produits. Ainsi, le document d'architecture présenté en juin 2020 détaillait un potentiel schéma de fonctionnement de GAIA-X. Une version consolidée de ce document d'architecture a été présentée au cours du mois de mars 2021 et a permis de préciser le modèle fonctionnel de GAIA-X.

M. Francesco Bonfiglio. Nous sommes sur le point de créer un troisième comité intitulé *business and data spaces committee*. Il est important de préciser que, si GAIA-X AISBL constitue une association organisée de manière traditionnelle, avec une assemblée générale et un conseil d'administration, l'univers de GAIA-X correspond à la combinaison entre cette structure et sa communauté d'utilisateurs.

En parallèle, les premiers *hubs* GAIA-X nationaux ont été créés en France, en Allemagne, en Finlande, en Belgique et en Italie. D'autres vont être créés dans un proche avenir. Nous devrions disposer de seize *hubs* de ce type d'ici au mois de juin.

Il en résulte au final une communauté internationale regroupant une centaine de membres qui collaborent pour porter des projets dans leur domaine de prédilection et dans leurs pays respectifs. Ces programmes peuvent être portés dans de multiples domaines (santé, secteur public, agriculture...).

En revanche, GAIA-X n'est pas une instance normative. Certes, cette entité peut bien évidemment proposer aux décideurs des projets de règles et de normes, mais son activité première consiste à définir une nouvelle génération d'architecture de *cloud* et à la mettre en œuvre à travers des logiciels en *open source*. Nous rédigeons des codes qui nous permettront de créer cette couche d'intercommunication entre différentes sources informatiques dans un environnement souverain et sécurisé. Il s'agit d'une initiative sans précédent, dans la mesure où nous permettons à tous les membres de GAIA-X, ou à tout type d'acteur souhaitant y implémenter ses services, de bénéficier de cet environnement.

Par ailleurs, nous développons une collaboration très étroite avec les différents *hubs* nationaux, afin de prendre en compte les spécificités réglementaires et les exigences des différents pays, des éléments qui ne sont jamais pris en compte par les prestataires de service traditionnels dans le domaine du *cloud.* L'objectif est de permettre aux utilisateurs de renforcer leur capacité à adapter leurs données, afin de créer une communauté de données, de concevoir un nouveau système et de le mettre à disposition des utilisateurs.

GAIA-X n'est pas une société commerciale ou un prestataire de services commerciaux chargé de déployer des solutions. Nous souhaitons conserver notre autonomie et notre indépendance. Notre objectif est que tous les acteurs recourant aux services de GAIA-X mettent en œuvre et implémentent de manière autonome cette couche de *cloud* fédérée. Concrètement, GAIA-X restera la propriété des utilisateurs, afin de garantir la concurrence et l'ouverture du marché.

Pour répondre aux interrogations nées de la présence de membres non européens au sein de GAIA-X, je veux préciser que les statuts disposent que le conseil d'administration de GAIA-X AISBL peut uniquement accueillir des membres dont la société mère est implantée sur le territoire de l'Union européenne. En revanche, des entreprises de tous horizons peuvent nous rejoindre. Ceci explique pourquoi de grandes entreprises américaines et chinoises font partie du projet. Certes, l'opportunité de les accueillir a fait l'objet de débats. Cependant, j'ai estimé que réunir les meilleurs acteurs du marché du *cloud* constituait une opportunité extraordinaire, dès lors que la condition de base de leur participation est l'acceptation des valeurs que nous incarnons.

Par ailleurs, la participation de ces leaders mondiaux signifie que nous sommes potentiellement en train de changer les règles du jeu. Je ne veux pas entrer dans les détails techniques, mais il convient de rappeler que tous les *hyperscalers* fonctionnent sur la base d'un modèle reposant sur la concentration des données : plus les capacités de calcul sont importantes, plus les données captées sont nombreuses, plus les ressources technologiques sont concentrées, plus les services sont efficaces, compétitifs et rentables. Or ce modèle n'est pas le plus approprié pour gérer des données disséminées à travers le monde, un phénomène appelé le *far edge computing*.

En réalité, les données devraient être stockées et gérées au plus près de leur source, ce qui impose de développer un modèle horizontal et fédérateur. GAIA-X permet de construire un tel modèle auquel chacun devra se conformer. Avec ce projet, l'Europe dispose d'une chance de revenir dans la compétition avec les plus importants acteurs du marché. De ce fait, je pense sincèrement que le *cloud* aura profondément évolué dans quelques années.

M. Philippe Latombe, rapporteur. Votre présentation a permis d'expliquer la présence d'acteurs américains ou chinois dans GAIA-X. Je pense que cette intervention permettra de répondre aux nombreuses réticences exprimées en France à ce sujet.

En revanche, j'aimerais entendre votre réaction aux propos de plusieurs personnes auditionnées par notre mission d'information qui considéraient que l'avance prise par les Américains, en particulier par les GAFAM, était quasiment irrattrapable. Cette avance ne concerne pas la capacité à stocker des données, mais le volet relatif à l'Intelligence artificielle embarquée dans le *cloud*. Pensez-vous que GAIA-X permettra de rattraper ce retard ?

M. Pierre Gronlier. Les GAFAM ont effectivement pris une avance considérable. Cependant, nous disposons en Europe, et notamment en France, de nombreux savoir-faire. Ceci explique pourquoi de nombreux *spins-off* sont créés, par exemple au sein du commissariat à l'énergie atomique et aux énergies renouvelables (CEA). Malheureusement, dans la plupart des cas, ces derniers sont ensuite rachetés par les GAFAM.

L'Europe dispose donc des capacités intellectuelles et technologiques lui permettant d'innover et de créer de nouvelles façons de travailler à partir des données. Le projet GAIA-X vise à conserver ces projets en Europe.

M. Philippe Latombe, rapporteur. Pouvez-vous préciser l'objectif de GAIA-X en la matière ?

M. Pierre Gronlier. L'objectif de GAIA-X est de permettre à ces acteurs européens d'éclore en évitant qu'ils se tournent immédiatement vers les GAFAM afin de conquérir rapidement un marché. Il convient au contraire de les orienter vers des acteurs partageant un certain nombre de valeurs en matière de souveraineté, d'interopérabilité et de sécurité.

M. Francesco Bonfiglio. Bien évidemment, un projet visant à déployer une architecture comparable à celle d'acteurs tels Microsoft, Amazon ou Google serait voué à l'échec. D'ailleurs, nous ne pourrions pas consacrer les milliards de dollars investis par ces acteurs afin de disposer d'une technologie aussi sophistiquée.

Nous tentons donc de construire quelque chose de nouveau, à savoir une infrastructure capable de se connecter aux infrastructures existantes. Cette solution nous évitera de déployer notre propre technologie et nous permettra de rassembler des données permettant de créer un *cloud* encore plus vaste.

Par ailleurs, notre approche représente une alternative à la stratégie des *hyperscalers,* qui consiste à disposer d'un réseau sans cesse plus puissant et d'une bande passante leur permettant de stocker l'ensemble des données produites. Ces acteurs cherchent par ailleurs à conserver un point central d'analyse des données, afin de rentabiliser les investissements faramineux qu'ils ont réalisés. Cependant, cette démarche ne correspond pas à une approche évolutive. Au contraire, notre approche reposant sur la convergence permettra d'utiliser des données conservées dans de multiples endroits. La stratégie que nous portons sera ainsi moins énergivore, puisqu'elle permettra d'utiliser les données à proximité de leur source d'émission, sans avoir à les stocker à l'autre bout du monde.

L'approche de GAIA-X permettra par ailleurs de garantir la mise en œuvre d'une des valeurs les plus importantes pour les acteurs technologiques européens, à savoir la fourniture de services dans un cadre sécurisé et garantissant l'interopérabilité, la portabilité, la réversibilité, alors que les *hyperscalers* sont spécialisés dans la vente de services.

Mme Marine de Sury, coordinatrice du French GAIA-X Hub. Outre mes fonctions au sein du French GAIA-X Hub, je suis directrice de mission du Club informatique des grandes entreprises françaises (Cigref), une association représentant les plus grandes entreprises et administrations publiques françaises, exclusivement utilisatrices de services et solutions numériques, et ce dans tous types de secteurs d'activité. Depuis cinquante ans, le Cigref a pour mission de développer la capacité de ses membres à intégrer et maîtriser le numérique.

GAIA-X permet à des fournisseurs de solutions et de services de ne pas rester cantonnés à l'échelle nationale, mais de passer immédiatement à l'échelle européenne.

M. Philippe Latombe, rapporteur. Lors de nos précédentes auditions, la problématique les projets de mégaconstellations de fournisseurs d'Internet par satellite a été abordée. Comment GAIA-X a-t-il intégré cette problématique ? L'objectif sera-t-il simplement de disposer d'une bande passante plus rapide pour accéder au *cloud* ? Comment articuler les deux projets européens portés en parallèle ?

M. Pierre Gronlier. La problématique des mégaconstellations de fournisseurs d'Internet par satellite a été prise en compte dans GAIA-X à travers la notion d'*edge cloud*. Un satellite – tout comme une voiture, un train ou un bateau – peut être considéré comme une

unité de calcul qui peut être fédérée. Dans ce contexte, disposer d'une bande passante plus importante et d'une moindre latence permettra de construire de nouveaux scénarios de cas d'usage. Par ailleurs, GAIA-X représentera une offre complémentaire en termes de régulation.

M. Philippe Latombe, rapporteur. GAIA-X est un projet très innovant porté par l'Union européenne et décliné dans les *hubs* nationaux. Un projet comparable pourrait-il être adopté pour des problématiques du numérique autres que le *cloud* ? En cas de réponse positive, quelles problématiques pourraient-elles être traitées dans un projet et une gouvernance comparables à GAIA-X ?

M. Pierre Gronlier. D'une manière générale, la consommation de tous les services informatiques, dont le *cloud*, implique que l'utilisateur s'authentifie. Or la gestion de l'identité fait partie des problématiques prises en compte dans GAIA-X. Ainsi, les banques, ou les hôpitaux, doivent se conformer aux règles de KWC. Or il est actuellement très difficile en Europe de maîtriser trois briques de base en la matière, à savoir identifier une personne physique, identifier une personne morale et identifier le mandat d'une personne physique sur une personne morale.

En France, FranceConnect, qui constitue une déclinaison de la directive européenne eIDAS, commence à être utilisée. Cependant, ce type de solution est bien moins utilisé en France que dans d'autres pays, par exemple en Estonie. Ayant travaillé cinq ans dans ce pays, je sais que la puce équipant une carte d'identité estonienne permet d'accéder à l'ensemble des services de l'État estonien, à l'ensemble des services sociaux estoniens (assurance maladie, retraite...), mais aussi que de nombreux acteurs privés (banques, fournisseurs d'accès Internet...) peuvent s'y connecter. Ce schéma permet d'éviter de recourir à une multitude d'identifiants compliqués à fédérer.

Outre FranceConnect, il est possible de citer l'identité numérique obtenue en enregistrant une entreprise auprès d'un greffe de tribunal.

Le problème est qu'une telle gestion d'identités très parcellaires ne permet pas de passer à une plus vaste échelle. Les travaux menés dans GAIA-X devront prendre en compte cette difficulté.

La gestion des identités numériques des personnes physiques et morales constitue donc une autre problématique susceptible d'être traitée dans un cadre comparable à celui de GAIA-X. Par ailleurs, GAIA-X va s'appuyer sur les travaux relatifs aux *blockchains* réalisés dans le projet *European blockchain services infrastructures (EBSI)*.

Je souhaite enfin répondre à la question posée en introduction de cette audition concernant le *Data Governance Act*. Ce projet prévoit notamment d'imposer à certains organismes de partager leurs données. Un tel schéma a d'ailleurs déjà été mis en œuvre dans la directive sur les services de paiement bancaires (DSP2), avec un succès limité. En effet, en l'absence de base contractuelle et de rémunération, les banques acceptent uniquement de partager les données de leurs clients relatives aux comptes courants, et non aux comptes de dépôts. L'obligation réglementaire a donc conduit à partager des données parcellaires difficilement utilisables, par exemple, pour détecter du blanchiment d'argent. Le *Data Governance Act* constitue donc un élément positif, mais il conviendra de se doter en complément d'un cadre réglementaire plus général.

M. Philippe Latombe, rapporteur. Dans quelle mesure GAIA-X contribuera-t-il à trouver un équilibre entre l'innovation et la protection des données ?

M. Pierre Gronlier. GAIA-X comprend un *data space* franco-germanique dédié à la finance. L'objectif consiste à utiliser de nouveaux algorithmes permettant de passer d'une gouvernance humaine à une gouvernance numérique. Cependant, si les banques sont prêtes à mutualiser leurs efforts afin de limiter le blanchiment d'argent en Europe, elles s'opposent à ce que cette démarche leur impose de communiquer des données dont elles perdraient le contrôle.

Dans ce contexte, il serait nécessaire de disposer d'algorithmes de *federated learning* permettant d'entraîner un modèle au sein de chaque banque, puis d'agréger dans un modèle mutualisé les différents modèles entraînés dans les différentes banques. Cette démarche permettrait de détecter des opérations de blanchiment d'argent tout en garantissant aux banques que leurs données ne seraient pas exportées. Il s'agit clairement d'une demande du secteur *data space finance*.

Mme Marine de Sury. Nous retrouvons une demande comparable du groupe de travail français consacré à la santé. J'appuie donc les propos de M. Pierre Gronlier concernant la nécessité d'évoluer vers une gouvernance numérique, mais j'ajoute qu'il convient, en parallèle, de prévoir des mécanismes contractuels permettant de rémunérer l'utilisation de certaines données. En effet, les acteurs impliqués dans le traitement des données ne sont pas des sociétés philanthropiques. Leur objectif consiste bien à créer de la valeur, même s'ils ne sont pas opposés à la diffusion de données ouvertes dans un souci de bien commun.

Je précise que les acteurs participant aux groupes de travail du French GAIA-X Hub sont des entreprises, mais aussi des instituts de recherche ou des administrations publiques.

M. Philippe Latombe, rapporteur. GAIA-X est une initiative européenne ayant des déclinaisons nationales. Actuellement, quel est le rôle de l'Union européenne dans le domaine de la souveraineté numérique ? Est-ce la bonne et la seule échelle pour traiter cette question de souveraineté et ensuite la diffuser au niveau national ? À l'inverse, des initiatives peuvent-elles ou doivent-elles être initiées au niveau national avant d'être portées au niveau européen ?

Mme Marine de Sury. Le Cigref représente un certain nombre d'utilisateurs désireux de travailler en amont sur des questions de souveraineté, notamment en ce qui concerne le *cloud* de confiance, ou encore les critères de la souveraineté numérique, afin de partager le fruit de leurs réflexions. Ainsi, nous avons transmis différents courriers à MM. Bruno Le Maire et Cédric O, afin de les informer de l'état d'avancement de nos travaux concernant les sujets qui intéressent l'État. Les acteurs nationaux peuvent donc porter des initiatives, à condition que la démarche s'inscrive en convergence.

M. Pierre Gronlier. Je ne peux qu'appuyer ces propos. Bien évidemment, les approches européennes et nationales doivent être complémentaires. C'est bien dans cette logique que fonctionne GAIA-X : l'association GAIA-X fixe les grandes lignes directrices, mais tous les membres, ainsi que les non-membres, contribuent à la démarche. Les deux types d'action sont nécessaires et doivent converger.

Ainsi, disposer d'un dispositif homogénéisé serait très utile concernant la gestion de l'identité et les normes permettant de définir un contrat. Le cas d'espèce mis en avant dans le cadre du *Data Space Industry* correspond à la situation d'un sous-traitant automobile dont les productions sont assemblées par des constructeurs automobiles. En l'état actuel, le constructeur automobile ne dispose d'aucun retour d'information pour savoir si le composant fourni par le sous-traitant doit être remplacé par un garagiste après un certain nombre de kilomètres. Plus précisément, l'information relative au taux de panne d'un composant implanté dans un type de véhicule à un certain kilométrage existe, mais n'est pas monétisée.

Certes, un constructeur peut parfaitement conclure un contrat avec quelques concessionnaires afin de collecter ce type d'informations, mais il serait bien plus intéressant pour lui d'automatiser ce dispositif auprès des centaines de milliers de garagistes opérant en Europe. Cette démarche implique de disposer d'une réglementation européenne, au besoin d'une réglementation nationale, permettant d'harmoniser les accords.

M. Philippe Latombe, rapporteur. En quoi l'association GAIA-X peut-elle contribuer à cette harmonisation ? Une telle démarche figure-t-elle dans le cahier des charges de GAIA-X ? Existe-t-il un canal officiel lui permettant de proposer ce type d'harmonisation au Parlement européen ou à la Commission européenne ?

M. Pierre Gronlier. Certains canaux de communication permettent effectivement de faire part de ce type de besoin. À titre personnel, je suis en contact avec la DG Connect et nous vérifions si les dispositifs existants concernant la thématique des *blockchains* ou la directive européenne eIDAS peuvent nous être utiles.

M. Philippe Latombe, rapporteur. GAIA-X est un projet d'initiative européenne. Tous les pays de l'Union sont-ils impliqués de manière identique dans ce projet ? Je précise que ma question ne vise pas à identifier les bons et les mauvais élèves, mais à vérifier si cette thématique de souveraineté numérique est partagée par tous les États, et si la prise de décision à l'unanimité en Europe pose problème pour porter ce type d'initiative.

M. Pierre Gronlier. Je ne pense pas que cette caractéristique pose problème. La meilleure preuve est que, alors que le projet résulte d'une initiative franco-allemande et que les principaux participants proviennent actuellement de ces deux pays, nous comptons de nombreux contributeurs provenant d'autres pays, dont l'Espagne et l'Italie, et que des *hubs* nationaux créés en Estonie, en Finlande, en Suède, rejoignent le processus.

Mme Marine de Sury. À ce sujet, j'ai été contactée par les acteurs de différents pays souhaitant s'informer de la manière de construire et animer des *hubs* nationaux. Par ailleurs, des réunions sont régulièrement organisées entre représentants des différents *hubs* nationaux afin de présenter les organisations déployées dans les pays ayant initié la démarche et de vérifier comment des acteurs d'autres pays pourraient se saisir de certaines thématiques. Ces échanges sont pour l'instant très fluides et visent à contribuer au succès de la feuille de route assignée à GAIA-X.

M. Francesco Bonfiglio. J'aimerais revenir sur certains sujets déjà évoqués. En premier lieu, je confirme que le réseau de *hubs* nationaux est une initiative très importante. Ce réseau s'avère extrêmement efficace. La prochaine assemblée générale de GAIA-X AISBL programmée le 7 juin 2021 permettra de désigner de nouveaux membres du conseil d'administration, qui pour l'instant comprend uniquement onze Français et onze Allemands. Nous pourrons ainsi élargir l'éventail des nationalités représentées et intégrer un certain nombre de nos partenaires.

Je tiens par ailleurs à assurer que tous les pays membres de l'Union européenne ont exprimé leur intérêt pour la démarche portée par GAIA-X. Par ailleurs, depuis le lancement de la stratégie en 2020, l'Europe s'est dotée d'un fonds de relance de 750 milliards d'euros. Ceci signifie que les fonds susceptibles d'être mobilisés proviennent de différentes sources, et non plus uniquement de la Commission européenne. Dans ce contexte, il nous revient d'inciter les autorités nationales à utiliser ces ressources de manière cohérente, afin de garantir que les projets portés respectent les principes européens et les objectifs de GAIA-X.

Ainsi, lorsque la Commission européenne a porté l'initiative *European alliance for industrial data and cloud*, nous nous sommes, dans un premier temps, demandés si cette démarche concurrençait GAIA-X. En réalité, nous avons rapidement compris que GAIA-X allait jouer un rôle moteur dans cette alliance. Nous avons donc rejoint ce projet afin d'instaurer une nouvelle infrastructure.

Nous observons la multiplication des synergies avec les gouvernements nationaux, alors qu'au minimum 20 % des fonds octroyés dans le plan de relance devront être investis dans des projets en lien avec la transformation numérique. Nous travaillons donc avec la Commission européenne et les gouvernements nationaux dans des appels à projets consacrés aux données et à la souveraineté numérique. Par ailleurs, un nombre croissant de gouvernements nationaux ont participé à la création de réseaux nationaux.

Enfin, je tiens à souligner que nous assistons peut-être à un évènement qui ne s'est jamais produit par le passé. Tout d'abord, GAIA-X a permis de rassembler en moins d'un an une cinquantaine d'acteurs, à savoir des utilisateurs de données et de technologie et des fournisseurs de technologie, autour d'un objectif commun de partage des données et de création de valeur dans un environnement sécurisé.

Par ailleurs, alors que nous pouvions nous demander pourquoi l'économie numérique n'avait pas encore connu une croissance exponentielle, alors qu'existaient des mesures d'incitation, la pandémie que nous venons de vivre a permis à chacun de découvrir que le partage des données était un secteur crucial. En effet, sans partage de données, il aurait été impossible de continuer à enseigner aux enfants, de travailler à distance, d'acheter de la nourriture et de poursuivre les activités économiques durant le confinement. Par ailleurs, le projet de passeport sanitaire est un exemple de collaboration entre acteurs publics et privés en matière de partage de données. Il s'agit d'un projet très concret pour les citoyens. C'est pourquoi je pense que nous nous trouvons à la croisée des chemins et que nous comprenons mieux que jamais que nous avons intérêt à améliorer le partage de données et à créer des réseaux permettant d'échanger des données.

Mme Marine de Sury. Les entreprises souhaitent que les données puissent circuler, mais pas à n'importe quel prix. Elles voient en GAIA-X l'architecture et l'infrastructure permettant de garantir une circulation maîtrisée de ces données, dès lors que les *policy rules* permettent de garantir l'ouverture, l'opérabilité, la transparence, la confiance, la réversibilité, la portabilité, sans être soumis à des lois extraterritoriales.

M. Philippe Latombe, rapporteur. La nomination des responsables de GAIA-X est très récente. À quelle date GAIA-X atteindra-t-il sa vitesse de croisière ? À quelle date les entreprises pourront-elles faire appel à ses solutions ? À quel moment estimerez-vous avoir atteint les objectifs assignés ?

M. Francesco Bonfiglio. Deux éléments permettent de caractériser le projet de transformation numérique.

La première caractéristique est que seuls les meilleurs réussiront et que les autres échoueront, sans qu'il existe une voie intermédiaire. Dans ce contexte, nous devons avoir les bonnes idées au bon moment. Or GAIA-X semble constituer cette bonne idée au moment opportun.

Par ailleurs, nous assistons à l'explosion des projets de transformation numérique, mais, par nature, ces projets ne connaissent pas un développement linéaire, mois après mois et année après année. Leur croissance s'apparente en général à une courbe en « crosse de

hockey », c'est-à-dire que les résultats progressent fortement seulement après une longue période préparatoire. GAIA-X connaît actuellement cette phase préparatoire et le travail à réaliser est encore conséquent.

Ainsi, en 2021, nous devons choisir un ensemble de projets qui nous permettront de concrétiser les concepts que nous avons élaborés, à savoir la fédération de service au plus petit niveau, mais aussi les différents composants de l'architecture de GAIA-X (autocertification, autodéfinition, autocontrôle...), qui n'ont jamais été développés par le passé. Nous espérons enregistrer des résultats tangibles dans ces différents chantiers dès la fin de l'année 2021, en nous appuyant sur les travaux de *start-up* d'excellent niveau.

Sur cette base, j'espère que les premiers bouquets de services portés par GAIA-X pourront être proposés dès 2022, par exemple, dans le domaine de la santé ou de la finance. Nous assisterons ensuite à l'avènement de services d'intermédiation transversaux couvrant plusieurs domaines d'activité.

Au cours de la troisième année, si les objectifs assignés ont été atteints, au moins 20 % des membres de GAIA-X développeront des services répondant à nos critères, ce qui permettra de passer un cap et d'enregistrer une forte croissance des projets de ce type. Dans la mesure où GAIA-X devrait à cette date compter plusieurs centaines de membres, la dynamique engagée permettra alors de peser suffisamment en Europe et au-delà. Nous assisterons alors à l'apothéose, à savoir la création d'un système de vente de services par les différents membres de GAIA-X et par l'ensemble des utilisateurs ayant adopté ce système.

Enfin, j'espère que nous serons en mesure d'enregistrer des économies d'échelle entre la troisième et la cinquième année, afin de rendre GAIA-X compétitif sur la scène internationale et de ne plus être considéré commune une simple alternative européenne.

M. Philippe Latombe, rapporteur. La feuille de route est très claire, mais très ambitieuse. Quels indicateurs vous permettront de mesurer l'atteinte de vos objectifs ?

M. Francesco Bonfiglio. La réponse est assez simple, car désormais nous pouvons présenter GAIA-X comme une alternative aux *hyperscalers*. Je précise que notre démarche ne vise pas à nous opposer à qui que ce soit, nous proposons simplement une solution alternative inclusive.

Actuellement, le taux de pénétration du *cloud* dans les différents pays européens est compris entre 20 % et 25 %. Concrètement, entre 20 % et 25 % des entreprises européennes adoptent la technologie du *cloud*, qui couvre trois catégories : les infrastructures en tant que service, les plates-formes en tant que service, et les logiciels en tant que service. Cependant, le taux de pénétration du *cloud* est très inférieur à 15 % concernant les infrastructures en tant que service. Ce taux doit progresser. Il convient néanmoins de préciser que la situation actuelle s'explique uniquement par un manque de confiance dans les solutions proposées, en particulier en raison des risques de verrouillage des données par certains fournisseurs. Or il est anormal que les consommateurs soient pénalisés par de telles stratégies commerciales.

Dans ce contexte, le succès de GAIA-X se mesurera en fonction de la progression du taux de pénétration du *cloud*. En effet, si GAIA-X est en mesure d'assurer l'interopérabilité, la migration d'une plate-forme à une autre, la souveraineté, la transparence, je suis persuadé que de nombreux acteurs adopteront alors la technologie du *cloud*, car un tel schéma leur permettra de réduire les coûts de gestion de leurs infrastructures. Or je veux insister sur le fait que, à l'heure actuelle, aucun projet autre que GAIA-X n'a pour objectif de garantir la migration d'une plate-forme à une autre et d'un fournisseur à un autre de manière sécurisée.

M. Philippe Latombe, rapporteur. Au-delà de l'identité numérique, l'Europe devrait-elle investir immédiatement d'autres domaines techniques pour protéger sa souveraineté numérique, sous peine d'être à nouveau en retard ? Disposons-nous de secteurs d'excellence pour conserver nos talents ?

M. Francesco Bonfiglio. Il existe de nombreux domaines d'excellence. Le premier que je souhaite évoquer correspond à l'Intelligence artificielle. Vous pourriez rétorquer qu'il ne s'agit pas vraiment d'un domaine, mais cela l'est. Il s'agit en réalité du domaine des domaines. Or dans les prochaines années, nous serons submergés de services reposant principalement sur l'Intelligence artificielle. Cependant, au même titre que la plomberie transporte l'eau, l'Intelligence artificielle a besoin de données, et surtout de données de qualité.

Or, grâce à son héritage industriel, à son modèle social, à son modèle environnemental, et dans la mesure où les données ne sont que les représentations de ces écosystèmes, l'Europe dispose des meilleures données au monde. Nous avons donc la possibilité d'entraîner la prochaine génération de *smart services* reposant sur l'Intelligence artificielle à partir de nos données européennes et de construire ainsi les algorithmes des sites de *e-commerce* permettant de créer le plus de valeur.

M. Pierre Gronlier indiquait au cours d'une de ses interventions que l'Europe avait vu l'éclosion des meilleures technologies et des meilleures *start-up*, qui malheureusement ont dans la plupart des cas été rapidement rachetées par les GAFA. La solution pour ne pas perdre cette richesse est de construire quelque chose de plus grand. GAIA-X se propose d'être le cadre permettant de conserver cette richesse en Europe.

M. Pierre Gronlier. Je tiens à compléter ces propos afin de répondre à la question relative aux domaines d'expertise qu'il conviendrait de protéger en Europe. Pour se faire, je rappelle qu'en matière d'Intelligence artificielle, la pertinence du modèle dépend uniquement de la qualité des données utilisées. En effet, un modèle entraîné sur la base d'un jeu de données contenant trop de données biaisées et non nettoyées, par exemple des données dupliquées ou dont certains champs ne sont pas renseignés, ne sera pas pertinent. L'intérêt de GAIA-X est qu'il permet de garantir un partage de données de plus en plus pertinentes.

M. Philippe Latombe, rapporteur. Plus précisément, quels domaines technologiques doivent immédiatement bénéficier d'investissements ? Alors que la France a lancé un plan quantique, des investissements doivent-ils être immédiatement portés dans ce domaine au niveau européen, ou dans les différents pays avant de fédérer les démarches au niveau européen ? Identifiez-vous des secteurs technologiques que l'Europe a ignorés, mais pour lesquels d'autres pays ont consacré un effort de recherche ?

M. Pierre Gronlier. Je ne me prononcerai pas concernant la technologie quantique, qui est très prometteuse. Je sais simplement qu'il existe des *start-up* très prometteuses en France dans ce domaine, par exemple la *start-up* Pasqal. Par ailleurs, l'entreprise française LightOn fait partie des cinq entreprises au monde capable de réaliser du calcul photonique. Cette compétence est utilisée afin de réaliser des calculs d'approximation de poids sur la base de lasers. La technologie utilisée consiste à diffuser des photons à travers des lentilles, ce qui est plus rapide et moins consommateur d'énergie qu'utiliser des électrons sur des pistes de cuivre.

Il est bien évidemment nécessaire de conserver ces talents en Europe, et donc d'investir dans ces secteurs. Le problème est que ces investissements seront utiles uniquement si la réglementation évolue afin de permettre à des acteurs économiques de s'en emparer. À titre

d'exemple, l'Europe doit être en mesure de se doter un *corpus* juridique permettant d'encadrer les transactions en cryptomonnaies.

M. Philippe Latombe, rapporteur. Nous avons évoqué ce sujet dans notre précédente audition et nous l'évoquerons à nouveau la semaine prochaine.

Avant de clore nos débats, quel dernier message aimeriez-vous faire passer aux députés et aux personnes visionnant cette audition concernant les thématiques du *cloud* et de la souveraineté numérique ? Qu'attendez-vous de nous ?

M. Francesco Bonfiglio. Je n'attends rien, je n'exige rien, mais j'espère beaucoup. J'espère que nous avons été clairs dans notre présentation de GAIA-X. J'espère plus généralement que, en Europe, chacun comprendra l'intérêt de cette initiative unique et sans précédent, qui est portée dans l'intérêt de tous les Européens, qu'il s'agisse des entreprises, du secteur public et, surtout, des citoyens. J'espère surtout que GAIA-X ne sera pas perçu comme une initiative intéressante, mais sans postérité. En effet, notre objectif est d'aller au bout de ce projet pour changer la donne.

Dans la Rome antique, l'accès à l'eau était considéré comme un bien commun. Chacun avait accès gratuitement à une eau potable. Il s'agissait d'une grande nouveauté. En ce qui nous concerne, nous accordons un accès gratuit à nos données et nous avons la chance de disposer d'un énorme stock de données. Cependant, en considération de la pandémie que nous subissons depuis treize mois, nous devons nous imaginer ce que serait un monde dans lequel les citoyens n'auraient aucun contrôle de leurs données personnelles et des outils permettant de communiquer, de voyager, de se rencontrer, ou encore d'acheter des biens. En réalité, à l'image de l'eau, ces données sont désormais vitales en Europe. C'est pourquoi j'espère que notre projet ne restera pas expérimental, mais au contraire bénéficiera à chacun, grâce à la contribution des différents acteurs.

M. Pierre Gronlier. Pour ma part, je veux insister sur la réglementation à déployer afin de développer, ou de retrouver, la confiance dans les outils numériques. Cette démarche est indispensable pour passer d'une gouvernance humaine à une gouvernance numérique, qui est la condition *sine qua non* d'une démarche visant à fédérer les efforts réalisés dans les différents pays pour instituer une cohérence européenne.

Afin d'illustrer mon propos, je vais citer un exemple de gouvernance numérique : le cadenas vert apparaissant sur le site Internet de votre banque constitue non seulement un indicateur de votre confiance dans la banque, mais aussi un indicateur de votre confiance dans le certificat délivré par l'autorité compétente qui a audité la banque. En l'occurrence, l'intervention humaine est limitée à la délivrance du certificat, mais la confiance est ensuite assurée dans une gouvernance numérique.

M. Philippe Latombe, rapporteur. Je vous remercie. Je confirme qu'il convient de promouvoir la confiance dans la gouvernance numérique.

Mme Marine de Sury. Ma demande est comparable à celle exprimée par M. Francesco Bonfiglio concernant la constitution d'un environnement capable d'imposer aux fournisseurs de *clouds* et de services numériques de proposer des offres conformes aux valeurs européennes et aux attentes de nos entreprises. Nous devons faire en sorte que les *hyperscalers* américains et asiatiques se conforment aux règles du jeu et aux valeurs européennes. Dans ce but, tout doit être fait pour garantir le succès de GAIA-X, car il sera ensuite trop tard pour agir.

M. Philippe Latombe, rapporteur. Je vous remercie pour vos interventions, pour la clarté de vos propos. Cette présentation était importante, car le projet GAIA-X a suscité beaucoup d'espoirs, mais aussi un certain nombre d'interrogations du fait de la participation des principaux acteurs américains du numérique. Votre présentation a permis de clarifier le mode de fonctionnement de GAIA-X et les objectifs du projet.

Les personnes qui ont précédemment été auditionnées dans notre mission d'information placent leurs espoirs dans GAIA-X. Il était donc important de vous permettre de présenter ce projet et de l'incarner devant nous.

Audition, ouverte à la presse, de M. Simon Polrot, président, et Mme Faustine Fleuret, directrice stratégique et relations institutionnelles, de l'association pour le développement des actifs numériques (ADAN)
(27 avril 2021)

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. L'ADAN (association pour le développement des actifs numériques) est une association professionnelle, créée en 2020, qui vise à fédérer les acteurs du secteur des crypto-actifs et de la *blockchain* pour faire de la France et de l'Europe des leaders dans ce domaine. Il nous a semblé important de vous entendre alors que nous cherchons à approfondir le sujet de la *blockchain* sous le prisme de la souveraineté numérique. Nous avons auditionné la semaine dernière la fédération française des professionnels de la *blockchain*, et nous nous réjouissons de vous entendre aujourd'hui.

M. Philippe Latombe, rapporteur. Je souhaiterais évoquer avec vous trois sujets liminaires. Le premier concerne votre approche de la notion de souveraineté numérique. Il s'agit d'une question rituelle de cette mission, qui procède de la grande diversité des définitions existantes. J'aimerais savoir, d'une part, comment vous définissez cette notion, et d'autre part, comment la *blockchain* peut être un levier de souveraineté pour la France et l'Europe. À cette occasion, j'aimerais que vous nous rappeliez en quelques mots le principe de cette technologie, ses cas d'usage et son niveau de maturité, puisque cette audition est publique et ouverte à toutes les personnes pouvant s'intéresser à ce sujet.

Mon deuxième point porte sur le développement en France d'un écosystème *blockchain* performant. En un sens, c'est l'objet de votre association : rassembler et professionnaliser un secteur technologique en cours de construction. Comment jugez-vous l'action des pouvoirs publics dans ce domaine, alors qu'une stratégie nationale *blockchain* a été lancée à l'initiative du gouvernement et des acteurs de votre secteur ? Où en sommes-nous de cette stratégie aujourd'hui et quelles sont vos attentes ? J'aimerais, enfin, que vous évoquiez le sujet des crypto-actifs pour connaître le cas échéant vos propositions concernant l'évolution de leur réglementation.

Enfin, je souhaiterais que nous échangions sur la dimension européenne de la *blockchain* et des actifs numériques. Comment la France se situe-t-elle par rapport à ses voisins européens dans ce domaine ? Que pensez-vous de l'action de l'Union européenne en la matière ? Ceci nous permettra d'évoquer au passage l'enjeu de la force probante de la *blockchain*, qui est une question juridique importante, pour laquelle le législateur doit se mobiliser.

M. Simon Polrot, président de l'association pour le développement des actifs numériques (ADAN). Notre association compte à peu près soixante-dix membres, tous dans le domaine des crypto-actifs. Nous avons donc un angle particulier, autour de la représentation de valeurs sur la *blockchain*. C'est le domaine dans lequel nous constatons le développement d'une réelle industrie *ad hoc*, avec beaucoup d'enjeux liés au développement économique, à la compétitivité de la France et à la souveraineté. Nous souhaitons que la France devienne un acteur très compétitif dans le domaine des crypto-actifs – domaine qui est en train de se développer de façon exponentielle depuis maintenant quelques années. Nous en parlons beaucoup en ce moment, mais c'est le résultat de nombreuses années de travail.

La souveraineté dans le domaine du numérique, et plus particulièrement dans celui des crypto-actifs, peut se définir comme la maîtrise par la France de son destin à l'heure du numérique, ce qui suppose de garder une forme de contrôle, de comprendre et d'anticiper les enjeux (et d'abord les enjeux numériques mondiaux), de construire une position stratégique permettant d'assurer la compétitivité économique de la France ainsi que la liberté et la sécurité des citoyens dans le cyberespace, c'est-à-dire dans l'espace numérique dans lequel citoyens et entreprises interagissent. Avoir une souveraineté numérique, c'est, à la fois, en tant qu'État, assurer une compréhension et une présence, et assurer aussi à ses citoyens une forme de protection et de liberté dans ce monde numérique.

Dans le domaine des crypto-actifs, et de la valeur numérique en particulier, les grands enjeux de souveraineté sont :

– la connaissance des technologies et des usages par les différents services de l'État, une maîtrise qui permet ensuite d'agir ;

– l'existence, l'émission d'une ou plusieurs valeurs souveraines (c'est toute la question de l'euro numérique, sous différentes formes de représentation) ;

– le déploiement d'outils publics à destination des citoyens et des entreprises sur ces réseaux publics que constituent les *blockchains*, qui sont un peu similaires à Internet ;

– et une régulation adaptée des usages, qui permet une protection et favorise l'innovation sur ces réseaux.

Les crypto-actifs présentent des intérêts intrinsèques du fait de leur sous-jacent technologique. Ils sont à la fois traçables, transparents, « auditables ». Il est possible d'automatiser leur transfert *via* les *smart contracts*. Il existe des enjeux de liquidité. D'autres États ont pris la mesure des avantages de ces crypto-actifs dans le système économique, et sont en train d'inciter très fortement au développement de ces cas d'usage. Il existe donc un enjeu de compétitivité lié à ces actifs. Dans une vision souveraine de ces actifs, il convient de les évaluer de façon experte, compte tenu des différentes caractéristiques qui peuvent varier selon la technologie, les niveaux de décentralisation du protocole, les règles de confidentialité, de gouvernance, de résilience, etc.

Il est très important de ne pas confondre souveraineté et technologie nationale. J'y reviens dans le contexte d'une technologie de rupture comme les crypto-actifs, en faisant le parallèle avec Internet. L'erreur qui a été faite en France fut de vouloir recréer un Internet national, de faire une version centralisée et française d'un réseau public d'échanges de données, et donc de créer le Minitel, ce qui était une mauvaise stratégie à long terme, puisque Internet a pris le dessus et que nous ne nous y sommes pas positionnés en tant que fournisseurs de cas d'usage – pas suffisamment tôt, en tout cas, et pas suffisamment fortement.

Dans le numérique, nous accusons aujourd'hui un retard sous différents aspects. Notre message consiste à dire que la *blockchain* est un peu comme Internet, mais pour la valeur. Ce sont des réseaux publics, accessibles, ouverts, *open source*. La tentation de créer une *blockchain* française, selon nous, est mauvaise. Nous avons déjà des réseaux qui fonctionnent et qui sont plus ou moins résilients en fonction de leurs différentes caractéristiques. Il existe un enjeu de maîtrise, mais il convient aussi de ne pas « réinventer la roue ». Utiliser les réseaux ouverts qui existent et déployer des cas d'usage sur ces réseaux nous semble être la meilleure façon de contribuer et de fournir aux citoyens des services qui leur sont réellement utiles, puisque c'est là que se situent l'attraction et l'activité économique dans ce secteur. Les *blockchains* publiques existantes (Bitcoin, Ethereum, Tezos, Cosmos, Volcano) doivent être

regardées. Parler de *blockchain* nationale, à ce niveau-là, n'a pas vraiment de sens. La souveraineté sur les réseaux publics comme Internet ou les *blockchains* passe essentiellement par le développement de cas d'usage, la maîtrise des technologies et des réseaux existants, de leur gouvernance, et non par la création d'un nouveau réseau français. Ce serait mal diriger les efforts que de vouloir diriger un équivalent franco-français des réseaux publics qui existent aujourd'hui.

S'agissant des actifs, en revanche, les enjeux ne sont pas les mêmes. Quand on a des actifs qui sont émis par des personnes, il est important d'avoir une certaine maîtrise sur eux, et notamment de posséder des actifs souverains (l'euro numérique, par exemple). Cela fait partie des enjeux très importants en matière de représentation de valeurs. La recommandation générale est d'envahir ces réseaux plutôt que d'en créer de nouveaux.

Mme Faustine Fleuret, directrice stratégique et relations institutionnelles de l'ADAN. Les technologies *blockchains* sont un ensemble très vaste de technologies, avec des caractéristiques de décentralisation des règles de protocole qui peuvent être très différentes d'une *blockchain* à l'autre. Cependant, il existe des caractéristiques communes et intéressantes, notamment quant à la souveraineté numérique : la transparence, la traçabilité, l'auditabilité, qui est un aspect souvent méconnu et mal interprété de ce que sont les *blockchains* et les transactions sur crypto-actifs. Il est très facile de retracer les parcours des crypto-actifs sur les *blockchains* et d'arriver à auditer facilement ces transactions. L'automatisation par les *smart contracts* permet aussi, de façon très intéressante, de conditionner ce que peuvent être ces transferts dans le cas de politiques liées à des cas d'usage, mais aussi dans le cas d'une réglementation, ce qui apporte une sécurité juridique supplémentaire, grâce à la technologie.

La technologie – la façon dont sont réalisés les transferts et les transactions, la possibilité de pouvoir fractionner les actifs – apporte une certaine liquidité. Le fait que l'accès à ces actifs soit également facilité par la technologie apporte une profondeur de marché à ces crypto-actifs, qui peut parfois manquer pour certains instruments, dans le monde financier traditionnel.

L'industrie française s'est déjà très bien saisie de ces caractéristiques pour essayer de développer des cas d'usage des entreprises. Aujourd'hui, l'écosystème français des crypto-actifs se compose de 150 à 200 entreprises spécialisées dans ce domaine. Notre association compte une soixantaine de membres actifs, dont l'activité principale est liée aux crypto-actifs, tandis que d'autres membres s'y intéressent de façon périphérique. Ces soixante membres actifs représentent environ un tiers de l'écosystème global. Leur relative jeunesse et leurs effectifs relativement réduits constituent la caractéristique commune aux entreprises dont l'activité principale est liée aux *start-up* – on parle plus souvent de TPE, et un peu de PME. Cet écosystème est donc en maturation.

Si je dois donner quelques exemples de membres de l'ADAN et des activités que représente l'écosystème des crypto-actifs en France, ce sont bien sûr des conservateurs, des plateformes d'échange, des fournisseurs de liquidités pour ces plateformes, sur l'aspect plutôt financier, en soutien technologique des fournisseurs de solutions technologiques, d'informations, mais aussi de services de ménage que l'on voit se développer, et des produits basés sur la *blockchain*, mais pas nécessairement financiers, comme le transfert de capacités de calcul et de stockage grâce à la *blockchain*.

Nous représentons cette industrie assez hétérogène. Si l'on doit la comparer avec l'industrie américaine, nous sommes en retard de quelques cycles de marché, ce qui s'explique principalement par le fait qu'en termes de financement, il existe une énorme différence entre

ce qui se passe aux États-Unis, avec une structure de financement largement occupée par les marchés, et ce qui se passe en France et en Europe, où le financement bancaire prévaut. Finalement, ce financement est beaucoup plus important dans l'industrie *blockchain* et crypto-actifs qu'il ne l'est en Europe, ce qui a permis le développement plus rapide de l'industrie américaine. Aujourd'hui, elle est un peu plus établie que l'industrie européenne. La maturité générale du marché américain est plus avancée. Par exemple, l'une des plus importantes plateformes crypto américaine, à savoir Coinbase, est valorisée à 40 milliards de dollars, avec 500 millions de dollars investis. La plateforme d'échange française Paymium représente 1,1 million de dollars investi, soit 0,1 % de ce que l'on voit sur Coinbase. L'ordre de grandeur est donc très différent, et explique cette différence de maturation et de maturité entre l'écosystème français et l'écosystème américain.

Pour nous montrer plus positifs en ce qui concerne l'écosystème français, nous avons pu voir, durant l'année 2020, que cette industrie se renforce, gagne en visibilité et en reconnaissance. La crise de la Covid-19 explique aussi cette croissance, avec une démocratisation plus importante des technologies *blockchain* et des actifs numériques durant cette période. La croissance perdure malgré le contexte. L'industrie est établie en France grâce à son cadre légal, une expertise, une ingénierie largement reconnue, ainsi que la structuration autour de l'association afin de lever quelques obstacles au développement de l'écosystème.

M. Simon Polrot. La France est un peu en retard en termes de cycles de marché, mais c'est une réalité européenne. Le marché européen est assez morcelé. L'essentiel des acteurs et des volumes sur le territoire européen, au sens large, sont localisés au Royaume-Uni et en Suisse. Finalement, parmi les pays membres de l'Union européenne et situés en Europe continentale, il y a assez peu d'acteurs significatifs. Il existe quelques exceptions de taille moyenne, des plateformes d'échange, des conservateurs. En France, Ledger est tout de même un acteur important en taille, qui a largement dépassé les autres acteurs de l'écosystème. Une des spécificités du marché européen est de se concentrer sur la fourniture de liquidités et sur les *brokers*.

Le marché européen est réglementairement très morcelé. Chaque pays a son approche différente, ce qui va jusqu'à une différence d'approche juridique des crypto-actifs, que certains assimilent à des actifs financiers, d'autres à des biens. D'autres encore ont créé des régimes *ad hoc*, comme la France avec la loi relative à la croissance et à la transformation des entreprises (loi PACTE) – ce qui crée des distorsions assez importantes pour un acteur souhaitant aborder l'ensemble du marché européen, et qui devra mener des analyses juridiques pays par pays, ce qui constitue un vrai obstacle aujourd'hui.

Pour faire un peu de prospective, le projet de Règlement européen sur les crypto-actifs MICa *(Markets in crypto-assets)* et le *Pilot Regime for market infrastructures based on distributed ledger technology* (régime pilote pour les infrastructures de marché reposant sur la technologie des registres distribués) sont des initiatives très positives qui viennent compléter les initiatives déjà réalisées en France. MICa est très inspiré du régime français. Il s'agit d'un régime *ad hoc*, qui accorde un statut particulier aux crypto-actifs et aux acteurs. En tant qu'association, nous avons quelques remarques à faire sur le régime, mais son principe est très positif. Il va permettre de construire un marché unique européen des crypto-actifs, et aux acteurs européens d'aborder immédiatement l'ensemble du marché, ce qui va dans la bonne direction.

Les faiblesses du marché portent sur le financement, et sont dues à des blocages institutionnels, qui sont à la fois culturels et fonctionnels. Pour les acteurs des crypto-actifs, par exemple, il est quasiment impossible de créer des comptes bancaires, les acteurs bancaires ne souhaitant pas s'engager sur le marché des crypto-actifs. Ce refus va jusqu'au refus d'ouvrir

un compte. Ce n'est pas seulement qu'ils ne souhaitent pas accompagner, c'est qu'il est impossible pour les acteurs de réaliser une activité économique en France. Les acteurs français sont obligés d'ouvrir des comptes à l'étranger pour réaliser leurs activités, ce qui pose un certain nombre de problèmes en termes d'accès au financement, d'accès à la clientèle – il est beaucoup plus difficile d'*onboarder* des clients quand vous avez un RIB allemand ou luxembourgeois. Un certain nombre de problèmes fonctionnels sont liés à l'accès au compte. Il est important de le dire.

Cela dit, la France possède des atouts. Ledger, par exemple, représente une belle *success story*. Les acteurs ont eu l'intelligence, compte tenu des problématiques locales, de se tourner très vite vers l'international. Les entreprises françaises réalisent des volumes importants avec des acteurs étrangers. Nous avons une industrie dont quelques acteurs sont assez connus dans l'écosystème crypto-actifs, en dehors de la France.

Nous ne parlons que des crypto-actifs car nous sommes concentrés sur ces cas d'usage. On y voit l'industrie se développer ainsi que les grands enjeux de souveraineté pour le futur. Les grands groupes industriels s'intéressent également à la *blockchain*, ce qui est positif. Nous espérons que cet intérêt pour les crypto-actifs va se généraliser, puisque, selon nous, c'est là que se situent les enjeux.

M. Philippe Latombe, rapporteur. Avez-vous une opinion sur la force probante de la *blockchain*, ou des recommandations à faire ?

M. Simon Polrot. Parlez-vous de l'admissibilité de la preuve devant le juge ?

M. Philippe Latombe, rapporteur. C'est cela.

M. Simon Polrot. Pour nous, la preuve *blockchain* est une preuve de droit commun – je ne crois pas que la loi ait évolué. La preuve est admissible devant les tribunaux en fonction de critères de fait. La problématique de la preuve sur la *blockchain* est profondément liée aux enjeux de compréhension de la technologie sous-jacente, car les *blockchains* ne sont pas égales. Une *blockchain* est une technologie. La façon dont elle fonctionne, sa gouvernance, son degré de résilience et de fiabilité vont forcément avoir un impact sur la valeur de la preuve qui sera inscrite. Elle dépend de la robustesse du réseau. Plus le réseau est distribué, public, plus on a de garanties quant à la résilience et au fait qu'il n'a pas été altéré et plus l'inscription sur le réseau aura une force importante.

En outre, la *blockchain* ne valide pas la véracité d'une information, mais la validité de l'inscription qui a été réalisée, qui peut être la preuve d'une opération réalisée, la preuve d'existence d'un document, la preuve d'une authentification réalisée par un tiers. Tous ces éléments doivent être traités de façon *ad hoc*, car il s'agit de cas d'usage différents. Nous parlons beaucoup d'identité décentralisée et d'identité numérique. Un réseau *blockchain* public peut être le support de ce type d'authentifications, lesquelles permettent ensuite d'utiliser des preuves pour faire état de son identité, qui aurait été vérifiée sur une *blockchain*. Tout cela nécessiterait des ajustements, à la fois sur les modalités de détermination de l'identité et sur le caractère probant de ces preuves sur la *blockchain*. Nous n'avons pas encore beaucoup travaillé sur le sujet en tant qu'association, mais nous venons de constituer cette semaine un comité juridique au sein de l'ADAN. C'est un des sujets dont nous allons nous saisir cette année pour faire des propositions concrètes d'ajustement.

M. Philippe Latombe, rapporteur. La loi PACTE a eu un effet sur les crypto-actifs. Depuis cette loi, y a-t-il eu des régressions, des choses qui ont empêché le développement des crypto-actifs en France ? Que faudrait-il défaire, refaire ou modifier pour que l'on puisse avoir

un développement important, sachant que l'un des enjeux du Brexit était de transformer la place de Paris en place financière importante. Ne sommes-nous pas en train de passer à côté de quelque chose sur les crypto-actifs ? N'existe-t-il pas deux voies parallèles, ou deux objectifs différents qui ne se rejoignent plus ?

M. Simon Polrot. La loi PACTE a été un signal très positif pour le développement de l'écosystème. Elle a encouragé de nombreux entrepreneurs à se lancer. en 2018 et 2019. Un peu moins d'un tiers des membres de l'ADAN ont été créés durant ces deux années, ce qui est un signal positif. La mise en place du régime a été et reste compliquée. Cela prend du temps. Dans un secteur innovant, il est compliqué de mettre en place une régulation nouvelle. Les régulateurs doivent s'adapter, se former. Les acteurs doivent aussi se former, car les exigences de régulation sont parfois mal comprises. Les acteurs ne viennent pas du monde bancaire et financier et les obligations sont adaptées de ces mondes-là.

La période d'ajustement, qui est toujours en cours, a été très difficile pour le secteur. Quelques acteurs ont dû fermer boutique car ils ont perdu trop d'argent pendant la période durant laquelle ils ont dû arrêter de travailler. Depuis le 18 décembre, tous les acteurs qui ne sont pas enregistrés ont interdiction d'exercer en France. Ceux qui n'ont pas eu le temps de ou qui n'ont pas réussi à s'enregistrer avant cette date ont dû *de facto* cesser leur activité. Pour certains d'entre eux, cela a été fatal à l'activité. Ces difficultés de mise en place peuvent se comprendre, mais il est dommage que nous n'ayons pas pu mieux anticiper. Peut-être la responsabilité est-elle partagée dans l'industrie avec les régulateurs, mais le résultat est qu'il y a eu des effets de bord plutôt négatifs de la réglementation.

Pour autant, ce qui manque est plutôt l'effectivité complète de ce régime. Le régime encadre les acteurs. Il faudrait que le reste de l'industrie, et notamment l'industrie bancaire, en prenne la pleine mesure, et qu'il y ait un droit effectif au compte, qui permette aux acteurs de se développer et à l'industrie d'avoir accès aux crédits, à des instruments bancaires performants, etc. C'est aujourd'hui un fort blocage dans le secteur. Il serait important de renforcer le soutien public de l'industrie aux crypto-actifs.

Des enjeux de souveraineté s'attachent à l'existence d'une infrastructure de marché des crypto-actifs en France. Cet enjeu n'est pas encore identifié par les décideurs. On voit se dessiner une infrastructure financière de demain, qui le sera au moins partiellement sur la base des crypto-actifs. Le fait d'avoir une maîtrise, une visibilité, une surveillance possible des flux – que ce soit les flux qui concernent les citoyens ou les entreprises – nous semble essentiel. C'est un enjeu de souveraineté très important.

Pour que cette industrie fonctionne et que l'on puisse rattraper le retard par rapport aux équivalents européens et asiatiques, l'un des axes serait de renforcer le soutien du secteur public aux crypto-actifs. Nous avons constaté que le soutien du secteur public portait davantage sur la technologie. Il est évidemment très important de maîtriser la technologie, mais le cas d'usage le plus important des crypto-actifs est souvent mis de côté, un peu mal vu : son importance est diminuée et on le voit comme quelque chose d'annexe. Nous parlons beaucoup *blockchain* mais pas crypto-actifs, *blockchain* mais pas *bitcoins*, etc., ce qui est pour nous une erreur stratégique, car ces marchés concentrent des enjeux de souveraineté majeurs pour le futur. Voilà les éléments que je voulais évoquer : le soutien public à l'industrie, que ce soit par les financements ou par des accès à des marchés, et le droit effectif au compte bancaire, qui permettrait aux acteurs de se développer.

M. Philippe Latombe, rapporteur. Pourquoi les banques – je ne parle pas seulement des établissements bancaires, mais aussi des banques centrales, comme la Banque centrale européenne – sont-elles aussi frileuses en ce qui concerne les crypto-actifs ? Qu'est-ce qui le

justifie selon vous ? Quels sont les freins qu'il faut lever – et pas seulement juridiquement, comme dans le cas du droit au compte, que vous demandez ? Qu'est-ce qui fait qu'aujourd'hui il n'y a pas de confiance, et qu'il y a même une méfiance à l'égard des crypto-actifs, d'où une impossibilité d'y recourir pour un certain nombre d'établissements bancaires ?

M. Simon Polrot. Les crypto-actifs se sont créés en dehors du monde financier traditionnel. C'est un outil technologique qui a été créé par des technophiles. Cela a été construit – et c'est toujours le cas aujourd'hui – par des acteurs qui ne font pas partie du monde des acteurs financiers traditionnels. Dès le départ, cela a été quelque chose d'un peu marginal. C'est d'abord un support technologique sur lequel s'est construite une valeur. Ensuite, c'est à partir de l'usage, de la création de produits autour de ce support technologique que s'est créée une industrie. C'est un phénomène inédit dans la création de la valeur – en tout cas depuis bien longtemps. Le monde financier est un monde extrêmement réglementé. Quand elles arrivent dans le secteur, même les *fintechs* sont déjà intégrées aux réglementations existantes. Elles demandent parfois des extensions ou la possibilité de réaliser des choses nouvelles. Des progrès sont réalisés de façon incrémentale dans la réglementation financière, mais les crypto-actifs sont disruptifs par rapport à cette industrie, puisqu'ils se construisent en parallèle. Cela s'est construit, dans un premier temps, dans une absence de réglementation, dans un vide juridique, puisque cela était complètement nouveau et que ce n'était pas capté par la réglementation existante.

Les caractéristiques particulières des crypto-actifs, qui les rapprochent beaucoup plus de biens physiques, comme l'or, que d'une monnaie telle qu'on la connaît aujourd'hui, ont entraîné beaucoup d'incompréhension. Les communautés crypto-actifs et les communautés financières se sont assez mal comprises. Elles employaient les mêmes mots, sans désigner les mêmes choses. Dans l'historique de développement du *bitcoin*, il y a des usages liés au marché noir, au financement d'activités illicites, etc. Il y a donc un historique un peu compliqué dans la création de ces actifs, qui a entraîné une méfiance du secteur bancaire traditionnel, et même une forme de mépris pour cet outil de *geek*, de technophile, qui n'était pas sérieux. C'est souvent le cas des innovations de rupture : on les considère au début comme ridicules et marginales, avant que cela ne devienne quelque chose d'important.

Une vraie transformation s'est produite dans certains secteurs d'activités, et ces usages entrent. Une collision entre le monde financier traditionnel et le monde des crypto-actifs se fait un peu dans la douleur. Nous avons une normalisation progressive de ces activités, qui sont maintenant complètement encadrées. S'agissant de la lutte contre le blanchiment d'argent et le financement du terrorisme, il existe des guidances internationales et des implémentations spéciales en France. Certains acteurs sont supervisés par l'autorité de contrôle prudentiel et de résolution (ACPR), et leurs dispositifs de lutte contre le blanchiment sont validés avant que l'activité puisse démarrer. Certains établissements « cryptos » deviennent des banques : cela devient assez régulier aux États-Unis, où de telles annonces sont effectuées tous les quinze jours. Des acteurs du paiement traditionnel s'intéressent aux crypto-actifs. Des initiatives mènent à une convergence, et finalement une utilisation de ces crypto-actifs en conservant l'intérêt de leurs caractéristiques essentielles : la possibilité de pouvoir appréhender directement l'actif, de pouvoir l'échanger de pair à pair, d'utiliser des cas d'usage innovants, etc., tout en ayant des acteurs réguliers, qui permettent de construire une infrastructure de confiance autour de ces crypto-actifs.

Le problème est le passage de la construction de tous ces outils à leur prise en compte effective par l'industrie bancaire et financière. Nous constatons un retard, qui peut être lié à de nombreuses raisons, des blocages culturels, des positions fortes prises par les acteurs bancaires ces dernières années, qui se sont prononcés contre les crypto-actifs et peuvent difficilement se dédire. Pour nous, ce n'est qu'une question de temps. Nous souhaitons

accélérer ce mouvement afin que la confiance se reconstruise. Il s'agit aujourd'hui vraiment d'un problème de confiance des acteurs bancaires, difficile à appréhender, parce que nous manquons de ressorts en dehors d'envoyer des messages positifs et de montrer des gages de sérieux.

Nous constatons tout de même une assez mauvaise volonté d'un certain nombre d'acteurs dans l'industrie pour se pencher sur ce sujet sensible. Nous espérons que ce type d'initiatives – notamment ce rapport, mais d'autres également – enverront des messages plus positifs autour du développement de l'industrie.

M. Philippe Latombe, rapporteur. Le fait que battre monnaie est l'une des caractéristiques de la souveraineté d'un État ou d'une fédération d'États, n'est-il pas en contradiction avec ce que sont des crypto-actifs, situés en dehors de cette notion ? Cela fait le lien avec la souveraineté dans notre mission d'information. Le Libra en est un exemple, initiative d'un GAFAM, qui, s'il ne s'appellera plus Libra, arrivera en 2022, si les annonces sont suivies. N'est-ce pas la raison de la crainte et de l'opposition ? On ne parvient pas à faire le lien entre crypto-actifs et souveraineté, et on va même jusqu'à opposer les deux.

M. Simon Polrot. Il existe une incompréhension des enjeux de souveraineté. Nous parlons beaucoup de monnaies privées pour désigner les crypto-actifs. C'est une erreur fondamentale, parce que les crypto-actifs natifs, comme le *bitcoin*, sont des monnaies communes, créées par des initiatives, mais n'appartenant pas à une personne en particulier. Des distinctions doivent être faites entre un projet privé comme le Libra et un projet d'initiative privée qui devient un commun, puisqu'une *blockchain* publique est par nature une *open source* : chacun peut l'exécuter, participer au réseau et devenir acteur du développement du réseau. C'est une grande distinction, qui n'est pas suffisamment faite. Le niveau de connaissance n'est pas suffisamment important sur cette distinction fondamentale. On confond souvent dans une même catégorie le Libra et le *bitcoin*. C'est une erreur très significative, en termes de concept.

Le Libra est un projet d'initiative privée de la part d'une *Big Tech* américaine, sur le sujet fondamental de la monnaie, puisque ce projet s'est constitué avec un objectif monétaire : une monnaie mondiale, qui serait plus ou moins stabilisée avec des paniers de devises. Effectivement, la réaction a été assez naturelle et logique de voir cette nouvelle monnaie comme une menace à la souveraineté monétaire des États. Nous rejoignons les conclusions des institutions sur cette menace : il est tout à fait cohérent de penser qu'une entreprise privée qui créerait une nouvelle monnaie mondiale n'est probablement pas quelque chose de souhaitable. Si cela se fait, il faudra que ce soit dans des cadres extrêmement stricts qui permettent de contrôler le développement de ces initiatives.

Aujourd'hui, le Libra qui s'appelle Diem a été complètement abandonné, en tout cas pour l'instant. Le projet qu'il souhaite lancer en 2022 sera juste un *stablecoin* dollar, c'est-à-dire un actif qui représentera un dollar. Les enjeux ne sont plus les mêmes : il s'agit d'une monnaie collatéralisée par un dollar, il n'y a même pas de création monétaire. On collatéralise en banque un dollar, et on représente le dollar sur *blockchain*. Cela pose tout de même des questions d'encadrement, pour être sûr qu'il existe bien un dollar derrière. D'ailleurs, la réglementation européenne prévoit un début de cadre à ce propos, même si elle est très protectrice – un peu trop, à notre sens.

Nous nous trompons en pensant que le *bitcoin* et ce type d'actifs sont des menaces similaires pour la souveraineté monétaire des États. Dans les faits, sur les *blockchains* publiques, il y a une très forte demande pour les représentations de monnaies fiduciaires, qui se développent de plus en plus. Plusieurs dizaines de milliards de dollars sont représentés sur la *blockchain* publique – les *stablecoins*. Il s'agit de dollars USDT (Tether), USDC (USD

Coin), qui sont des représentations de dollars sur la *blockchain* publique. Nous n'avons malheureusement pas ou très peu d'équivalent européen pour des raisons de clarté réglementaire, de développement du marché. Il s'agit donc aussi d'un enjeu de compétitivité.

Nous portons des messages très ambitieux pour le développement d'une représentation d'euros sur *blockchain* publique qui doit se faire probablement suivant une initiative publique-privée en Europe, ou *a minima* avec le soutien des pouvoirs publics. Ce sont des enjeux différents. Un *bitcoin* ou un ethereum ne vont pas remplacer un euro. Ce n'est ni le même usage, ni la même problématique. Le rôle fondamental de ces crypto-monnaies, comme tezos, est de faire fonctionner un réseau public, et de servir de représentation de valeurs sur ces réseaux. Ce n'est pas vraiment un objectif de monnaie d'échange. Certains le souhaitent, mais ce n'est pas du tout l'usage constaté. Dès qu'il est question des monnaies d'échange, on retombe sur des *stablecoins*, c'est-à-dire des représentations de dollars ou d'euros, et les enjeux ne sont plus les mêmes. Il s'agit plutôt de garantir que ces représentations sont suffisamment contrôlées et matures. Nous ne sommes pas du tout face à des menaces à la souveraineté monétaire.

M. Philippe Latombe, rapporteur. Ne pourrait-on pas trouver un autre mot que celui de « monnaie » pour éviter cette confusion, ou cette opposition systématique ? Pour certains, les crypto-actifs ressemblent à des actions et peuvent avoir un cours qui fluctue, pour d'autres il s'agit d'une cryptomonnaie. Cela génère de la confusion. Le cadre européen, très protecteur, est peut-être lié au fait que nous ne savons pas exactement ce dont il s'agit, ni comment le définir. Ne faudrait-il pas utiliser un mot quasiment unique et le définir de façon claire ? N'est-ce pas le rôle d'une association comme la vôtre ?

M. Simon Polrot. Nous avons fait ce travail. Il existe tout de même plusieurs catégories d'actifs. Il est donc difficile de ne retenir qu'un seul terme. Le terme le plus large est « crypto-actifs » ou « actifs numériques ». Ce sont les termes que nous utilisons de façon interchangeable pour désigner tous ces actifs.

Ensuite, nous entrons dans le détail, en distinguant :

– d'une part, des *tokens* de protocole qui sont ce qu'on appelle couramment les cryptomonnaies, les *tokens* qui sont là pour faire fonctionner le protocole, qui sont nés du protocole, et qui sont nécessaires au fonctionnement de celui-ci ;

– et d'autre part, tous les autres crypto-actifs, créés à l'initiative d'une ou plusieurs personnes privées ou publiques pour un cas d'usage déterminé : le *stablecoin* qui a vocation à représenter un euro ; le *security token* qui a vocation à représenter un titre financier ; l'*utility token*, qui peut représenter plusieurs formes de services ou de biens sur une *blockchain* publique ; les *non fongible token* (NFT), dont on parle beaucoup, qui représente des objets numériques.

Nous avons créé une taxonomie, que nous pourrons bien sûr vous faire parvenir et qui est disponible sur notre site Internet, pour clarifier cette variété d'actifs et la variété de cas d'usage qui en découlent. Je vous rejoins sur la confusion entretenue autour de la notion de cryptomonnaie. Il existe toujours ce fameux débat sur le thème de : « est-ce une monnaie ? » Pour nous, cela passe complètement à côté du sujet.

M. Philippe Latombe, rapporteur. Nous serons preneurs d'une contribution écrite sur ces éléments. Quelles modifications estimez-vous nécessaires pour permettre le développement des crypto-actifs et de leur place en Europe ou en France, et pour quelles raisons ? Devrait-on effectuer ce changement au niveau national ou au niveau européen ?

M. Simon Polrot. L'axe le plus simple et le plus évident est le financement de l'infrastructure, l'objectif étant d'avoir des entreprises de taille suffisante. Nous sommes déjà dominés économiquement, mais il s'agirait de contrebalancer cette domination par des acteurs de taille importante. Il faudrait régler ce problème d'accès au financement, problème à la fois privé et public, puisqu'il n'y a pas de financement public dans l'écosystème des crypto-actifs et que le financement privé est complètement « à la traîne », dans la mesure où il n'y a pas de connaissance fine de la part des investisseurs. Ces problématiques ne concernent pas les seuls crypto-actifs, mais sont particulièrement fortes à leur égard, car ceux-ci n'ont pas du tout accès au financement bancaire, les banques étant hostiles au secteur. Si l'on ne devait choisir qu'une action, ce serait celle-là. Il y a aussi la réglementation, mais il existe déjà des initiatives dans ce sens.

Mme Faustine Fleuret. Pour ma part, j'évoquerais la dichotomie qui existe traditionnellement entre la *blockchain* et les crypto-actifs, et à laquelle il conviendrait de mettre un terme. Il s'agirait d'avoir globalement une image plus positive et une compréhension plus fine de ce que sont ces crypto-actifs, qui sont souvent tous mis « dans le même panier », ce qui provoque des réticences du côté de l'industrie bancaire, l'approche réglementaire des institutions européennes, l'approche de la BCE.

Manque aussi peut-être, et ce qui est sous-jacent de l'ensemble, un souffle plus positif de la part des décideurs, qui permettrait une meilleure compréhension des enjeux des crypto-actifs pour la souveraineté numérique, pour l'économie et la transformation de la finance en général, et de l'ensemble des innovations que portent ces crypto-actifs.

M. Philippe Latombe, rapporteur. Les investisseurs n'ont pas forcément une connaissance fine des crypto-actifs, ce qui complique l'investissement. Des filières d'ingénieurs, de financiers commencent-elles à se créer pour les crypto-actifs – filières, à terme, porteuses d'excellence et d'emploi ? Sinon faut-il créer ces filières ? S'agit-il d'un effet collatéral de ce que vous demandez pour les financements ?

M. Simon Polrot. Il existe des initiatives privées, des écoles privées qui ont identifié un secteur porteur et qui ont créé des filières spécialisées. Il manque peut-être une vision stratégique de la part de l'État quant à des formations dans les écoles publiques et au-delà des filières d'excellence. Avoir une formation générale sur les crypto-actifs et leurs enjeux serait extrêmement important. Il serait intéressant que l'État soit moteur d'une démarche stratégique de formation aux crypto-actifs. Nous avons des filières d'excellence, d'ingénieurs, etc. Sur le plan technique, une *blockchain* n'est pas incompréhensible. Un bon ingénieur français qui s'intéresse culturellement au secteur, qui a une appétence particulière, progresse très vite et peut être très bon. De nombreux Français participent aux projets en vogue dans les crypto-actifs – ce ne sont pas des projets français, mais ils travaillent pour eux. Il y a une place pour des filières d'excellence, et aussi pour une meilleure culture générale de ce secteur. Une stratégie de formation un peu construite par l'État sur ces aspects serait bienvenue.

M. Philippe Latombe, rapporteur. Comment envisagez-vous les crypto-actifs ? Quelle est leur place à moyen et à long termes ? Les établissements bancaires et financiers ont peur de se faire détrôner, de disparaître à cause de la technologie des crypto-actifs. Est-ce une crainte justifiée ? Cela pourrait-il arriver, ou les deux vont-ils cohabiter, et cela pour longtemps ? Quelle est la place du secteur à terme ? Je vous demande votre vision. Comment cela peut-il se passer, en fonction des différentes plaques géostratégiques, si l'Europe est très en retard, que les États-Unis se développent très fortement, et qu'en réaction les Chinois en développent une, mais sous forme complètement publique ? Quels sont les éventuels écueils à éviter ?

M. Simon Polrot. Notre vision à moyen et long termes est que tout ou partie de l'industrie financière au sens large va se construire sur les crypto-actifs, sur des réseaux publics de valeurs, avec tous les cas d'usage innovants qui le permettent. Nous voyons déjà des signaux faibles de cette fusion, dans certains cas marginaux. Dans notre vision à dix ou vingt ans, l'industrie financière et l'industrie des crypto-actifs seront une même chose. Selon moi, la peur des banques s'assimile à la peur de l'industrie culturelle face à Internet. Il est inévitable que tout ou partie de la finance passe par les crypto-actifs dans les prochaines années. Toute velléité de freiner ou d'empêcher cette réalisation ne fera que provoquer un retard considérable de l'industrie bancaire et financière dans ce secteur. Elle va se trouver confrontée à des nouveaux géants qui la remplaceront, si elle ne devient pas compétitive.

Le premier signal extrêmement fort, qui est un tremblement de terre dans le système financier, est l'entrée en bourse de Coinbase ce mois-ci. Aujourd'hui, Coinbase est tellement « gros » qu'une banque ne peut pas le racheter. C'est un acteur qui offre des services sur un nouveau secteur complètement distinct du secteur bancaire, complètement parallèle. Du fait du refus d'aller dans ce secteur, un dépassement intervient déjà pour un certain nombre de cas d'usage – pas tous bien sûr. Ce signal doit être pris très au sérieux.

L'industrie bancaire et financière doit entrer de plain-pied dans ce secteur car elle est extrêmement puissante en Europe, très structurante dans l'économie et dans la manière dont l'économie peut fonctionner de façon efficiente. Si des acteurs américains acquièrent la domination sur toute l'infrastructure économique parce qu'ils sont allés vers cette économie, vers ces nouveaux actifs, alors que les Européens n'auront pas voulu le faire, nous allons nous retrouver dans un écosystème davantage dominé par d'autres pays. Nous sommes déjà complètement dominés économiquement, sur le plan des « autoroutes de l'information » d'Internet. Si l'on refait la même erreur pour les autoroutes de la valeur, nous ferons face à un vrai problème de souveraineté à long terme. Il convient de lever le plus vite possible les blocages de l'industrie bancaire et financière. C'est une urgence pour l'Europe, qui repose, beaucoup plus que les États-Unis, sur ces acteurs pour financer son économie.

M. Philippe Latombe, rapporteur. Y a-t-il un sujet dont nous n'avons pas parlé et que vous aimeriez mettre en lumière ?

M. Simon Polrot. Concernant l'infrastructure, des initiatives, notamment européennes ont vu le jour. Dans d'autres auditions, il a été question de l'EBSI *(European blockchain services infrastructures)*, notamment pour l'infrastructure *blockchain*. Ces initiatives sont extrêmement positives. En tant qu'association, nous nous positionnons dans des réseaux publics ouverts. Nous pensons que ces réseaux vont fortement interagir avec des réseaux plus contrôlés, plus fermés (notamment l'EBSI), qui seront des réseaux hybrides, accessibles mais contrôlés par les institutions pour un certain nombre de points d'entrée et de cas d'usage.

Il nous semble essentiel d'utiliser des technologies ouvertes, connues et utilisées par le marché, afin d'assurer l'interopérabilité la plus forte. Porter des projets nationaux et internationaux d'infrastructures autour de la *blockchain* est extrêmement important, mais il faut s'assurer que ces projets sont compatibles avec les réseaux publics les plus importants, et qu'ils puissent créer des cas d'usage d'interopérabilité et qu'ils apportent quelque chose au marché. Le marché est déjà là. Il est en train de se développer sur ces réseaux publics. Il ne faut pas construire en « silo » une solution parallèle et séparée. Ce message vaut aussi pour les projets d'euro numérique de la Banque centrale européenne. Ces projets réellement importants sont complémentaires des initiatives privées, peuvent les porter vers l'avant et venir au soutien de l'industrie française. Ils doivent absolument se développer à l'écoute et en synergie avec les initiatives privées, pour qu'ils aient du sens pour l'industrie et pour les acteurs privés.

Audition, ouverte à la presse, de Me Nathalie Chiche, avocate au Barreau de Paris, déléguée à la protection des données, rapporteure de l'étude du Conseil économique, social et environnemental : « Internet : pour une gouvernance ouverte et équitable »
(27 avril 2021)

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. Cet échange s'inscrit dans nos réflexions sur la *blockchain*. Nous avons auditionné la fédération française des professionnels de la *blockchain* la semaine dernière, et nous venons d'entendre l'association française de développement des actifs numériques. Dans un souci d'approche pratique par des cas d'usage, nous souhaitons pouvoir échanger avec vous sur l'avenir de cette technologie, sur les nombreuses possibilités qu'elle offre et qu'elle va continuer à offrir dans les prochaines années.

M. Philippe Latombe, rapporteur. J'aimerais vous interroger à titre liminaire sur trois sujets. Le premier, qui est une question rituelle de nos auditions, concerne votre approche de la notion de souveraineté numérique. Cette question procède de la grande diversité des définitions qui existent de cette notion. Comment la définissez-vous et comment la *blockchain* peut-elle être un levier de souveraineté pour la France et pour l'Europe ? Je souhaiterais que vous nous présentiez le cas d'usage possible que vous aviez évoqué dans une tribune des *Échos* du 19 août 2018, qui concerne l'inscription du registre national de la commission nationale de l'informatique et des libertés (CNIL) dans une *blockchain*.

En ce qui concerne le développement, en France, d'un écosystème *blockchain* performant, comment jugez-vous l'action des pouvoirs publics, alors qu'une stratégie nationale *blockchain* a été lancée à l'initiative du gouvernement et des acteurs dans ce domaine? Nous auditionnerons jeudi la *task force blockchain* du ministère de l'Économie, des Finances et de la Relance, qui en est l'une des structures d'appui.

Enfin, je souhaiterais que nous puissions évoquer la dimension européenne de la *blockchain*. Comment la France se situe-t-elle par rapport à ses voisins européens dans ce domaine ? Que pensez-vous de l'action de l'Union européenne sur ce sujet ? Cela nous permettra d'évoquer au passage l'enjeu de la force probante de la *blockchain*, qui est une question juridique importante, pour laquelle le législateur doit être fortement mobilisé.

Me Nathalie Chiche, avocate au Barreau de Paris, déléguée à la protection des données, rapporteure de l'étude du Conseil économique, social et environnemental : « Internet : pour une gouvernance ouverte et équitable ». Force est de constater que la crise sanitaire que nous traversons a accentué la dépendance de nos modes de vie vis-à-vis de ces géants du numérique – pour travailler, pour communiquer, pour se divertir. Le concept de souveraineté numérique est plus que jamais au centre du discours politique et de l'opinion publique – d'où, je suppose, cette mission d'information. J'ai été rapporteure d'une étude du CESE (Conseil économique, social et environnemental) sur la gouvernance d'Internet en 2014, juste après l'affaire Edward Snowden, qui nous a alertés en 2013 d'une surveillance massive de nos données par la NSA (l'Agence nationale de sécurité américaine). En utilisant le programme PRISM, la NSA avait un accès direct aux données hébergées par ces mêmes géants de l'Internet, comme Google, Microsoft, Apple, Facebook ou YouTube, dont nous sommes si dépendants. Un autre scandale a suivi, en 2018 : celui de l'affaire Cambridge Analytica, *via* l'application Facebook.

Ces affaires nous démontrent que les géants du numérique peuvent servir d'instruments à des puissances étrangères pour porter atteinte à la souveraineté de la France et de l'Europe. À terme, ces affaires ont profondément altéré la confiance des utilisateurs que nous sommes envers notre État, qui est l'ultime garant de nos libertés et de nos droits. Personnellement, je pense que la technologie *blockchain* pourrait s'inscrire dans cette démarche de souveraineté, puisqu'elle peut venir en renfort de la société civile, là où les gouvernements n'ont pas eu concrètement les moyens d'assurer le respect de leurs normes dans le cyberespace. Elle est révolutionnaire, car elle instaure d'emblée une confiance dans le réseau et permet surtout de réaliser ce qu'Internet n'a jamais permis de faire, c'est-à-dire de se passer d'intermédiaires, comme les GAFAM.

Nous entendons beaucoup parler de la technologie *blockchain*. Elle est la promesse technologique du moment. Elle est attendue, annoncée comme une réorganisation complète du paysage de l'Internet. En 2018, j'avais été auditionnée par une mission d'information sur les usages des *blockchain*s et des registres de certification. Je m'étais exprimée sur la nécessité d'avoir des applications concrètes de la *blockchain* pour espérer une adhésion massive des entreprises et des utilisateurs. *In fine*, le rapport a fortement lié le développement des technologies *blockchain* au recours à des crypto-actifs, dont elles sont souvent le support. De même, nous assistons en ce moment à un engouement du marché de l'art pour le crypto-art, qui est basé sur la même technologie que les cryptomonnaies.

Force est de constater que ces applications ayant recours à la cryptomonnaie sont réservées à des initiés et sont hautement spéculatives, comme le marché de l'art. Pour ma part, je suis convaincue que l'essor de la *blockchain* sera lié à des applications concrètes et à des besoins quotidiens. Je pense à l'utilisation de la *blockchain* en lien avec le secteur alimentaire. Face à la multiplication des scandales sanitaires, comme par exemple celui de Lactalis, l'entreprise Carrefour avait compris que le consommateur désirait toujours plus de transparence et d'assurance sur les produits qu'il achète, et a voulu nouer des relations de confiance avec le consommateur, comme entre le producteur et le distributeur. Pour moi, la *blockchain* alimentaire, à l'inverse des cryptomonnaies, est une réponse aux besoins de ce client. En scannant le QR code présent par exemple sur l'étiquette d'un poulet, le consommateur peut accéder *via* son smartphone à des informations transparentes pour connaître le nom de l'éleveur, l'alimentation reçue, l'absence de traitement antibiotique et le lieu d'abattage.

Il faut savoir que la technologie est parfaitement générique et peut s'appliquer à de nombreux services de notre vie quotidienne. C'est cela qui est le plus intéressant : une mise en relation entre taxi et usager est possible sans passer par Uber, par exemple, et une mise en relation est possible entre une librairie et des lecteurs sans passer par Amazon. Nous le voyons, le développement de la technologie *blockchain* représente pour la France et pour l'Europe un facteur déterminant de compétitivité, pour espérer rattraper notre retard dans l'économie numérique.

Il se trouve que j'ai assisté à la présentation de la stratégie nationale *blockchain* par M. Bruno Le Maire. Cet événement, qui s'appelait « Paris *Blockchain* Conférence », se demandait si la *blockchain* allait bouleverser l'ordre économique mondial. J'avais écouté longuement le discours de M. Bruno Le Maire, dans lequel il dévoilait les ambitions de la France : permettre le développement d'un modèle de *blockchain* sûr et surtout compatible avec l'exercice de notre souveraineté. Il partait du constat que la France et l'Europe avaient des difficultés à assumer leur fonction régalienne face à de puissants acteurs, souvent américains ou chinois, qui sont dotés d'une avance technologique indiscutable. Pour le ministre, la *blockchain* serait un modèle concurrentiel, parce que ce modèle s'érige par principe contre les monopoles. M.

Bruno Le Maire avait parlé de la situation monopolistique de ces géants du numérique, qui étaient devenus, d'un point de vue financier, technologique, économique et même politique, un sujet absolument majeur.

J'ai lu votre tribune dans *Next INpact*, M. le rapporteur, où vous citez Mme Linda Khan, commissaire de la FTC (*Federal Trade Commission*). Comme elle, nous pensons qu'il est temps de faire évoluer le droit de la concurrence, qui ignore bien trop souvent que la lutte contre les positions dominantes ne peut se réduire à une question économique. Cette lutte doit prendre aussi en compte le sociétal et le politique. Dans sa thèse d'université, Mme Linda Khan a pu démontrer comment des prix bas, apparemment profitables au consommateur et que proposent les GAFA, pouvaient éliminer la concurrence et l'innovation sans que les lois anti-trust ne s'appliquent à l'entreprise concernée.

À mon avis, la technologie *blockchain* peut rebattre ces cartes, parce que les utilisateurs ont la faculté d'animer, de créer leur propre réseau de commerces, de services, sans l'intermédiation d'aucune plateforme privée étrangère. M. Bruno Le Maire, lui, pensait que la technologie *blockchain* pouvait rattraper notre retard technologique, qui place actuellement la France et l'Europe en situation de dépendance. Il est difficile d'envisager la souveraineté numérique sans l'idée d'une souveraineté technologique. Pour ce faire, la France a misé principalement – je le regrette – sur la technologie *blockchain* dans le domaine monétaire et financier avec la loi relative à la croissance et à la transformation des entreprises (loi PACTE) – cela pour créer un cadre de régulation unique au monde, pour garantir la sécurité des émissions de jetons et de transactions sur les crypto-actifs. L'objectif de ce gouvernement était de créer un cadre de régulation fixé dans la loi PACTE, qui devienne un cadre de référence, et qu'il soit mis en place au plan européen et même à l'international. Pour ma part, je pense que cet objectif n'a pas été atteint, puisque personne ne copie ce modèle de référence.

M. Philippe Latombe, rapporteur. Par rapport à nos voisins européens, où en sommes-nous du cadre juridique ? Sommes-nous très en retard ? Nos voisins ont-ils pris des initiatives qu'il nous faut prendre ? Que faut-il que nous fassions, en tant que législateurs, pour améliorer ou pour donner un cadre juridique à la *blockchain*, y compris sur la partie relative à la force probante ?

Me Nathalie Chiche. Comme je vous l'ai dit, j'ai participé à la dernière mission d'information sur les usages de la *blockchain*. La proposition 14 recommandait déjà d'envisager une adaptation du régime applicable en matière de preuve électronique et de signature électronique par une révision du Règlement européen dit eIDAS *(Electronic Identification and trust Services)*. Ces questions de preuve électronique et de signature électronique constituent des enjeux majeurs pour l'attrait de la technologie *blockchain*. Actuellement, il existe une vraie insécurité juridique en matière d'utilisation de la *blockchain*. Il est donc urgent de s'assurer que la preuve de type *blockchain* dispose d'une portée juridique reflétant la fiabilité revendiquée par cette technologie.

Pour le ministère de la Justice, en l'état du droit positif, aucune législation spéciale n'est prévue. Il appartiendra aux juridictions, conformément aux règles de droit commun de la preuve, d'apprécier la force probante d'une preuve par *blockchain*. Cela crée une insécurité juridique parce que ce sera toujours à l'appréciation d'un juge. La France a progressivement légiféré en matière de *blockchain* pour répondre à la nécessité d'encadrer cet écosystème. Pour autant, il faut savoir que les textes de loi n'utilisent pas le terme « *blockchain* », mais celui de « dispositif d'enregistrement électronique partagé », même si cette notion reprend exactement les traits essentiels de la *blockchain*. Malgré ces avancées législatives majeures pour intégrer celle-ci dans l'ordonnancement juridique français, rien n'est prévu à ce jour au titre de la preuve par *blockchain*.

Comme vous l'avez dit, d'autres pays s'y sont intéressés : la Chine, qui a reconnu la valeur d'une preuve ancrée sur la *blockchain* en 2019 ; l'Italie, qui, pour des raisons sûrement liées à la mafia, a validé l'horodatage par *blockchain* comme moyen de preuve admissible devant les tribunaux. À ma connaissance, en France, aucune décision n'a été rendue par une juridiction sur la valeur probante d'une preuve établie par la *blockchain*.

Il faut savoir que le droit de la preuve n'est pas précisément codifié. La preuve est abordée par différents codes. Il existe des règles de preuves au sein du livre III du code civil. Le code civil renvoie au code de procédure civile. Le code du commerce prévoit aussi des règles de preuve spécifiques aux commerçants. La preuve en matière pénale est régie par le code de procédure pénale. Il n'y a pas d'autre choix que d'appliquer le droit commun de la preuve et de l'appliquer au cas spécifique de la *blockchain*.

La force probante est liée à la notion de preuve. Rien ne peut s'opposer au fait de conférer à la *blockchain* une forme de présomption de valeur probante, dans la mesure où la preuve des faits peut être apportée par tous moyens. Il est aussi possible d'associer la *blockchain* au mode de preuve que constitue l'écrit électronique, par capillarité. L'admissibilité de ce mode de preuve sera en tout état de cause soumise à l'appréciation des juridictions, qui devront vérifier si les conditions de validité de l'écrit, sous le format électronique, sont remplies. Un écrit électronique a la même force probante que l'écrit sur support papier, sous réserve de deux conditions, pour que la preuve du contrat conclu sur la *blockchain* soit rapportée : il faut qu'il y ait identification de l'auteur et il faut qu'il y ait la garantie du maintien de l'intégrité de l'acte. Sur la *blockchain*, on peut considérer que cette seconde condition est acquise. La première condition renvoie aux exigences de la signature électronique.

En 2017, un décret a mis en conformité les conditions de validité de l'écrit électronique avec le Règlement européen eIDAS. Aux termes de ce décret, la fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve du contraire, lorsque ce procédé est mis en œuvre par une signature électronique qualifiée. Il existe plusieurs niveaux de signature électronique dans le Règlement eIDAS, et la signature qualifiée figure évidemment au niveau le plus élevé. Pour que la fiabilité de la signature électronique sur *blockchain* soit présumée, il faudrait :

– non seulement que cette signature puisse être considérée comme une signature avancée, ce qui correspond au deuxième niveau de signature électronique dans le Règlement eIDAS. Cela veut dire qu'elle doit être liée aux signataires de manière non équivoque, qu'elle doit permettre d'identifier les signataires, qu'elle a été créée par des moyens sous le contrôle du signataire, et qu'elle garantit que l'acte auquel elle s'attache ne pourra être modifié ;

– mais aussi qu'elle constitue une signature qualifiée. Le problème de la signature qualifiée est qu'elle suppose l'intervention d'un prestataire de confiance agréé.

J'ai lu attentivement les conclusions du rapport de France Stratégie sur les enjeux de la *blockchain*, qui a été rédigé sous l'autorité de Mme Joëlle Toledano, aux termes duquel la signature *blockchain* constitue vraisemblablement une signature avancée telle que je l'ai décrite tout à l'heure au sens du Règlement eIDAS. Cela donne déjà une force probante élevée, sans toutefois lui faire bénéficier de la présomption de fiabilité. Celle-ci sera à l'appréciation du juge. Ce niveau de garantie est donc insuffisant pour faire de la signature *blockchain* l'équivalent de la signature manuscrite.

Le problème se pose aussi pour l'horodatage de la *blockchain*. Ce n'est pas instantané, il y a toujours un petit décalage. Le Règlement eIDAS prévoit aussi une présomption

d'exactitude de la date et de l'heure qu'il indique, et de l'intégrité des données auxquelles se rapportent cette date et cette heure. Là aussi, pour l'horodatage de la *blockchain*, il faudra l'intervention d'un tiers certificateur pour avoir un horodatage qualifié, et pour bénéficier encore de la présomption de fiabilité. À défaut de respecter les exigences de la signature qualifiée et de l'horodatage qualifié – qui n'est pas à la portée de toutes les bourses, je le précise – et de faire intervenir un tiers de confiance qualifié, on peut considérer que la signature sur *blockchain* et l'horodatage sur *blockchain* ne bénéficient pas de la présomption de fiabilité, et que, sans cette fiabilité d'identification de la personne et de l'exactitude de l'horodatage, le juge sera libre d'apprécier ces éléments de preuve comme il le souhaite, ce qui crée une insécurité juridique dans l'utilisation de la *blockchain*.

Afin que cesse cette incertitude juridique, il apparaît souhaitable de modifier les textes existants, afin que la signature et l'horodatage, qui interviennent dans une *blockchain*, bénéficient d'emblée de la présomption de fiabilité. En effet, la *blockchain* dispose par nature d'éléments qui garantissent un haut niveau de fiabilité, à savoir l'identification du déposant, la vérification de l'intégrité du document, l'horodatage du document, le lien entre le signataire et le document dont le droit de la preuve doit tenir compte.

Pour confirmer la proposition 14 du rapport qui avait été réalisé sur les usages de la *blockchain*, je pense qu'il faut engager une réflexion, qui devrait aboutir à une révision du Règlement eIDAS. Il faudrait aussi reconnaître la fiabilité de la signature électronique et de l'horodatage sur la *blockchain* sans l'intervention d'un tiers certificateur. Il faudrait conférer une force non pas élevée, mais renforcée, à la signature avancée sur la *blockchain*. Peut-être faudrait-il également se faire aider par l'ANSSI (Autorité nationale en matière de sécurité et de défense des systèmes d'information) pour savoir comment renforcer le niveau de sécurité des modalités techniques d'application, dont le juge pourrait tenir compte.

M. Philippe Latombe, rapporteur. Aujourd'hui, comment expliquez-vous – vous, praticienne du droit – à un juge que le recours à la *blockchain* a valeur de preuve ? Êtes-vous uniquement dans la démonstration mathématique ? Comment faites-vous pour que le juge puisse retenir des éléments portés sur une *blockchain* comme des éléments de preuve ?

Me Nathalie Chiche. Pour qu'il y ait une présomption de fiabilité, il faut absolument qu'il y ait une signature qualifiée – il faut que l'on puisse utiliser une signature qualifiée et un horodatage qualifié, sans quoi la fiabilité sera à l'appréciation du juge.

M. Philippe Latombe, rapporteur. Cela veut-il dire que vous faites constater une inscription dans la *blockchain* par une profession réglementée de type huissier ?

Me Nathalie Chiche. Pas de type huissier. Il existe des tiers de confiance agréés pour qualifier une signature électronique. Ce ne sont pas des huissiers, ce sont des tiers de confiance certifiés – et le coût est assez élevé.

M. Philippe Latombe, rapporteur. Continuer à recourir à ce type de professions est-il la solution, ou est-ce en donnant une présomption de force probante, qu'on pourra se passer de ce type d'intermédiaires, relativement onéreux ?

Me Nathalie Chiche. Comme je l'ai dit, la *blockchain* a une force probante élevée. Je suis d'accord avec les conclusions du rapport de France Stratégie. Je ne pense pas que l'on puisse le remettre en doute. Le problème se situe au niveau de la présomption de fiabilité. Les éléments inscrits dans cette *blockchain* bénéficient-ils d'une présomption de fiabilité ? Pour cette fiabilité, il est nécessaire d'avoir recours à la signature électronique qualifiée et à l'horodatage électronique qualifié, sans quoi la fiabilité sera à l'appréciation du juge.

M. Philippe Latombe, rapporteur. Cela veut dire que l'on gardera ces prestataires agréés.

Me Nathalie Chiche. Sauf si l'on fait évoluer le Règlement eIDAS en disant que la *blockchain* dispose par nature d'éléments qui garantissent un haut niveau de fiabilité, et que l'on peut reconnaître la fiabilité de la signature électronique et de l'horodatage sur la *blockchain*.

M. Philippe Latombe, rapporteur. Comment les Italiens ont-ils fait ?

Me Nathalie Chiche. Je ne sais pas. Les Italiens ont des raisons qui ne sont pas les nôtres.

M. Philippe Latombe, rapporteur. À l'origine, c'était de l'anti-blanchiment.

Me Nathalie Chiche. Comme je l'ai dit en préambule, cela se situe surtout sur l'horodatage. Ils ont reconnu la fiabilité de l'horodatage de la *blockchain*. Je ne suis pas sûre qu'ils aient reconnu l'identification.

M. Philippe Latombe, rapporteur. À votre connaissance, y a-t-il d'autres pays européens qui réfléchissent à cela ?

Me Nathalie Chiche. Je précise que je ne suis pas un avocat spécialiste de la *blockchain*, mais je m'y intéresse. Vous le savez, j'ai signé des tribunes sur le sujet de la *blockchain*, mais surtout sur la gouvernance de l'Internet et de la *blockchain*. Je n'ai pas d'information sur les autres pays européens, ni sur la Chine, qui reconnaît, elle, la présomption de fiabilité.

M. Philippe Latombe, rapporteur. Dans l'audition précédente, il a été dit qu'il fallait développer des infrastructures au niveau européen, parce que nous étions un peu en retard, notamment par rapport aux Américains. Dans d'autres auditions, il nous a été expliqué que l'Europe ne pouvait trouver une voie entre la Chine et les États-Unis qu'en mettant en avant ses valeurs – le bon exemple étant le RGPD (Règlement général sur la protection des données). Peut-on cumuler les deux, et se dire qu'il faut que l'Europe développe des infrastructures avec des valeurs de gouvernance spécifiques et européennes ? Est-ce ainsi que l'on pourrait avoir un écosystème *blockchain* européen souverain ?

Me Nathalie Chiche. C'est justement le propos de mon projet de cas d'usage de la *blockchain*, d'inscrire le registre RGPD dans une *blockchain*.

M. Philippe Latombe, rapporteur. Cela fait référence à la tribune que vous avez publiée dans les *Échos* en août 2018.

Me Nathalie Chiche. L'idée était de trouver un socle commun, comme celui du RGPD, et de proposer de l'utiliser comme cas d'usage de la *blockchain*. L'avantage est qu'il est d'emblée applicable à tous les organismes établis en Europe, et même au-delà, puisque le RGPD est d'application extraterritoriale. Il s'applique aux organismes établis sur le territoire de l'Union européenne, que le traitement ait lieu ou non dans l'Union, mais il s'applique aussi aux organismes qui traitent des données à caractère personnel des personnes qui sont situées sur le territoire de l'Union, même si l'organisme n'est pas établi sur ce territoire, dès lors que ses activités sont liées à une offre de biens ou de services ou au suivi du comportement de ces personnes au sein de l'Union. Le spectre est très large. Il couvre énormément d'organismes publics et privés.

Cette idée m'est venue car je me suis dit qu'à l'instar du dirigeant d'une entreprise quelconque, qui a l'obligation d'établir un bilan comptable pour avoir une vision globale de la situation de son entreprise, et qui doit déposer ses comptes auprès du greffe du tribunal de commerce dont il dépend, depuis la mise en application du RGPD, tout dirigeant d'un organisme public ou privé a l'obligation de tenir un registre de ses activités de traitement. C'est l'article 30 qui le mentionne. Il a aussi l'obligation de mettre ce registre à la disposition de l'autorité de contrôle. J'ai fait une analogie entre le bilan comptable et le registre des activités de traitement, car ce sont des obligations légales. Dans ma pratique, je constate que le registre des activités de traitement n'est pas souvent tenu.

Ce registre se présente sous forme écrite, mais également sous forme électronique. Il est important de le préciser par rapport à ce que j'ai dit tout à l'heure quant à la preuve. Dans ma pratique, j'observe qu'il n'y a pour l'instant aucune sanction de la CNIL pour la non-tenue du registre. Je rappelle que ce registre est par excellence un outil de conformité au RGPD. Avant l'application du RGPD, c'était la CNIL qui tenait le registre national des traitements qui étaient déclarés et mis en œuvre par les organismes publics et privés. Tout un chacun pouvait demander la liste de tous les traitements ayant été déclarés à la CNIL par un organisme, ainsi qu'une copie du registre, si l'organisme avait désigné un CIL (correspondant informatique et libertés). Depuis l'application du RGPD, personne n'a accès au registre national, dont je rappelle qu'il a été gelé pour une dizaine d'années. Seule la CNIL peut y avoir accès, sur demande.

À mon avis, l'application de la *blockchain* au registre des activités de traitement permettrait d'avoir l'ensemble des registres des activités de traitement et aussi à tout le monde d'avoir accès aux registres, comme avant l'application du RGPD. La tenue et l'ancrage du registre RGPD sur *blockchain* permettraient surtout aux organismes publics et privés de démontrer que la tenue du registre est faite en toute transparence. Elles permettraient une certification et un horodatage du registre, en ligne avec les pratiques de la CNIL avant l'application du RGPD. Nous avons parfois besoin de nous assurer qu'un sous-traitant est en conformité avec le RGPD. Le fait d'avoir copie du registre pourrait rassurer un responsable de traitement.

Je rappelle que les greffiers des tribunaux de commerce utilisent la *blockchain* pour faciliter les changements et les évolutions des sociétés entre greffes, sans avoir recours aux notifications par mail, par lettre recommandée, etc. L'utilisation de la *blockchain* au registre RGPD pourrait créer un cadre de régulation unique au monde. Comme nous l'avons vu, le spectre est très large. De nombreux organismes publics et privés sont soumis au RGPD et doivent tenir un registre. Appliquer la technologie *blockchain* au registre RGPD pourrait être un nouveau cadre de régulation, unique au monde, pour garantir la sécurité, la datation et l'intégrité de ce registre utilisé par tous les organismes français, européens, et même internationaux, dès lors que leurs activités sont liées à une offre de biens ou de services, ou au suivi du comportement de ces personnes.

Pourquoi est-ce important ? Parce que ce cadre de régulation permettrait d'avoir accès même au registre des GAFA, en toute transparence, les GAFA devant répondre aux exigences listées à l'article 30. On saurait le nom du responsable de traitement, ou le cas échéant d'un représentant, on connaîtrait toutes les finalités du traitement, les catégories de personnes concernées, les catégories des données à caractère personnel. On connaîtrait les destinataires ayant accès aux données. Nous saurions s'il y a des transferts de données à caractère personnel, et nous connaîtrions les durées de conservation des différentes catégories de données. Nous aurions également une description générale des mesures techniques et organisationnelles de ces acteurs privés.

Cette régulation pourrait même être un modèle de référence, car, d'emblée, elle peut être mise en place au niveau européen, puisque le RGPD s'applique, et même à l'international. Elle pourrait même – pourquoi ne pas en rêver – devenir un standard européen de la *blockchain*.

M. Philippe Latombe, rapporteur. Dans votre tribune de 2018, vous l'envisagez au niveau français. Cela veut-il dire qu'il faudrait d'emblée le faire au niveau européen ?

Me Nathalie Chiche. Pour agir face à ces acteurs privés dont nous sommes si dépendants, il faut agir *a minima* au niveau européen. J'ai évolué depuis 2018 et je pense qu'il faut placer cette *blockchain* au niveau européen.

M. Philippe Latombe, rapporteur. Depuis 2018, avez-vous identifié d'autres cas d'usage, de cette importance, pour lesquels la *blockchain* pourrait être une solution, ce qui permettrait de « remettre de la souveraineté » dans le numérique en Europe ?

Me Nathalie Chiche. Oui, bien sûr. Vous m'avez présentée comme la rapporteure d'une étude sur la gouvernance d'Internet. J'avais écrit dans le journal *Le Monde* une tribune sur la technologie *blockchain* qui redistribue la gouvernance d'Internet. Nous avions constaté que les États-Unis, tellement convaincus d'avoir une responsabilité historique dans le fonctionnement et le développement d'Internet, voulaient une gouvernance de l'Internet, avec une association de droit privé californien, qui s'appelle l'ICANN, et qui est au centre du dispositif d'adressage (attribution des adresses IP) et de nommage (allocation des noms de domaines). Les adresses IP et les noms de domaines du monde entier sont centralisés dans un répertoire DNS, qui attribue à chaque adresse IP un nom de domaine. Depuis 2019, c'est l'ICANN qui gère ce répertoire DNS. C'est donc elle qui contrôle la ressource-clé de l'Internet, car si vous n'êtes pas répertorié sur Internet, vous n'existez pas.

Comme nous l'avons écrit dans cette tribune, M. Mehdi Benchoufi et moi-même, nous pensons que la technologie *blockchain* pourrait offrir une alternative à la gestion étatisée des noms de domaines ou DNS, sous la férule des États-Unis, et qu'elle viendrait en renfort de la société civile, là où les gouvernements n'ont pas les moyens d'assurer le respect de leurs normes dans le cyberespace. Il faut savoir que c'est une association de droit privé américain qui gère ces ressources critiques.

Comment pourrait-on faire ? Comme nous l'avons dit précédemment, la gestion des DNS par l'ICANN est structurellement liée à la gestion d'une ressource rare, qui est le nom de domaine, et donc à la nécessité d'en certifier l'authenticité et l'unicité. Il y a un seul nom de domaine pour l'Assemblée nationale : assemblée-nationale.fr. Or, la technologie *blockchain* a proposé en 2010 l'apparition d'un DNS centralisé et sécurisé, le .bit DNS, dont l'objectif est de veiller à ce qu'aucun gouvernement ni aucune personne ne puisse censurer ou attaquer ce service. C'est le même *coin* qui a été conçu pour créer un service de noms de domaines qui est basé sur la *blockchain*. Ce *coin*, qui est basé sur la technologie *blockchain*, permet une gestion robuste, sécurisée et parfaitement décentralisée des url, et concrétise la possibilité de soustraire la gouvernance de l'Internet, par les États-Unis, à une autorité centrale. Nous avons donc des alternatives à la gestion de l'ICANN par le même *coin*. Il convient d'adopter cette solution pour redistribuer la gouvernance de l'Internet, qui est à ce jour verrouillé par les États-Unis.

M. Philippe Latombe, rapporteur. L'écosystème de la *blockchain* en France et en Europe évolue-t-il de façon rapide et exponentielle, ou l'acculturation est-elle limitée pour les citoyens et les pouvoirs publics ? Comment jugez-vous l'écosystème ? Est-il loin de la

maturité ? Y a-t-il encore beaucoup d'efforts à faire pour expliquer ce qu'est cette technologie et à quoi elle peut servir ?

Me Nathalie Chiche. Comme je l'ai souligné tout à l'heure, il faut des cas d'usage de la *blockchain* pour que cette technologie puisse percer, surtout auprès des utilisateurs. La France a privilégié la technologie *blockchain* dans le domaine monétaire et financier. Nous l'avons vu dans le domaine de l'art, cela ne parle pas à tout un chacun. L'idée serait de trouver des cas d'usage dans notre vie quotidienne, comme je le disais tout à l'heure à propos de la chaîne alimentaire. Ce qui freine la technologie *blockchain*, c'est surtout cette insécurité juridique, et la question des moyens de preuve – d'où la nécessité de revoir le Règlement eIDAS.

M. Pierre-Alain Raphan. Dans ces auditions, nous allons techniquement très loin dans le détail. Nous parlons de gouvernance, nous essayons de réfléchir à un système de gouvernance, mais finalement, ces systèmes numériques sont-ils gouvernables ? Peut-on réguler un espace qui n'a pas de frontières sans une gouvernance globale qui serait partagée par l'ensemble des usagers et des utilisateurs ? Est-ce une utopie ? Peut-on avoir une gouvernance sur un territoire donné qui serait l'Europe, mais qui n'aurait pas forcément les mêmes objectifs que les autres régions du monde ?

Me Nathalie Chiche. Les réseaux numériques terrestres sont complètement dominés par des acteurs privés – américains ou chinois. Je ne vois pas comment nous pourrions reprendre la main sur ces réseaux numériques terrestres. Ce qui est encore plus grave, c'est l'actuelle guerre de souveraineté et de puissance entre les États, avec la privatisation de l'espace, la ruée satellitaire en orbite basse. Nous en avons beaucoup parlé avec le vol de notre astronaute français. Il se livre une guerre dans l'espace entre, d'un côté, des acteurs privés comme Amazon et Elon Musk, qui ont lancé respectivement 30 000 et 42 000 satellites, et de l'autre les Chinois. La guerre de positions a démarré à 400 mètres au-dessus de nos têtes. Avec la règle du « premier arrivé, premier servi », si la France et l'Europe ne se réveillent pas, nous allons être encore assujettis à ces acteurs privés américains et chinois, sans compter le défi environnemental que cela pose. Je suis un peu pessimiste. Si l'on n'utilise pas des outils, comme je l'ai proposé avec un registre RGPD qui pourrait être un standard, ou un DNS… Il est compliqué d'essayer de reprendre la main sur l'ICANN ; ce n'est pas que nous n'avons pas essayé. Il faut déjà regarder au-dessus de nos têtes pour avoir « un coup d'avance » en ce qui concerne notre souveraineté.

M. Pierre-Alain Raphan. Peut-on avoir « un coup d'avance » dans la régulation avec un système politique qui n'est pas forcément acculturé de manière globale à ces enjeux-là ? Nous nous en rendons compte tous les jours. Il faut regarder la vérité en face. Nous ne sentons pas que ces grands défis sont une préoccupation majeure. Ces sujets n'apparaissent pas comme des priorités dans la régulation, au moins nationale. On sent que l'Europe peut accuser une forme de retard, même si des efforts ont été réalisés. L'arrivée de M. Thierry Breton, par exemple, a pu accélérer certaines choses. Le temps politique est « à la traîne » – temps législatif, judiciaire – si on le compare au temps des affaires, au temps du numérique. Est-ce rattrapable ? Nous faisons parfois de la prospective avec certains étudiants et certains acteurs. Le système politique ne devrait-il pas être accompagné d'une Intelligence artificielle pour rattraper le retard ? De nombreuses questions se posent sur ces sujets.

M. Philippe Latombe, rapporteur. Comment voyez-vous les initiatives européennes – *Digital Markets Act (DMA), Digital Governance Act (DGA), Digital Services Act (DSA)* – ce triptyque tel qu'il est proposé aujourd'hui ?

Me Nathalie Chiche. Nous parlions tout à l'heure de la présentation de la stratégie *blockchain* au niveau national. La DGE (Direction générale des entreprises) était dans la boucle, je crois. L'ambition de la France était même de devenir un acteur majeur de la *blockchain*. Nous n'avons pas encore trouvé le cas d'usage qui permette de sensibiliser vraiment tous les utilisateurs à la *blockchain*. Il faut le trouver. Je vous ai proposé ce cas d'usage autour du RGPD, car il concerne tous les organismes publics et privés, en France, en Europe et à l'international, dès lors qu'il cible des personnes se trouvant sur le sol européen. Il faut trouver un cas d'usage qui serve d'électrochoc, et je ne pense pas que nous l'ayons trouvé pour l'instant.

M. Pierre-Alain Raphan. Ne peut-il pas porter sur les sujets de l'identité numérique ? Tout le monde en parle, cela peut peut-être aider. Il y a peut-être un enjeu en ce qui concerne les données de santé au niveau européen.

Me Nathalie Chiche. À quoi pensez-vous ?

M. Pierre-Alain Raphan. Au partage des données de santé. On en revient à l'insécurité.

Me Nathalie Chiche. Non, pas à l'insécurité, surtout à la souveraineté. Vous l'avez souligné, M. le rapporteur, dans une tribune sur le *Health Data Hub*. Pour l'instant, nous ne sommes pas encore rassurés qu'un acteur privé américain puisse héberger nos données de santé en France. Il faudrait déjà y remédier. Je pense que cela va être le cas, mais cela prend du temps.

M. Philippe Latombe, rapporteur. M. Éric Bothorel, qui fait partie de la mission, a rendu un rapport sur l'*open data* et les *open sources*. Selon vous, est-ce quelque chose qui permettrait, avec la *blockchain*, de mettre de la transparence et de la bonne gouvernance au sein de l'État ?

Me Nathalie Chiche. Oui, je le crois. Cette *blockchain*, qui serait dédiée au registre des activités de traitement, serait en *open data*. Elle permettrait d'avoir accès à toutes les informations. En tant que *data protection officer*, je me suis rendu compte que depuis l'application du RGPD, il y avait un recul de la transparence. Avant, nous avions accès à tous les traitements déclarés à la CNIL. Nous avions accès au registre, dès lors qu'un organisme avait désigné un CIL. Maintenant, depuis l'application du RGPD, nous n'avons plus accès à rien, sauf la CNIL sur demande. Il y a bien un recul de la transparence. Je pense que celle-ci est importante pour être informé et surtout pour restaurer la confiance des utilisateurs.

M. Philippe Latombe, rapporteur. L'État doit-il se saisir de la *blockchain* pour cette transparence, qui est de plus en plus demandée par les citoyens ? L'utilisation de la *blockchain* doit-elle devenir un réflexe pour l'État ?

Me Nathalie Chiche. La *blockchain* permet de se passer d'intermédiaires, de ces acteurs privés. Oui, bien sûr, je recommande l'utilisation de la *blockchain*. L'État devrait systématiquement y avoir recours pour essayer de se dégager de ces acteurs privés qui ont la mainmise sur notre économie.

M. Philippe Latombe, rapporteur. Aujourd'hui, beaucoup de villes et de territoires ont décidé de mettre en place des *smart cities*. Ils ont d'ailleurs des leviers de financement pour le faire. Cela représente des masses de données extraordinairement importantes. La *blockchain* y a-t-elle sa place ? Selon vous, le réflexe *blockchain* est-il suffisamment présent dans les *smart cities*, ou est-ce que l'on passe complètement à côté ?

Me Nathalie Chiche. Je n'en connais pas. Je ne suis pas une spécialiste de la *blockchain*, mais de la protection des données. Pourquoi pas ? Toutefois, cela passerait tout de même par le registre, qui permet d'écrire tous les traitements qui sont faits. Ces *smart cities* occasionneraient des traitements.

M. Philippe Latombe, rapporteur. Oui, sur la question de l'attribution des places de crèche, le paiement de la cantine, etc., qui sont des données avec des traitements.

Me Nathalie Chiche. Selon moi, la *blockchain* possède deux vertus, de par sa technologie : elle restaure la confiance et permet la transparence.

M. Philippe Latombe, rapporteur. Y a-t-il un point que nous n'avons pas évoqué et que vous voudriez mettre en avant lors de cette audition ?

Me Nathalie Chiche. Nous sommes à un an de l'élection présidentielle. Les enjeux du numérique étant très importants, il serait bien de se doter d'un ministère du numérique de plein droit et d'essayer de faire du numérique une priorité pour le gouvernement. Quel meilleur gage que d'avoir un ministère d'État du numérique ?

M. Philippe Latombe, rapporteur. Y aurait-il une initiative législative urgente à prendre – pas uniquement en ce qui concerne la *blockchain* ?

Me Nathalie Chiche. Oui, il faudrait modifier le Règlement eIDAS, pour qu'il reconnaisse au moins la *blockchain*.

M. Philippe Latombe, rapporteur. Nous rencontrerons jeudi prochain le ministère de l'Économie et des Finances.

Me Nathalie Chiche. Allez-vous interviewer le ministère de la Justice ?

M. Philippe Latombe, rapporteur Cela fait partie des auditions envisagées concernant l'évolution législative et les initiatives à cet égard.

Audition, ouverte à la presse, de Mme Liliane Dedryver, directrice de projets « Technologies et solutions numériques émergentes » du service de l'économie numérique à la direction générale des entreprises (DGE), et de Mme Pauline Faucon, adjointe au responsable du pôle « Affaires internationales, coordination européenne et enjeux technologiques du secteur financier », MM. Thimothée Huré, bureau « Épargne et marché financier » (FinEnt1), et Clément Robert, bureau « Services bancaires et moyens de paiement » (BancFin4), de la direction générale du Trésor (DGT) (ministère de l'économie, des finances et de la relance)
(29 avril 2021)

Présidence de M. Philippe Latombe, rapporteur

M. Philippe Latombe, président et rapporteur. Nous avons le plaisir d'auditionner la *task force blockchain*, pilotée par le ministère de l'économie, des finances et de la relance. La création de ce groupe d'experts nationaux, en avril 2019, dans le cadre de la stratégie nationale *blockchain*, a fait suite au rapport qu'ont consacré à cette technologie les parlementaires M. Jean-Michel Mis et Mme Laure de la Raudière. La *task force blockchain* rassemble des administrations et investisseurs publics, dont plusieurs ministères, Bpifrance, la caisse des dépôts et consignations, l'autorité des marchés financiers (AMF), l'autorité de contrôle prudentiel et de résolution (ACPR) des représentants de comités stratégiques de filières, des pôles de compétitivité, des associations et des représentants du monde académique, parmi lesquels le commissariat à l'énergie atomique et aux énergies alternatives (CEA), l'Institut national de recherche en sciences et technologies du numérique (Inria), l'Institut de physique (INP) et l'université Paris Dauphine.

La *task force blockchain* a présenté un premier rapport au mois de février 2020, à partir d'une étude menée par sept chercheurs de l'Institut Mines-Télécom (IMT), du CEA-List et de l'Inria. Je ne doute pas que vous nous en direz un mot.

Je souhaite vous interroger, à titre liminaire, sur trois sujets. Je commencerai par votre approche de la souveraineté numérique, objet d'une question rituelle lors de nos auditions, du fait de la grande diversité des définitions qui en sont données. Comment l'envisagez-vous pour votre part ? En quoi la *blockchain* pourrait-elle constituer un outil de souveraineté en France et en Europe ? J'aimerais, à cette occasion, que vous nous présentiez dans le détail les premiers constats effectués par la *task force blockchain*, ainsi que ses recommandations.

Mon second point portera sur le développement en France d'un écosystème *blockchain* performant. Quelles actions devraient mener les pouvoirs publics pour soutenir les entreprises technologiques porteuses de projets dans ce domaine ? Comment la réglementation actuelle pourrait-elle, ou devrait-elle évoluer pour encourager l'innovation ? Comment la crise sanitaire a-t-elle impacté cet écosystème d'entreprises si particulier ? Comment celles-ci envisagent-elles leur proche avenir, au vu des circonstances actuelles ?

Enfin, je voudrais que nous échangions à propos de la dimension européenne de la *blockchain*. D'une part, je m'interroge sur le positionnement de la France vis-à-vis de cette technologie, par rapport à ses voisins européens. Je souhaite, d'autre part, connaître votre opinion sur l'action de l'Union européenne dans ce domaine. Nous évoquerons sans doute au passage l'enjeu de la force probante de la *blockchain*, d'une grande importance pour nous, législateurs.

Mme Liliane Dedryver, directrice de projets « Technologies et solutions numériques émergentes » du service de l'économie numérique à la direction générale des entreprises (DGE) (ministère de l'économie, des finances et de la relance). La direction générale du Trésor pourrait commencer par aborder la question sous ses aspects financiers les plus connus, puisqu'ils ont fait l'objet d'une réglementation dans la loi Pacte (loi relative à la croissance et la transformation des entreprises).

M. Timothée Huré, bureau « Épargne et marché financier » (FinEnt1), de la direction générale du Trésor (DGT) (ministère de l'économie, des finances et de la relance). Vos questions portent sur la technologie *blockchain*, or celle-ci ne concerne pas que des aspects financiers, puisqu'elle peut être déployée dans de nombreuses industries. La DGT ne sera en mesure de vous apporter qu'une réponse restreinte. Elle ne suit en effet que des entreprises utilisant la technologie *blockchain* à des fins financières, par exemple pour réaliser des paiements, échanger des actifs numériques ou cryptoactifs ou, éventuellement, de la monnaie sous forme de token, de la monnaie de banque centrale tokenisée ou encore des titres financiers.

Nous ne traitons pas des entreprises de l'industrie *blockchain* en général, mais uniquement de celles qui recourent à cette technologie dans un contexte financier. Nous n'en avons pas moins un message à délivrer, car nous avons progressivement mis en place un cadre national, de portée croissante, depuis qu'il fait l'objet de discussions au niveau européen.

Ce cadre englobe les actifs numériques apparus en même temps que la *blockchain* et désignés sous le vocable contestable de « cryptomonnaies », comme bitcoin ou Ethereum. Ces tokens, initialement de paiement, sont rapidement devenus des objets de spéculation. Échappant par ailleurs au droit existant, ils ont parfois servi à des fins criminelles (blanchiment d'argent ou financement du terrorisme).

Plusieurs réglementations se sont succédé. La première visait à lutter contre le blanchiment d'argent et le financement du terrorisme, sous l'égide internationale du Groupe d'action financière (GAFI), dont la France est membre et qui dépend de l'Organisation des nations unies (ONU). En 2015, une cinquième directive de la Commission européenne, relative à la lutte contre le blanchiment des capitaux et le financement du terrorisme, a ensuite couvert une partie des activités liées aux cryptoactifs. La loi Pacte a transposé l'ensemble en droit français en imposant l'assujettissement d'une partie des acteurs qui vendent, achètent ou conservent des cryptoactifs.

La sécurisation des données relatives aux actifs numériques constitue un enjeu crucial. Il faut, pour accéder à ceux-ci, des clés privées, sortes de mots de passe, dont la perte ou le vol prive de tout contrôle sur ces cryptoactifs. Voilà pourquoi les prestataires proposant de sécuriser les portefeuilles d'actifs numériques ont été à leur tour assujettis au dispositif relatif à la lutte contre le blanchiment d'argent.

Une ordonnance promulguée le 9 décembre 2020 a étendu ce premier socle réglementaire, qui englobe désormais à peu près tous les acteurs se livrant à l'échange, la négociation ou la conservation de cryptoactifs.

La France a poussé la lutte contre le blanchiment d'argent plus loin que d'autres pays membres de l'Union européenne. Se pose aujourd'hui la question d'une révision des textes européens, encore incomplets. Ils comportent moins d'exigences que les textes français, quant au type d'entité éligible ou à l'imposition d'un contrôle préalable à l'exercice de l'activité. Des négociations porteront, à partir de juin, sur les propositions de Règlement que devrait nous soumettre l'Union européenne.

Par ailleurs, le contexte actuel d'envolée du cours du bitcoin depuis la fin de l'année 2020 laisse présager un risque que certaines personnes mal informées placent des sommes conséquentes auprès d'entités peu scrupuleuses. Le deuxième aspect de la réglementation de la technologie *blockchain*, visant à la protection de l'épargne, rejoint la réglementation classique en matière de marchés financiers et de souscription à des produits d'épargne. La France a décidé, *via* la loi Pacte, de soumettre à un agrément les prestataires d'achat et de vente de cryptoactifs.

L'originalité de la position française vient du caractère optionnel de ce cadre, largement inspiré du droit financier classique. Les législateurs ont craint qu'au cas où la France serait le seul pays à contraindre les entreprises de l'industrie des cryptoactifs à obtenir un agrément à l'issue d'une procédure lourde, semblable à celle qui pèse sur les prestataires de services d'investissement classiques, celles-ci finiraient par s'installer ailleurs.

Ce cadre optionnel permet aux prestataires qui le souhaitent de se démarquer, leur choix de s'y plier témoignant dès lors de leur sérieux. Selon nous, ce cadre ne doit devenir obligatoire qu'à condition qu'il s'impose aussi au niveau européen. Nous en discutons justement à l'occasion du Règlement MiCA (*Market in Crypto-Assets*), proposé par la Commission européenne à l'automne et maintenant en débat, tant au Parlement européen qu'au Conseil européen. M. Clément Robert et moi-même participons aux négociations.

Le troisième aspect de la réglementation ne porte pas sur les objets apparus avec la *blockchain*, à savoir les cryptoactifs, mais sur l'utilisation de la *blockchain* à des fins auxquelles servaient auparavant d'autres technologies. L'échange de titres financiers implique traditionnellement une série d'intermédiaires : les chambres de compensation. Celles-ci s'assurent, lors de l'achat d'un titre financier, que son détenteur en est bien propriétaire et que l'acquéreur dispose de la somme requise. Elles assument ainsi une position de notaire.

Certains se sont avisés de la possibilité, grâce à la *blockchain*, d'accélérer considérablement ce processus d'échange, d'une durée allant parfois jusqu'à deux jours, malgré la dématérialisation des titres financiers. Autrement dit, l'usage de la technologie *blockchain* en tant que « tuyau » d'échanges de titres financiers entraînerait un gain de temps, en particulier dans les marchés peu liquides.

En France, une ordonnance de 2017 autorise à utiliser la technologie *blockchain* pour échanger des titres financiers, essentiellement non cotés, à savoir des parts de fonds correspondant à un segment restreint du marché. Recourir à la *blockchain* sur le marché des titres cotés en bourse présenterait également un intérêt évident. Si la France ne le permet pas, c'est parce que prévaut dans ce domaine le droit européen. Seul un Règlement européen autoriserait à modifier en ce sens la loi française.

Des discussions portent actuellement sur un projet parallèle au Règlement MiCA, auquel la Commission européenne a donné le coup d'envoi à l'automne. Il s'agit d'un régime pilote proposant, pendant cinq ans, aux acteurs qui le souhaitent, une dérogation aux règles européennes, le temps pour eux de tester la technologie *blockchain* comme moyen d'échange de titres financiers.

Une nouvelle classe d'actifs numériques est apparue, voici un an et demi : les *stablecoins*. Il a beaucoup été question d'eux à l'occasion du projet Libra, à l'origine de nombreuses craintes justifiées, notamment de la part des autorités publiques. Le Règlement MiCA s'intéresse également à ces *stablecoins*. Plusieurs ministres de la zone euro se sont publiquement dits inquiets de monnaies privées prenant le pas, à terme, sur des monnaies publiques. La question est en ce moment débattue au Conseil européen, voire au Parlement

européen. Il est de notre intérêt de nous assurer que ces *stablecoins* ne supplanteront pas et ne concurrenceront pas les monnaies nationales. Il convient de ne pas faire de fausses promesses à ceux qui en attendraient autant de stabilité que d'une monnaie publique.

M. Clément Robert, bureau « Services bancaires et moyens de paiement » (BancFin4), de la direction générale du Trésor (DGT) (ministère de l'économie, des finances et de la relance). J'apporterai une précision à propos du paysage global des cryptoactifs.

Ceux de première génération, comme les fameux bitcoins, à l'origine conçus comme des moyens de paiement, ont donné lieu à des échanges à des fins plutôt spéculatives ou d'investissement. La dimension de paiement s'est toutefois introduite dans le débat sur le Règlement MiCA, où elle occupe une place croissante. Les cryptoactifs de première génération ont finalement peu servi à des paiements, du fait de leur volume global réduit et de leur forte volatilité, illustrée par les fluctuations quotidiennes du cours du bitcoin.

Sur fond de projet Diem (au départ Libra), le constat s'impose que les *global stablecoins* – actifs numériques de deuxième génération – entendent surmonter les deux limites qui s'opposaient à l'usage, en tant que moyen de paiement, de ceux de première génération. D'une part, leur valeur promet de rester stable, d'autre part, le circuit de commerçants qui les accepteront est appelé à s'étendre.

Peu de commerçants recevaient jusqu'à présent des cryptoactifs comme moyens de règlement, même si le nombre de ceux qui reconnaissent la valeur du bitcoin augmente depuis peu. Les *global stablecoins*, dont Diem pourrait constituer le premier exemple type, amorçant le passage à une autre dimension. En s'appuyant sur les deux milliards et demi d'utilisateurs de Facebook, Diem pourrait en effet se déployer à une échelle inédite. Beaucoup plus de commerçants l'accepteraient alors, au point qu'en tant qu'actif de paiement privé, il concurrencerait l'euro.

M. Philippe Latombe, rapporteur. Vous avez déclaré, à propos de l'ordonnance du 9 décembre 2020 concernant la lutte contre le blanchiment d'argent, que la France était allée plus loin que ses voisins européens, notamment *via* le contrôle *a priori* des acteurs du secteur.

L'écosystème de la *blockchain* estime que la position trop avancée de la France, quant à ces questions d'encadrement, s'oppose à la volonté de substituer Paris à Londres en tant que place financière de l'Europe, au lendemain du Brexit. Ne voyez-vous pas, vous aussi, une incohérence entre la réglementation française plus poussée que celle de ses voisins et notre ambition nationale, qui porte, en l'occurrence, sur un aspect de notre souveraineté ?

M. Timothée Huré. Ce genre de réflexion nous est déjà parvenu, évidemment. Nombre d'acteurs du secteur nous ont signalé qu'ils échapperaient, à l'étranger, aux contrôles pesants que leur impose la loi française. Notre réglementation s'est élaborée à partir du raisonnement suivant : les professions financières sont traditionnellement contrôlées en France, il n'y a donc pas lieu de distinguer les nouveaux opérateurs des acteurs classiques du secteur.

Nous avons également songé au risque, pour ces acteurs émergents, parfois de très petite taille, que dès le lendemain de leur début d'activité, l'autorité des marchés financiers (AMF) ou l'autorité de contrôle prudentiel et de résolution (ACPR) les soumette à un contrôle, sans qu'un examen préalable leur ait garanti de le réussir, ce qui les exposerait à des sanctions des plus dissuasives.

Enfin, les entreprises *blockchain* entretiennent avec le secteur bancaire des relations parfois difficiles, en raison de la crainte de celui-ci de voir sa responsabilité engagée en matière de blanchiment d'argent ou de financement du terrorisme. Nous avons songé qu'un contrôle exigeant, *a priori*, rassurerait les acteurs bancaires, qui accepteraient ainsi plus volontiers d'entrer en relation avec les opérateurs du marché des cryptoactifs.

Reconnaissons toutefois que nos partenaires européens n'ont pas forcément opté pour le même type de contraintes.

L'ordonnance du 9 décembre 2020 prévoit de ce fait un allègement du contrôle *a priori* pour certains services. Les nouveaux assujettis y échapperont quant à eux : ils n'en auront en tout cas pas besoin pour exercer leur activité, même si, en cas de contrôle ultérieur, ils devront prouver leur respect des normes en vigueur.

Nous décelons une volonté de l'ensemble des pays de l'Union européenne d'opter pour la même approche, imposant à leur tour un contrôle *a priori*, auquel cas la France n'aurait plus qu'à affronter une concurrence réglementaire limitée.

M. Philippe Latombe, rapporteur. Pour autant, les relations avec le secteur bancaire ne se sont pas améliorées. Comment les rendre plus fluides ? Des acteurs de l'industrie *blockchain* nous ont indiqué qu'aucune banque ne se montrait prête à les soutenir et qu'ils rencontraient toutes les difficultés du monde à survivre, la transformation de leurs jetons en euros s'annonçant hors de question. Pourquoi cette méfiance persistante du secteur bancaire, malgré l'ordonnance censée apaiser les tensions ?

M. Timothée Huré. D'abord, toutes les banques ne partagent pas la même vision. Hier encore, la Société Générale a publié un communiqué à propos des *blockchains*. Certaines banques attestent d'une grande ouverture à cette technologie et participent à la mise en place d'un premier type de *stablecoin*. La Société Générale travaille sur un projet d'euro digital avec la Banque de France. Elle a participé hier ou avant-hier à l'émission d'obligations de la banque européenne d'investissement (BEI).

Toutes les banques ne se montrent donc pas hostiles au secteur. Certaines y voient une piste de développement prometteuse. Les directions de la conformité des banques manifestent cependant une véritable frilosité, difficile à surmonter. Elles se sentent mal à l'aise, pour des raisons parfois historiques, vis-à-vis de ce secteur à la réputation encore quelque peu sulfureuse, à tort selon nous, vu que le cadre réglementaire en place garantit le sérieux des acteurs enregistrés auprès de l'AMF et de l'ACPR.

Il reste un travail de concertation à mener. Nous l'avons tenté, de même que l'AMF et l'ACPR. Nous œuvrons, à notre niveau administratif et à celui du ministère, au dépassement des incompréhensions mutuelles. Nos efforts s'avèrent d'autant plus ardus que certaines directions des conformités, échaudées par leurs déboires passés, ne veulent plus prendre, en gérant les acteurs de l'industrie de la *blockchain*, de risques qu'elles jugent démesurés, bien que nous ne partagions pas leur analyse.

M. Philippe Latombe, rapporteur. Les établissements bancaires ne sont pas les seuls en cause. La Banque centrale européenne (BCE) ne paraît pas des plus ouvertes à l'usage de la *blockchain* ; la Réserve fédérale des États-Unis (FED) l'est peut-être un peu plus. Ne pressentez-vous pas un risque à trop attendre avant que la France s'engage dans la technologie *blockchain* ? La nécessité de rattraper notre éventuel retard menacerait alors notre souveraineté.

M. Timothée Huré. Je ne saurais m'exprimer à la place de la Banque centrale ou de la Banque de France. Je vous conseille en tout cas de vous adresser à cette dernière, qui ne donne pas, à la DGT, l'impression de vouloir laisser passer l'opportunité de la technologie *blockchain*. En témoignent ses expérimentations et sa participation à l'émission, par la Banque européenne d'investissement, de monnaie digitale de banque centrale. La BCE mène, si ce n'est des réflexions, du moins des consultations sur le sujet.

M. Clément Robert. Je ne dispose pas d'éléments plus précis. En revanche, je partage le sentiment de M. Timothée Huré quant à l'attitude de la Banque de France, où ne transparaît, selon moi, aucune réserve quant aux expérimentations d'émissions.

M. Philippe Latombe, rapporteur. En sommes-nous arrivés au même point que nos voisins européens ? Certains sont-ils plus avancés que la France, en matière de réglementation de la *blockchain*, mais aussi en termes de cas d'usage ?

M. Timothée Huré. Côté financier, la France est à la pointe. Notre avance, du point de vue de la réglementation, répond à une demande de notre écosystème, très engagé sur le sujet. C'est parce que nous l'avons mise au point plus tôt que nos partenaires européens que des acteurs de l'industrie *blockchain* ont pu se lancer dans l'échange de titres non cotés. Des expérimentations ont débuté bien avant le projet de régime européen en cours de négociation, qui ne verra de toute façon pas le jour avant l'an prochain. En réalité, les acteurs français que nous rencontrons régulièrement se disent satisfaits du positionnement de la France. Nous avons fait tout notre possible, compte tenu de la marge de manœuvre nationale dont nous disposions, pour leur permettre d'exercer confortablement leur activité. Le débat porte désormais sur les moyens à mobiliser afin d'avancer suffisamment vite au niveau européen pour ne pas nous laisser distancer par les États-Unis et l'Asie. Quoi qu'il en soit, la France n'a pas à rougir de sa position en Europe.

M. Philippe Latombe, rapporteur. La crise sanitaire a-t-elle apporté des changements ? A-t-elle freiné ou, à l'inverse, accéléré le développement du secteur ?

M. Timothée Huré. Nous avons observé des mouvements contraires. Certaines activités annexes, telles que le conseil en matière de cryptoactifs, ont plutôt souffert, comme beaucoup de ce genre durant la crise. En revanche, l'achat, la vente et la négociation de cryptoactifs ont suscité une recrudescence d'intérêt de la part des consommateurs, qui ont dans l'ensemble plus investi. Le même constat vaut pour les titres financiers classiques. Nombre d'épargnants ont réalisé leurs premiers investissements pendant la crise liée au Covid. Entre le premier confinement et la forte envolée du bitcoin à la fin de l'année 2020, confirmée au début de 2021, les vendeurs et négociants de cryptoactifs n'ont pas souffert, au contraire.

M. Philippe Latombe, rapporteur. La crise sanitaire se serait donc accompagnée d'un mouvement de fond au profit des cryptoactifs. À quoi l'attribuez-vous : à un excédent de trésorerie dû au recul de la consommation, à une défiance envers les actifs classiques, ou encore à une inquiétude vis-à-vis de la dette Covid contractée par la France pour relancer l'économie ?

M. Timothée Huré. Le premier confinement n'a pas, selon notre analyse, donné lieu à une concurrence entre le bitcoin et les titres financiers classiques. Autrement dit, l'attrait des cryptoactifs ne s'est pas renforcé au détriment des autres types d'actifs : nous avons également observé une augmentation du nombre d'ordres passés sur les titres financiers classiques. De nouveaux investisseurs, ne disposant que d'un petit capital, se sont mis à jouer en bourse ou à ouvrir des plans d'épargne en actions (PEA), parce qu'ils disposaient enfin de temps pour se lancer.

En revanche, vers la fin de l'année 2020, un mouvement très net est apparu en faveur des cryptoactifs. Des investisseurs, plutôt jeunes, ont vu la valeur de certains d'entre eux décupler. De belles histoires ont circulé, de spéculateurs engrangeant des bénéfices mille fois supérieurs à leur mise de départ. L'impression s'est imposée que les cryptoactifs constituaient un moyen de s'enrichir facilement. Rappelons que le bitcoin est un actif purement spéculatif. Beaucoup s'y intéressent, car peu d'actifs ont permis de réaliser de telles plus-values.

M. Philippe Latombe, rapporteur. Quel avenir, à moyen et long terme, voyez-vous aux cryptoactifs ? Leur progression continuera-t-elle ? S'inscriront-ils dans le paysage en tant que simple classe d'actifs parmi d'autres ? Domineront-ils le marché ? Ou leur popularité, peut-être éphémère, s'explique-t-elle par un effet de mode ?

M. Timothée Huré. La réponse dépend des actifs que l'on considère. La valeur du bitcoin, un actif spéculatif, repose sur l'offre et la demande, or l'offre disponible est limitée. De plus en plus de bitcoins apparaissent sur le marché, mais leur émission, plafonnée, suit une courbe asymptotique, alors même qu'une forte demande persiste, parce que beaucoup de belles histoires circulent, d'enrichissement subit, et que certaines grandes banques américaines, ou même Elon Musk, ont investi dedans. En réalité, sa valeur sur le marché s'est décorrélée de sa valeur intrinsèque ou de sa valeur d'usage, à l'instar de ce qui est arrivé à l'or. Le bitcoin pourrait ainsi devenir une valeur refuge comme l'or. La remarque vaut pour les autres cryptomonnaies.

Par ailleurs, il faut garder à l'esprit que les cryptoactifs possèdent une valeur en tant que moyens d'échanger de la donnée ou de l'information. Au-delà de la spéculation sur les unités de compte qui circulent sur les *blockchains*, celles-ci permettent d'échanger des objets connus, tels des titres financiers. Il ne faut donc pas uniquement envisager cette technologie du point de vue de la valorisation des actifs qui y transitent. Nous sommes convaincus, en France, et nous ne sommes pas les seuls en Europe, de la remarquable utilité de la technologie *blockchain* en vue de la modernisation des marchés financiers classiques ou des échanges, au travers de celle des moyens de paiement.

Je distinguerai donc entre, d'un côté, des cryptoactifs tenant lieu de valeurs refuges et, de l'autre, une technologie prometteuse. Malgré les critiques visant Diem (à l'origine Libra) et les risques liés à son développement, ce projet a mis en évidence des manques ou insuffisances des moyens disponibles auprès du grand public pour échanger rapidement de la valeur au moindre coût.

Nous voyons en résumé un intérêt technologique à développer le secteur et à permettre aux acteurs qui le souhaitent d'utiliser la technologie *blockchain*.

M. Philippe Latombe, rapporteur. Vous avez cité deux exemples de cryptoactifs : bitcoin et Ethereum. Où en sont aujourd'hui les *blockchains* européennes ? Comment faire pour qu'elles se hissent au niveau du bictoin en servant à leur tour de valeur refuge ?

M. Timothée Huré. Je laisserai la DGE compléter mon propos au sujet de la stratégie de déploiement de la technologie *blockchain* pour ses usages techniques.

Nous ne cherchons pas forcément à créer, en Europe, un token constituant une valeur refuge. En revanche, nous souhaitons vivement disposer de solutions européennes de paiement ainsi que de *blockchains* facilitant l'échange de titres financiers. Nous ne sommes ni favorables ni hostiles à la création d'un bitcoin ou d'un Ethereum européens, qui incombe de toute façon au secteur privé. Nous voulons avant tout des *blockchains* européennes qui puissent servir d'outils souverains.

Nous ne sommes d'ailleurs pas en reste, de ce point de vue. Le lancement du projet de *blockchain* franco-suisse Tezos a rencontré, voici quelques années, un beau succès, attesté par une levée de fonds magistrale. Tezos commence aujourd'hui à être utilisé pour échanger des titres financiers. Il me semble que la Société Générale ou la BEI y ont eu recours récemment. Nous entretenons en tout cas des contacts réguliers avec les gestionnaires de Tezos.

Un enjeu majeur émerge, lié à une règle quelque peu complexe instaurée par le GAFI, visant à s'assurer de l'identification des émetteurs de cryptoactifs, un peu comme lors d'un virement bancaire, *via* le code Swift (de la *Society for Worldwide Interbank Financial Telecommunication*), de manière à éviter tout problème d'anonymat. Cette règle oblige à communiquer l'identité de chaque personne qui envoie ou reçoit des cryptoactifs *via* une *blockchain*. Or la conception initiale de la technologie *blockchain* ne le prévoyait pas, d'où l'enjeu de disposer de structures qui ne soient pas uniquement américaines ou asiatiques et comportent un système équivalent au code Swift, capable de transmettre les données, d'une banque ou d'un intermédiaire financier à l'autre. Il n'existe pas encore, à ce jour, de projet européen abouti de ce point de vue, ce qui nous préoccupe d'ailleurs. Une crainte subsiste d'une dépendance vis-à-vis de solutions *blockchain* non européennes.

M. Philippe Latombe, rapporteur. Je laisserai la DGE s'exprimer sur la question de notre écosystème *blockchain*. En quoi consiste-t-il aujourd'hui ? Comment se porte-t-il ? Comment le développer ?

Mme Liliane Dedryver. Je reviendrai d'abord sur la définition de la souveraineté numérique, proposée par le directeur général de la DGE, M. Thomas Courbe. Elle repose, selon lui, sur deux facultés. La première est de définir librement les règles encadrant les usages du numérique, afin de contrôler leur impact, sur les entreprises, mais aussi sur les consommateurs et citoyens. De ce point de vu, l'intervention de l'État a plutôt porté, en France, sur l'aspect financier, *via* la loi Pacte.

La seconde faculté cruciale pour la souveraineté numérique de la France implique une autonomie relative par rapport aux principales technologies à la base des usages du numérique. Concernant ce volet, le principal levier, pour la DGE, consiste à développer des stratégies industrielles du numérique permettant de soutenir transversalement la production de solutions innovantes par des acteurs français.

La stratégie nationale *blockchain* est intervenue suivant cet axe. Lancée en avril 2019, elle vise d'abord le développement des usages non financiers de la technologie *blockchain* et la croissance de l'écosystème d'entreprises françaises. Elle s'articule autour de quatre axes clés :

– la création de débouchés, que la DGE soutient, à la fois en accompagnant la filière, notamment dans les comités stratégiques de filières (CSF) qu'elle pilote, et en organisant, avec les acteurs, des cycles de réunions autour du partage d'information et de retours d'expérience ;

– le financement des porteurs de projets. Si les *blockchains* à usage financier ont procédé à d'importantes levées de fonds, un besoin subsistait toutefois de soutien public aux *blockchains* à usage non financier. La DGE, avec l'appui de Bpifrance, accompagne les entreprises par des subventions et des prêts ;

– l'accompagnement des entrepreneurs *blockchain*. La DGE facilite ainsi les échanges entre les différentes administrations compétentes et les *start-up* ;

– les ministres, M. Cédric O, Mme Frédérique Vidal et M. Bruno Le Maire, ont confié une mission prospective à des chercheurs de l'Inria, du CEA-List et de l'IMT. Elle a donné à lieu à la publication, le 15 avril dernier, d'un rapport sur les verrous technologiques des *blockchains*, assorti de recommandations aux pouvoirs publics en vue de les lever.

L'écosystème de la *blockchain* en France est en train de se consolider. Nous constatons un authentique dynamisme des *start-up*, ainsi qu'une appropriation progressive, par les grands groupes, de la technologie *blockchain*, ce qui nous laisse présager une augmentation des débouchés de l'industrie de la *blockchain* en France.

Le réseau foisonnant des *start-up* de l'industrie de la *blockchain* a réussi à faire face à la crise, dans certains cas grâce à l'accompagnement de l'État. Le rapport des chercheurs que je viens d'évoquer a dressé une première cartographie des acteurs de la *blockchain* en France, dénombrant une centaine de start-up vers la fin de l'année 2019 et le début de 2020. Au début de 2021, en revanche, Bpifrance relevait environ 400 *start-up* en France. Bien que toutes n'atteignent pas la même taille ni le même potentiel, la progression ne laisse aucun doute.

Ce foisonnement des *start-up* s'accompagne d'une consolidation de l'écosystème, *via* la structuration de sa représentation. La France peut se féliciter de compter deux associations représentant les intérêts des différentes entreprises de l'écosystème de la *blockchain* : l'association pour le développement des actifs numériques (ADAN), à la création relativement ancienne, et la fédération française des professionnels de la *blockchain* (FFPB), qui a vu le jour en 2020.

Malgré un petit ralentissement pendant la crise, les débouchés continuent à se développer grâce à une acculturation croissante des grands groupes et des intégrateurs de solutions. Pour accompagner cette croissance, la DGE travaille, au sein de la *task force blockchain*, à l'élaboration de guides de sensibilisation.

M. Philippe Latombe, rapporteur. Les grandes entreprises ont-elles intégré la technologie blockchain ? Tournent-elles leurs regards vers les *start-up* ?

Mme Liliane Dedryver. Nombre de multinationales et de grands groupes français commencent à tester la technologie *blockchain* et lancent des chantiers. Certaines sociétés font appel à des *start-up* françaises pour les aider à développer leurs services.

Des projets ont éclos dans les comités stratégiques de filières (CSF). La DGE accompagne pour l'heure cinq projets de filières, dont ceux du CSF industrie des nouveaux systèmes énergétiques et du CSF transformation et valorisation des déchets. D'autres projets suivent leur cours dans le secteur de la technologie juridique ou au service du droit (*LegalTech*) ainsi que dans celui des industries culturelles et créatives. Certains projets s'épanouissent enfin dans le secteur du luxe.

Parmi les entreprises ayant déjà noué des collaborations avec les acteurs de l'industrie *blockchain*, citons Schneider Electric ou Mondelez, qui a mis en place un système de traçabilité des biscuits « Petits LU », en partenariat avec la *start-up* française Connecting Food. Suez développe pour sa part des projets liés à la technologie *blockchain* dans sa filière déchets.

À côté de ces entreprises recourant à la technologie *blockchain* pour répondre à leurs propres besoins, de grands groupes français se positionnent sur le marché des services inter-entreprises, comme Atos, Thales ou Orange.

M. Philippe Latombe, rapporteur. Ces grands groupes développent-ils leurs solutions *blockchain* en interne ? Sollicitent-ils des intégrateurs ou contactent-ils directement les *start-up* ? Peut-être vont-ils jusqu'à développer des *start-up* à l'intérieur même de leur périmètre ?

Mme Liliane Dedryver. Tout dépend des situations. La société Mondelez a noué un partenariat avec une *start-up* française pour développer un système propre. Nous avons répertorié une multiplicité de cas différents. De toute façon, pour l'instant, les retours d'expérience demeurent assez rares.

M. Philippe Latombe, rapporteur. Pour reprendre la formule de votre collègue de la DGT, à propos de bitcoin : il faut aussi raconter de belles histoires. Le monde de l'entreprise en connaît-il à ce jour, à même de mettre la technologie *blockchain* en lumière ? Comment l'État peut-il y contribuer, si ce n'est en se faisant le relais de telles histoires, en expliquant, à tout le moins, en quoi la technologie *blockchain* a de l'avenir ?

Mme Liliane Dedryver. Les applications industrielles de la technologie *blockchain* sont encore trop récentes pour que je vous cite un cas de réussite spécifique.

Nous œuvrons actuellement avec un groupe de travail, sous-ensemble de la *task force blockchain*, à la rédaction d'un guide de sensibilisation destiné aux entreprises désireuses de développer à l'avenir des cas d'usage de la *blockchain*. Il propose un relevé de ceux qui sont en passe d'aboutir afin d'illustrer les possibilités offertes par la technologie *blockchain*.

Bon nombre d'applications se rapportent à des besoins de traçabilité et de transparence, en vue de rassurer des clients sur la qualité d'un produit. Un acheteur de biscuits Petit LU peut désormais scanner un QR code lui indiquant dans quel champ a poussé le blé entrant dans la composition du produit, ce qui crée de la confiance en rassurant sur ses caractéristiques environnementales. Beaucoup de projets relèvent pour le moment d'un souci de transparence dans le secteur agroalimentaire, aussi bien en ce qui concerne la production de vin bio que l'exportation à l'étranger de produits sensibles, tel le substitut de lait maternel. Le recours à la technologie *blockchain* permet au consommateur de vérifier qu'il n'achète pas un produit de contrefaçon issu du marché gris. Notre guide répond à un besoin actuel de capitaliser sur la sensibilisation naissante des entreprises françaises à la technologie *blockchain*. Il faut leur prouver que son usage ne se limite pas aux cryptoactifs.

M. Philippe Latombe, rapporteur. La crise sanitaire a-t-elle apporté des changements à l'utilisation ou à la promotion de la technologie *blockchain* ?

Mme Liliane Dedryver. Nous nous apprêtons à lancer une consultation publique auprès des acteurs de l'écosystème, des *start-up* aux associations de représentants en passant par les grands groupes. Nous souhaitons dresser un bilan des actions menées dans la stratégie nationale *blockchain* depuis 2019 et déterminer si les besoins des entreprises ont évolué, du fait de la crise sanitaire. Cette consultation devrait aboutir d'ici quelques mois. Nous en partagerons les conclusions lors des réunions semestrielles de la *task force blockchain*.

Revenons sur le financement des *start-up*, l'un des grands axes de la stratégie nationale *blockchain*. Depuis son lancement en 2019, la DGE et Bpifrance ont mis en œuvre trois types d'actions pour aider les *start-up* de l'industrie *blockchain* confrontées à des difficultés de financement.

– d'abord, Bpifrance leur a apporté un soutien direct, *via* les dispositifs *deep tech*, qui ont permis, en 2020, d'injecter un million d'euros à ces *start-up*. Dans le même temps, 100 000 euros ont été engagés *via* les bourses *French Tech Emergence* ;

– ensuite, des fonds partenaires de Bpifrance ont, en parallèle, réalisé des investissements, qui ont tout de même permis au secteur de lever trente millions d'euros en 2020 ;

– enfin, courant 2020, pendant la crise, nous avons consulté rapidement les *start-up* afin de mesurer leurs difficultés à lever des fonds, compte tenu du contexte. Pour y remédier, Bpifrance a accordé des prêts à une vingtaine d'entreprises, d'un montant cumulé de cinq millions et demi d'euros. Un besoin d'accompagnement spécifique existait donc.

Certaines questions de la consultation publique que nous allons lancer doivent déterminer si les entreprises connaissent les financements mis en place, *via* Bpifrance, si elles s'approprient ces outils et s'ils leur suffisent.

En plus de ces soutiens financiers directs de l'État, nous accompagnons le développement de débouchés, *via* les échanges bilatéraux avec les filières et la diffusion du guide de sensibilisation à la *blockchain*, mentionné plus tôt.

Nous nous efforçons enfin de faciliter les levées de fonds au travers d'un guide d'attractivité à l'intention des investisseurs potentiellement intéressés par les entreprises françaises du secteur de la *blockchain*.

M. Philippe Latombe, rapporteur. Faudrait-il aujourd'hui lever certains freins législatifs au développement de l'écosystème ? Je songe à la question de la force probante de la *blockchain*, voire à d'autres sujets sur lesquels devraient se pencher les législateurs.

Mme Liliane Dedryver. À ce stade, nous n'identifions pas de besoin particulier pour accompagner l'essor de l'écosystème de la *blockchain* à usage non financier en France.

Le rapport des chercheurs mentionné auparavant comportait des recommandations afin que les différentes administrations accompagnent la croissance de l'écosystème au jour le jour. La DGE a commencé à s'approprier ces conseils en les mettant en œuvre.

Un premier axe portait sur les obstacles aux rencontres entre les *start-up* et le monde de la recherche. Les solutions mises au point par les chercheurs ne participent pas assez, à ce jour, au développement économique. Nous tentons désormais de créer des ponts entre ces deux mondes. Nous avons ainsi organisé, en fin d'année dernière, une rencontre entre *start-up* et chercheurs, couronnée par un véritable succès. Plusieurs centaines de personnes y ont participé, l'occasion pour elles de nouer des contacts.

Beaucoup de demandes nous parviennent pour faciliter les interactions et la transmission d'informations entre administrations et *start-up*. Une rencontre aura lieu, à l'occasion de la « *Paris blockchain week* ».

Enfin, les deux guides mentionnés auparavant résultent eux aussi de recommandations formulées par les chercheurs dans leur rapport. En somme, la DGE parvient à mener à bien de nombreuses initiatives sans modification du dispositif législatif en place.

D'autres points relevés par les chercheurs auteurs du rapport échappent au périmètre de la DGE. Le ministère de l'enseignement supérieur, de la recherche et de l'innovation

(MESRI) en a pris connaissance. Ils portent sur la formation. Les chercheurs ont établi une cartographie de celles qui existaient en France. Les vingt-deux formations qu'ils ont relevées, interdisciplinaires, et de niveau master, ne leur semblent pas suffisantes pour accompagner les besoins en compétences de l'écosystème. Ils appellent de leurs vœux un développement plus important des formations, notamment dans le domaine de la recherche.

Il conviendra en dernier lieu de s'assurer que des projets de recherche suivent leurs cours dans les différents domaines prometteurs pour l'évolution de la technologie *blockchain* en France.

M. Philippe Latombe, rapporteur. Lors de nos précédentes auditions, il a été question de la notion de force probante de la *blockchain*, adoptée par certains pays européens. La France n'a pas encore légiféré sur le sujet. La plupart de nos voisins européens disposent-ils aujourd'hui du même cadre juridique que la France ? Devrions-nous nous inspirer des spécificités de certains pays ?

Mme Liliane Dedryver. De notre point de vue, le système actuel suffit. Le code civil prévoit d'ores et déjà la possibilité d'apporter la preuve par tout moyen, y compris les informations enregistrées sur un dispositif *blockchain*. Dans la pratique, chaque preuve est évaluée au cas par cas, ce qui nous semble plutôt une bonne chose. La notion, très large, de *blockchain* recouvre des réalités parfois extrêmement différentes. Mieux vaut donc, en matière de preuve, examiner chaque *blockchain* dans le détail. Toutes ne sauraient être considérées comme ayant, de manière générale, une force probante.

Nous ne relevons pas non plus d'obstacle au niveau européen, où prévaut un système de preuve par tout moyen. En raison du principe de neutralité technologique, il apparaît compliqué d'imposer une législation propre aux *blockchains*, au niveau européen. Dès lors que s'impose ce principe, au nom de quoi faudrait-il accorder un statut particulier aux *blockchains* ?

La France a joué un rôle précurseur en matière de stratégie nationale *blockchain*, encore que d'autres pays développent à présent, eux aussi, des stratégies comparables, comme l'Italie, l'année dernière. Il me semble que la stratégie italienne comprend un volet réglementaire traitant des aspects financiers de cette technologie, un autre s'intéressant au développement de l'écosystème et à son financement. L'Italie se révèle d'autant plus active qu'elle préside en 2021 le sommet du groupe des vingt (G20) numérique. Dans sa feuille de route pour 2021, l'Italie a souhaité inscrire les *blockchains*, notamment en lien avec les enjeux de traçabilité que j'évoquais tout à l'heure.

Les institutions européennes ont développé une stratégie *blockchain* de manière à mobiliser des financements européens. La DGE a participé aux discussions et à la constitution de ces financements, inclus dans le projet horizon Europe, d'un montant d'environ 55 millions d'euros. Une partie soutiendra le développement d'une infrastructure *blockchain* commune à l'Union européenne. Cette *European blockchain services infrastructure (EBSI),* développant une infrastructure basée sur des nœuds de réseau présents dans chaque État membre, servira surtout aux acteurs publics. Il reviendra à chaque pays d'en proposer ses propres utilisations. La DGE a par exemple soutenu, en France, la création d'un cas d'usage : l'apostille.

M. Philippe Latombe, rapporteur. Des cas d'usage de la technologie *blockchain* se développent-ils actuellement dans la sphère publique ? Comment les acteurs publics s'approprient-ils cette nouvelle technologie ?

Mme Liliane Dedryver. Je ne suis pas en mesure de vous fournir de données pertinentes à ce sujet.

M. Philippe Latombe, rapporteur. J'aurais simplement souhaité votre sentiment personnel sur la question. La technologie *blockchain* vous semble-t-elle désormais connue ? Vous faut-il encore expliquer à vos interlocuteurs publics en quoi elle consiste ?

Mme Liliane Dedryver. De nombreuses institutions en France me paraissent très fortement sensibilisées aux enjeux de la technologie *blockchain*, comme Bpifrance, l'AMF ou l'ACPR. D'autres, telles l'agence nationale de la sécurité des systèmes d'information (ANSSI), travaillent aussi sur la *blockchain*. Nous avons d'ailleurs échangé afin de clarifier la question des certifications des cas d'usage. En somme, il existe en France un réseau d'administrations, qui comprend et commence à intégrer la *blockchain* au développement des politiques publiques, au jour le jour.

M. Philippe Latombe, rapporteur. Comment voyez-vous l'avenir de la *blockchain* à moyen et long terme ? Deviendra-t-elle incontournable ? Ou fera-t-elle figure de simple technologie parmi tant d'autres ?

Mme Liliane Dedryver. Nous ne la considérons que comme une technologie parmi d'autres. Elle présente toutefois des avantages, déjà évoqués par la DGT, tels que sa rapidité de déploiement, son caractère décentralisé et ouvert, qui permettent de régler des problèmes que d'autres solutions technologiques ne parvenaient pas toujours à résoudre. Elle autorise ainsi la gestion en commun de bases de données par des entreprises d'un même consortium.

Certaines *blockchains* publiques sous preuve de travail devront tout de même dépasser une partie de leurs limites actuelles pour que l'on assiste à un essor de leurs applications. Je songe en premier lieu à leur consommation énergétique.

D'autres enjeux, relevés par les scientifiques, concernent l'appropriation, par les différents systèmes *blockchain*, du Règlement général sur la protection des données (RGPD). Nous en revenons ainsi à des questions de souveraineté numérique, portant, entre autres, sur le lieu de stockage de l'information, et qui s'apparentent à celles que soulève le *cloud*.

L'écosystème, encore assez jeune, nécessite en résumé un accompagnement étroit, sans même parler du besoin de sensibiliser les différents acteurs.

M. Philippe Latombe, rapporteur. Il est beaucoup question de deux protocoles : bitcoin et Ethereum. Certains protocoles européens récemment développés vous semblent-ils prometteurs ? Méritent-ils une mise en lumière particulière ? L'un des enjeux de la souveraineté numérique concerne l'existence de protocoles européens soutenus par de grandes entreprises. Avons-nous un retard à rattraper par rapport aux États-Unis ?

Mme Liliane Dedryver. Je n'ai malheureusement pas de réponse à vous apporter. Nous réfléchissons pour le moment, avec d'autres membres de *la task force blockchain*, au moyen d'encourager le développement d'infrastructures communes au moyen de consortiums. Elles fourniraient l'occasion de passer à une échelle supérieure. Cependant, nous n'en sommes encore qu'au début de nos réflexions.

M. Philippe Latombe, rapporteur. Le fait de savoir qu'un chantier a été lancé constitue déjà en soi une information.

Souhaiteriez-vous aborder d'autres points que nous aurions laissés de côté ?

Mme Liliane Dedryver. Non, il ne me semble pas que nous ayons omis quoi que ce soit.

M. Timothée Huré. L'impression nous est parfois venue d'un décalage, de notre part, vis-à-vis de vos questions, puisque nous les abordons sous un prisme financier, nous souciant moins que vous des enjeux de souveraineté. Nous nous sommes toutefois efforcés de vous communiquer tout ce qui relevait à notre sens de cette problématique.

M. Philippe Latombe, rapporteur. J'ai bien conscience que votre position vous place à la limite du champ, mais l'écosystème nous avait demandé, puisque la France souhaite devenir une importante place financière, quelle attitude l'administration adopterait par rapport à la technologie *blockchain* et aux cryptoactifs.

Audition, ouverte à la presse, de MM. Édouard Geffray, conseiller d'État, directeur général de l'enseignement scolaire, et Jean-Marc Merriaux, inspecteur général de l'Éducation nationale, directeur du numérique pour l'éducation (ministère de l'Éducation nationale)
(4 mai 2021)

Présidence de M. Jean-Luc Warsmann, président.

M. Jean-Luc Warsmann, président. Nous auditionnons M. Édouard Geffray, directeur général de l'enseignement scolaire, accompagné de M. Jean-Marc Merriaux, inspecteur général de l'Éducation nationale et directeur du numérique pour l'éducation.

Notre échange s'inscrit dans nos réflexions sur les enjeux de formation aux compétences numériques. La souveraineté numérique ne saurait être envisagée sans une bonne compréhension de ce que recouvre le monde des nouvelles technologies.

Nous souhaitons échanger avec vous sur la façon dont notre système d'enseignement a pris le virage du numérique pour enseigner de nouveaux savoir-faire, doter les personnels d'outils efficaces de conception récente et, enfin, évaluer les pratiques pédagogiques.

M. Philippe Latombe, rapporteur. Je voudrais évoquer trois sujets à titre liminaire.

Le premier concerne votre approche de la notion de souveraineté numérique. Il s'agit là d'une question rituelle lors de nos auditions, qui procède de la grande diversité des définitions données à cette notion. J'aimerais en connaître votre propre conception, d'une part, et d'autre part, savoir comment l'enseignement des compétences numériques, tel qu'il se pratique, en France, en 2021, intègre cette notion. Je souhaiterais, à cette occasion, que vous nous rappeliez les principaux dispositifs mis en place et que vous reveniez sur la manière dont l'Éducation nationale a eu recours au numérique afin d'assurer une continuité pédagogique au bénéfice des élèves durant la crise sanitaire.

Mon second point portera sur la transformation numérique de l'Éducation nationale. Pourriez-vous nous présenter les principaux projets destinés à l'accompagner ? En quoi le choix des outils utilisés par les personnels du ministère prend-il en compte la problématique de la souveraineté numérique ?

Je me demande également comment l'Éducation nationale entend se positionner par rapport à l'ouverture des données. La crise sanitaire nous a amenés à mesurer l'importance de cette question, notamment dans le domaine de la santé, où des efforts significatifs ont été menés. Je voudrais connaître les intentions du ministère à ce sujet.

Enfin, je souhaiterais échanger sur les causes et les conséquences des difficultés rencontrées lors de la mise en place de l'enseignement à distance, avant d'aborder la question de la sécurité des infrastructures numériques éducatives, dont celles du Centre national d'enseignement à distance (CNED).

Pour terminer mon propos liminaire, j'aimerais prendre un peu de champ afin d'évoquer la souveraineté numérique d'un point de vue européen. Concrètement, comment la France se positionne-t-elle par rapport aux pays voisins en termes d'enseignement des compétences numériques ? Dans quelle direction pourrions-nous progresser, selon vous ? Je voudrais, en somme, analyser, en les comparant, les bonnes pratiques en la matière, en Europe.

M. Édouard Geffray, conseiller d'État, directeur général de l'enseignement scolaire (ministère de l'Éducation nationale). La thématique de la souveraineté numérique revêt une grande importance pour le ministère, qui s'est beaucoup penché sur ce sujet.

Notre audition intervient dans un contexte de forte sollicitation numérique du ministère. En mars 2020, celui-ci a mis en place une continuité pédagogique pratiquement immédiate et globalement réussie. L'outil « ma classe à la maison » existait déjà avant la crise sanitaire. La création d'un tel service avait en effet été ordonnée, suite au cyclone Irma, dans l'hypothèse où des établissements ne pourraient accueillir les élèves. Nous ne pensions évidemment pas, alors, que douze millions d'entre eux devraient y recourir un jour.

Lors du confinement, nous avons mis en place un éventail de services d'une ampleur inédite, dont les Espaces numériques de travail (ENT) et les cours Lumni en ligne et à la télévision. À ma connaissance, aucun autre pays n'a réagi aussi vite ni de manière aussi extensive. Nous avons en outre été parmi les premiers à lancer une alerte sur le mirage du numérique, signalant que les outils numériques, à l'appui des professeurs, ne sauraient en aucun cas les remplacer. La circulaire du 28 février 2018 indiquait ainsi que le professeur assurait la continuité pédagogique au moyen de dispositifs lui servant d'appui.

Il convient de le souligner, car cela rejoint votre première question sur ce que recouvre la notion de souveraineté numérique et ce que nous sommes en droit d'en attendre en matière éducative. Au risque d'enfoncer une porte ouverte, je dirai que j'entends, par souveraineté, la capacité à décider de sa destinée, ce qui suppose à la fois la capacité d'exercer un jugement libre et une volonté non contrainte, que ce soit au niveau d'un pays, d'un peuple ou d'un individu, et celle d'agir en conséquence en construisant cette destinée. Deux aspects se conjuguent ici : le jugement et l'action.

En ce qui concerne le jugement, le principe de la souveraineté, appliqué à la sphère éducative, à l'ère numérique, recouvre l'enjeu de former des citoyens, ce qui passe par la formation des professeurs autant que des élèves. Il faut inculquer à ceux-ci l'esprit critique, la capacité de distanciation et la connaissance des outils numériques, tels que l'Intelligence artificielle ou les algorithmes, pour qu'ils comprennent comment le monde se modélise et comment leur volonté peut s'en trouver influencée. En somme, ils doivent parvenir, si ce n'est à se détacher des paramètres pesant sur leurs choix, au moins à en prendre conscience. Si vous le permettez, je glisserai ici une référence à Auguste Comte : il faut savoir pour prévoir et prévoir pour pouvoir.

Chaque futur citoyen doit se doter d'une culture numérique. L'univers numérique suppose des modalités particulières d'exercice de l'esprit critique. La question des moyens de traduire nos valeurs dans le monde numérique se pose au quotidien. Chacun détient, en tant qu'utilisateur, un pouvoir, certes asymétrique mais toutefois réel, qu'il exercera comme il se doit, pour peu qu'il ait reçu une formation adaptée. Nous en revenons dès lors à la formation au numérique des élèves, qui suppose aussi bien une éducation aux médias d'information, *via* la lutte contre les fausses nouvelles, par exemple, qu'une formation plus technique.

Je distinguerai à présent trois champs de la souveraineté, en ce qu'elle touche à la capacité d'action.

La souveraineté juridique équivaut à la capacité de faire appliquer son droit sur son territoire. Le Règlement général sur la protection des données (RGPD) européen en fournit un exemple abouti. Aujourd'hui, ce RGPD, extrêmement novateur lors de son instauration, protège les données de tout ressortissant de l'Union européenne, y compris lorsqu'elles circulent à l'étranger. J'estime ce point fondamental.

La souveraineté technique repose sur le recours à des outils qui nous appartiennent en propre. J'emploierais plus volontiers à ce propos la notion d'autonomie stratégique. Elle correspond à la capacité d'assurer un service de masse à tous, ainsi qu'à en limiter la vulnérabilité face à des menaces ou des paramètres extérieurs.

Enfin, j'assimile la souveraineté des usages à la capacité d'inculquer à chacun les compétences nécessaires pour agir dans l'univers numérique en maniant avec aisance les outils correspondants.

Je distinguerai deux champs d'application à cette souveraineté des usages. Commençons par nous pencher sur la pratique des métiers au quotidien. Nous avons tout à l'heure souligné le caractère essentiel de la formation des professeurs. Depuis un an, 200 000 d'entre eux se sont formés, *via* Canopé, notre plateforme de formation continue, aux usages du numérique et à l'enseignement à distance. S'appuyer sur le numérique ne se limite pas à faire la classe en mode virtuel, mais implique d'utiliser l'ensemble des outils numériques pour faciliter l'apprentissage des élèves.

Le programme Pix certifie le niveau des élèves en fin de troisième et de terminale, de manière à ce qu'ils puissent évoluer, au quotidien, dans l'univers numérique en y exerçant leurs droits et devoirs et, partant, une forme de souveraineté. Veiller à la protection de ses propres données rend capable d'exercer une influence déterminante sur le cours numérique de son existence.

À cette dimension quotidienne de la souveraineté des usages s'ajoute un enseignement de spécialité visant à former des élèves et des professeurs experts en numérique. La spécialité Numérique et sciences informatiques (NSI), créée en 2018 à l'occasion du nouveau baccalauréat, est aujourd'hui assez prisée, puisque 9,5 % des élèves la suivent en première. Elle a donné lieu à la création d'un Certificat d'aptitude au professorat de l'enseignement du second degré (CAPES) NSI, que suivra, en 2022, une agrégation NSI. Les professeurs déjà employés par l'Éducation nationale qui réussiront ce concours de haut niveau recevront de surcroît un diplôme interuniversitaire, élaboré avec 22 institutions partenaires d'enseignement supérieur en France. J'estime très intéressant de pouvoir former des spécialistes du numérique représentant près de 10 % d'une génération de lycéens généraux, dans la mesure où nous construisons ainsi une capacité d'action, de création et de développement autonomes pour l'avenir.

M. Jean-Marc Merriaux, inspecteur général de l'Éducation nationale, directeur du numérique pour l'éducation. La question de la souveraineté ne saurait être envisagée hors du contexte historique propre à notre pays. Rappelons le rôle de premier plan joué par la France dans le déploiement du RGPD, mais aussi la loi Informatique et libertés de 1978, sur laquelle repose en grande part ce RGPD. La logique suivie par la France l'amène à axer sa souveraineté sur l'enjeu de la protection des données et de leur usage possible en regard des libertés individuelles. Voilà pourquoi mon intervention s'intéressera beaucoup à l'approche des données et à la capacité à les protéger.

Le ministère de l'Éducation nationale est aujourd'hui amené à collecter les données de 12 millions d'élèves et d'1,2 million d'agents. Le RGPD nous fournit heureusement les outils nécessaires pour répondre aux enjeux de la protection de ces données. Le ministre de l'Éducation, lors de l'université d'été du numérique pour l'éducation en 2018, a insisté, dans son discours, sur l'enjeu de la protection et de la valorisation des données. Je reviendrai sur notre capacité à les ouvrir et les mettre à disposition. Notre action s'inscrit en tout cas dans cette optique, selon laquelle le ministère élabore, depuis trois ans, sa stratégie numérique.

M. Édouard Geffray a indiqué les outils mobilisés pour la continuité pédagogique. N'oublions pas les ENT, qui constituent une spécificité. Des difficultés ont surgi la semaine du 6 avril, liées à l'usage désormais quotidien de ces outils par l'ensemble de la communauté éducative. La quantité de connexions en ce début de mois nous a surpris. Nous escomptions une augmentation de 20 % par rapport à l'année dernière, or c'est à une véritable explosion à laquelle nous avons assisté, la première semaine d'avril. La souveraineté s'inscrit aussi dans la capacité à construire des outils. La mise en place des ENT découle d'une politique datant de 2004. Leur usage s'est progressivement imposé. Le ministère en partage la responsabilité avec les collectivités territoriales. Ont pris part à leur élaboration des acteurs souverains des nouvelles technologies, sans lesquels nous n'aurions pu intégrer ce type d'outils dans le paysage éducatif français. En somme, la souveraineté se construit à travers une complémentarité d'outils. Je tenais à le souligner.

Concernant les enjeux de la souveraineté en termes d'enseignements, je rappellerai d'abord que Pix, la plateforme de certification européenne à laquelle contribue le ministère, repose sur un référentiel de compétences numériques européen. L'UNESCO l'a sélectionnée pour répondre à des enjeux de certification des compétences au-delà de nos frontières. La construction de notre souveraineté passe par un outil comme celui-là également.

Je rappellerai en outre que l'enseignement en Sciences numériques et technologie (SNT), en seconde générale, procure une vision exhaustive des enjeux du numérique dans la vie quotidienne. Une certification en fin de troisième évalue les compétences numériques des élèves. Des cours de SNT leur sont ensuite proposés, puis de NSI, avant un nouveau test en fin de terminale. Leurs compétences numériques s'inscrivent ainsi dans la continuité de leur parcours, universitaire ou professionnel. L'action du ministère en matière de numérique trouve sa place dans une dynamique d'ensemble. Les classes de SNT abordent bien sûr les enjeux liés aux données et à la cybersécurité.

Pour répondre aux enjeux de protection et d'anonymisation des données, le ministère travaille étroitement avec l'ensemble de l'écosystème numérique éducatif. Nous terminons en ce moment de rédiger, en accompagnement des acteurs de la filière, un code de conduite, outil du RGPD permettant à un secteur d'activité de définir des règles spécifiques. Nous espérons qu'il entrera en vigueur à la rentrée de septembre. La Commission nationale de l'informatique et des libertés (CNIL) doit au préalable lui donner son aval, puis le proposer à ses homologues européens, puisqu'il pourrait intéresser aussi les secteurs éducatifs d'autres pays européens. À la différence des données de santé, celles de l'éducation ne sont pas considérées comme sensibles.

Depuis plusieurs années, le ministère a mis en place un autre outil : le GAR (Gestionnaire d'accès aux ressources), qui constitue un véritable tunnel d'usage autour de la ressource au sein des ENT. Concrètement, les élèves peuvent accéder, *via* ces ENT, à un centre géant comportant plus de 12 000 ressources, dès lors que leur établissement s'y est abonné. Nous garantissons, à travers ce tunnel, l'anonymisation des données de manière à renforcer la confiance, dans une visée de souveraineté.

Nous déployons par ailleurs un autre dispositif d'authentification propre à l'Éducation nationale, inspiré de FranceConnect, toujours par souci de garantir la sécurité des usagers. Baptisé EduConnect, il permettra à chaque parent de donner à ses enfants accès à des ressources, dans le respect, entre autres, du code de conduite et des principes du RGPD. Là encore, ce dispositif s'intègre pleinement dans notre stratégie de souveraineté.

Le ministère avait par ailleurs préconisé, au-delà des lois et réglementations existantes, la mise en place d'un comité d'éthique de la donnée d'éducation. Ce comité a remis un rapport

sur la continuité pédagogique lors du premier confinement, s'attachant aux enjeux de souveraineté, dont l'éthique constitue un pilier dans le domaine du numérique éducatif.

J'insisterai sur une dernière dimension de la souveraineté. Un acteur majeur avait développé un outil de vie scolaire pour le second degré : INDEX-ÉDUCATION. Un rapport de l'inspection générale en 2018 sur les données numériques à caractère personnel au sein de l'Éducation nationale a identifié un risque que des acteurs étrangers s'emparent de ces données à travers cet outil. Docaposte et La Poste ont récemment racheté l'acteur concerné afin de garantir la souveraineté sur les données qu'il traitait.

À l'aube de révolutions numériques majeures, en lien avec l'Intelligence artificielle, nous avons de surcroît développé des partenariats de l'innovation avec des acteurs industriels et des laboratoires de recherche, de manière à garantir notre capacité à peser sur les enjeux de l'Intelligence artificielle liés à l'éducation.

Enfin, GAIA-X, en tant que *cloud* souverain européen, devrait donner lieu à une réflexion sur la mise à disposition de l'ensemble des données. Preuve de notre attitude proactive, nous sommes le seul ministère européen de l'Éducation à siéger à son conseil d'administration en vue de développer l'ensemble des cas d'usage autour de la donnée d'éducation.

J'aurai sans doute l'occasion de revenir sur la plateforme Education Data-hub. Elle doit mettre les données d'éducation à disposition de l'ensemble des acteurs, tout en fournissant l'occasion d'une réflexion sur cette même mise à disposition.

M. Philippe Latombe, rapporteur. Cette audition compte beaucoup pour nous. Le sujet de l'éducation a été soulevé lors de toutes les précédentes auditions en raison de son importance majeure. Nous ne saurions concevoir de souveraineté, de technologie, ni même d'entreprises numériques sans étudiants appelés à devenir des citoyens, des ingénieurs ou des dirigeants de sociétés. L'éducation apparaît donc comme un besoin fondamental.

Je propose d'évoquer d'abord les trois catégories de population auxquelles vous avez affaire, au ministère : les élèves ou étudiants, les professeurs et les parents. Estimez-vous aujourd'hui que les élèves, à la fin de leur scolarité, ont acquis une maîtrise suffisante du numérique ? Je ne songe pas seulement à la capacité d'utiliser des outils numériques mais à la connaissance de leur fonctionnement, qui passe notamment par la compréhension de la notion d'algorithme. La plupart des parents et des professionnels du secteur estiment que ce n'est pas le cas. Je manque sans doute de diplomatie en vous relayant leur impression. Ceux qui commencent à recruter des « *digital natives* » leur reprochent de ne pas toujours être en phase avec la réalité du monde numérique actuel. Reçoivent-ils une formation assez poussée ? Les jeunes ne quittent-ils pas le système scolaire sans avoir acquis toutes les connaissances que le ministère souhaitait leur transmettre ?

M. Édouard Geffray. Je distinguerai le processus dans sa continuité et ce qu'en montre un arrêt sur image. Les dispositifs, à mesure que nous les mettons en place, toucheront une cohorte plus ou moins tardivement. À ce jour, toutefois, la construction de la compétence numérique m'apparaît assez complète.

Un élève arrivant en primaire bénéficie, dès le cycle 2 (CP, CE1, CE2) et, *a fortiori*, en cycle 3 (CM1, CM2, sixième) d'une initiation au code dans l'enseignement des mathématiques.

Au collège, en cycle 4 (correspondant aux classes de cinquième, quatrième et troisième), les notions d'algorithmique sont traitées lors des cours aussi bien de mathématiques que de technologie. La programmation est également enseignée, *via* divers logiciels, dont le plus connu reste Scratch.

En parallèle, la pratique d'outils numérique, certes non obligatoire, devient de plus en plus fréquente. Il n'est plus rare que des professeurs donnent des devoirs sur des outils en ligne, tels calcul@TICE développé par l'académie de Lille. Des centaines de milliers d'élèves l'ont utilisé lors du premier confinement.

La compréhension globale du numérique, encore inexistante voici quelques années, s'étend en tout état de cause. Ceux qui ont des enfants séparés par un écart d'âge conséquent s'en rendront compte au travers de l'évolution des programmes.

Tous les élèves de seconde suivent désormais, suite à la réforme du lycée, un enseignement commun en sciences numériques et technologie (SNT) d'une heure et demie par semaine. La spécialité NSI est ensuite proposée à raison de quatre heures hebdomadaires en première et six en terminale. Le programme de cette matière fournit une approche assez complète du numérique, allant de la technologie (le code) à l'éthique (le traitement des données personnelles) en passant par la compréhension globale de cet univers. La première cohorte à avoir suivi cette spécialité obtiendra son baccalauréat cette année.

En somme, considérer la situation avec plus ou moins de recul livrera l'impression que les élèves ont acquis plus ou moins d'expertise. Quoi qu'il en soit, une comparaison internationale poussée a révélé que la France se situait largement en tête des autres pays pour ce qui est de la profondeur des apprentissages numériques de la spécialité NSI.

La plateforme Pix, élaborée à partir d'un référentiel européen, participe de ce dispositif d'enseignement du numérique. Elle permet de sanctionner un niveau acquis à l'issue de préparations à des tests, à la fois en fin de collège et de lycée. Les évaluations, *via* Pix, auraient eu lieu pour la première fois cette année, si la crise sanitaire n'avait pas contraint à suspendre leur caractère obligatoire, au moins en terminale.

M. Jean-Marc Merriaux. Dès la fin de l'école primaire, en CM2, a lieu une première évaluation, renouvelée en sixième, des compétences numériques de l'élève, notamment dans leur dimension algorithmique. Ces compétences sont en résumé testées tout au long de la scolarité.

L'éducation au numérique touche à de nombreux enjeux abordés dans l'enseignement moral et civique, qui vise à développer l'esprit critique de l'élève et sa capacité à identifier des sources d'information. L'éducation aux médias et à l'information comporte également une dimension numérique.

L'acquisition d'une culture numérique repose autant sur une approche culturelle que sur l'appropriation d'outils, la capacité à coder, ou la compréhension de la nature et du fonctionnement d'un algorithme. L'ensemble des enseignements abordent dorénavant ces deux facettes de la question, de sorte qu'une telle approche transversale englobe tous les enjeux actuels du numérique.

M. Philippe Latombe, rapporteur. Comment expliquez-vous que la pratique du numérique d'une partie des collégiens, malgré les dispositifs mis en place dès le primaire, confine au harcèlement ou relève d'un mésusage des réseaux sociaux ? Certains ne possèdent toujours pas les réflexes qu'ils devraient pourtant avoir acquis, aussi bien en position de

victime que d'agresseur. Quel regard le ministère porte-t-il sur la situation ? Comment compte-t-il fournir, dès le primaire, bien au-delà de la simple sensibilisation aux fausses nouvelles, une sorte de mode d'emploi de ces comportements déviants ? Surtout, comment s'assurer que le message sera bien assimilé ? Des principes éthiques devront en effet guider nos concitoyens tout au long de leur vie d'adulte. Les aléas de la vie politique le démontrent assez. Autrement dit, quelles mesures prenez-vous pour préparer les élèves à l'avenir ?

M. Édouard Geffray. La question revêt en effet une importance majeure.

J'aborderai d'abord le cadre général de l'enseignement, puis son application pratique au harcèlement. Le ministre a défini comme aptitudes à acquérir à l'issue de l'école primaire : la lecture, l'écriture, la capacité à compter et le respect d'autrui. Ce respect d'autrui présente de multiples dimensions. Dans le domaine de la santé, il passe par l'éducation à la sexualité. L'élève de primaire apprend à respecter le corps d'autrui et à se faire lui-même respecter dans son corps, ce qui implique notamment la prévention des violences sexuelles ou familiales, mais aussi l'apprentissage du rapport à l'autre, de la vie de classe et de la résolution des conflits. Ces valeurs se traduisent, elles aussi, directement dans l'univers numérique.

Le lancement volontariste du programme « non au harcèlement » remonte à l'année scolaire 2018/2019. Assez exhaustif, puisqu'il inclut des formations, il va se généraliser dès la rentrée à l'ensemble des académies, et donc des établissements. Rappelons que les académies disposent toutes de référents « harcèlement ». Des ambassadeurs du programme, accompagné par des campagnes de sensibilisation, seront choisis parmi les élèves de chaque établissement.

À l'origine, le prix « non au harcèlement » récompensait les réalisations sous forme d'affiche ou de vidéo de collégiens ou de lycéens soucieux de sensibiliser leurs condisciples à ce problème. Depuis deux ans maintenant, des élèves de primaire peuvent concourir dès le CP. Certaines attitudes se mettent en effet très tôt en place. La difficulté liée aux violences surgit dans ce cas également : ces comportements s'expliquent aussi par des sollicitations échappant en partie à l'institution scolaire. Le ministre a rendu un formidable service aux jeunes en interdisant le téléphone portable au collège, leur offrant ainsi un espace où ils échappent enfin, pour un temps, aux sollicitations numériques. La prévention du mauvais usage du numérique dépasse le cadre scolaire. Certains environnements incitent les jeunes à prendre des risques en diffusant par exemple par SMS leurs photos intimes qui, deux ou trois mois plus tard, pourraient bien échouer entre de mauvaises mains.

Une action globale doit être menée. L'Éducation nationale y travaille. Tout ce qui peut participer à la prise de conscience des dangers du numérique mérite qu'on l'encourage. Le ministère œuvre avec les parents mais aussi la CNIL et le collectif « éducation au numérique ». La CNIL doit assumer un rôle particulier pour diffuser le message selon lequel des données personnelles ne se partagent pas, ou du moins pas n'importe comment. Il faut qu'au-delà du ministère, l'écosystème entier prenne part à l'éducation au numérique et inculque des notions de prudence de base.

M. Jean-Marc Merriaux. Soulignons l'enjeu du *continuum* pédagogique entre temps scolaire et hors scolaire. Nous devons travailler avec l'ensemble de l'écosystème, y compris la CNIL et les collectifs associés. Le ministère intègre dans ses politiques éducatives l'éducation au numérique, au-delà de sa dimension purement scolaire. Nous construisons une approche globale afin d'accompagner les parents aussi. Nous avons développé, à la suite des premiers confinements, des projets baptisés « territoires numériques éducatifs ». Deux expérimentations ont eu lieu, dans l'Aisne et le Val-d'Oise, intégrant pleinement la formation des familles, de manière que les parents puissent à leur tour accompagner leurs enfants.

M. Philippe Latombe, rapporteur. Venons-en justement aux parents, au rôle essentiel. Comment percevez-vous leur appréciation des enjeux numériques et leur capacité d'encadrer leurs enfants ? Les parents actuels appartiennent aux cohortes n'ayant bénéficié d'aucun apprentissage scolaire du numérique, qu'ils ont apprivoisé eux-mêmes, au fur et à mesure.

La fracture numérique se manifeste-t-elle aussi dans l'accompagnement des enfants ou dans le suivi de leur scolarité ? Tous les parents peuvent-ils accéder aux outils mis à leur disposition par le ministère, comme le logiciel PRONOTE, pour mieux suivre les progrès et l'attitude en classe de leur enfant ?

Sur quelles problématiques particulières liées au numérique les parents incitent-ils l'Éducation nationale à se pencher ? Vous adressent-ils des prescriptions ? Vous signalent-ils des lacunes dans la culture numérique de leurs enfants ? Préconisent-ils de renforcer certains enseignements ? Sous quel angle abordent-ils le numérique et comment ?

J'ai conscience de vous poser beaucoup de questions, mais j'envisage difficilement de parler de l'acculturation au numérique des enfants sans évoquer celle de leurs parents.

M. Édouard Geffray. Nous allons nous efforcer de vous apporter une réponse la plus complète possible.

Un cinquième de la société française, en comptant à la fois les élèves et le personnel de l'Éducation nationale, franchit quotidiennement les portes des établissements dépendant du ministère. Si nous leur ajoutons les parents d'élèves, nous nous retrouvons face à un très large éventail de la population, où coexistent, comme chez le reste de nos concitoyens, des sensibilités diverses et où l'on note de grandes disparités en termes d'équipement. Le champ du numérique ne saurait s'exonérer de cette diversité.

Je distinguerai les actions déjà mises en œuvre par le ministère, à l'intention des parents, de celles qui restent à mener.

Nous nous efforçons de mettre à la disposition des parents des ressources pour qu'ils s'approprient certains outils ou usages du numérique, ou encore certains enjeux relatifs à l'éducation de leurs enfants, tels que la protection des données et informations sensibles. Dans une logique d'accompagnement de la parentalité, le site web la « Mallette des parents » recense des dispositifs, de manière à ce que les parents puissent engager des discussions informées avec leurs enfants adolescents. À cet âge compliqué se crée en effet une distance nécessaire vis-à-vis des parents. Il convient d'éviter sa démultiplication par l'enjeu des écrans.

Nous travaillons avec les parents d'enfants, même en bas âge, sur le rapport à l'écran. Un dispositif baptisé « la famille Tout-Écran », développé avec le Centre pour l'éducation aux médias et à l'information (CLEMI), vise à promouvoir, de manière très pédagogique, une approche pondérée de l'usage du numérique. Il décline un ensemble d'outils conviviaux, faciles d'appropriation, permettant d'assimiler rapidement des règles et de prendre conscience de points de vigilance dans l'éducation des enfants.

Un autre enjeu, technique celui-là, a trait à la capacité pour les parents de se former eux-mêmes aux usages du numérique afin d'en améliorer leur pratique. Le projet « Territoires numériques éducatifs » se déploie déjà dans deux départements, l'Aisne et le Val-d'Oise. D'autres en bénéficieront prochainement.

Disposer de tablettes ou d'ordinateurs dans les salles de classe ne suffit pas. L'équipement doit s'articuler avec, aussi bien les ressources numériques, en termes essentiellement de logiciels, qu'avec la formation, pour éviter que les tablettes ne rendent pas tous les services qu'on est en droit d'en attendre. Les deux volets ne relevant pas directement de l'équipement priment en réalité, car l'acculturation collective au numérique dépend d'eux. Le ministère s'occupe de former les parents qui le souhaitent aux usages et aux pratiques du numérique avec des associations partenaires. La pédagogie des outils ne saurait en effet avancer indépendamment de celle des usages.

Ces projets de fonds, structurels, s'inscrivent enfin dans une dimension conjoncturelle.

Celle-ci a trait à la possibilité des parents de suivre la scolarité de leurs enfants, *via* les outils numériques. Elle renvoie également aux questions soulevées par la continuité pédagogique. Comment s'assurer que les familles, en dépit de leur situation parfois difficile, maintiennent un lien avec l'école, *via* les outils numériques ? Nous en revenons aux enjeux de la fracture numérique. Tout le territoire français n'est pas encore couvert par Internet. Certaines familles résidant en zone blanche ne peuvent pas s'y connecter depuis leur domicile. Certains établissements scolaires recourent certes à d'autres modes d'échange plus classiques avec les parents. Une telle situation n'en préoccupe pas moins le ministère, qui se heurte là à une contrainte géographique et non purement matérielle.

Se pose aussi la question de l'équipement des familles. Le suivi de celles-ci s'est renforcé durant la période que nous venons de traverser. Plusieurs dizaines de milliers de tablettes ont été distribuées. Saluons à ce propos l'engagement des collectivités locales. Je préciserai, à titre d'illustration de l'agilité du ministère, que celui-ci s'est doté d'une équipe nationale numérique, en mesure de mettre à disposition, dans un délai de 24 à 48 heures, 10 000 ordinateurs et plusieurs centaines de kits de connexion 4G. Ce dispositif s'est activé à l'occasion des coulées de boue dans les Alpes-Maritimes, ayant contraint certains collèges et lycées à fermer durant plusieurs semaines en décembre. 400 ordinateurs assortis d'un kit de connexion ont été acheminés, en moins de deux jours, aux élèves dans le besoin, pour qu'ils continuent à suivre leurs cours à distance. Les aléas, climatiques ou autres, augmentent le risque de perdre un contact, avec les élèves ou leurs familles, difficile à renouer ensuite.

M. Philippe Latombe, rapporteur. Au-delà des problèmes d'équipement, qu'est-ce que les trois confinements et les deux grands épisodes d'enseignement à distance ont révélé de la relation au numérique des parents ? Quelle leçon convient-il d'en tirer ? Le maintien d'une relation à distance entre l'Éducation nationale et les parents s'annonce-t-il impossible ou du moins non souhaitable ? Avez-vous noté une différence entre milieux urbains et ruraux ?

M. Jean-Marc Merriaux. La question de la relation aux parents soulève évidemment le problème de la fracture numérique. Dès la rentrée de septembre, nous avons cherché à mieux identifier les familles dans l'incapacité de suivre la scolarité de leurs enfants *via* des outils numériques, afin que les établissements mettent en place un accompagnement spécifique à leur bénéfice.

Se pose ensuite la question de la place de la classe virtuelle dans la continuité pédagogique. Les parents n'imaginent pas l'enseignement à distance hors de ces cours virtuels. Un *hiatus* apparaît toutefois, car il n'est pas envisageable de donner des leçons à distance tout le temps que dure en principe une journée d'école. Les parents éprouvent malgré tout le besoin de se raccrocher à la présence de l'enseignant et à sa capacité d'accompagner chaque élève.

Nous avons travaillé sur le renforcement du lien entre enseignants et élèves, *via* les classes virtuelles mais aussi en mobilisant tous les outils de communication disponibles, et

même des outils d'évaluation des compétences à distance. Des formations ont favorisé l'instauration d'un lien privilégié avec chaque élève, pour que les enseignants identifient mieux ceux qui risquaient, à un moment ou un autre, de décrocher. La continuité pédagogique implique la possibilité pour les enseignants de contacter les parents. La classe virtuelle ne saurait en constituer l'alpha et l'oméga, d'autant que tous les élèves n'y assistent pas.

M. Philippe Latombe, rapporteur. Passons au troisième groupe dont s'occupe le ministère : les enseignants. Là encore, je m'en veux de mon manque de tact, mais de nombreuses personnes nous ont signalé l'éloignement du numérique de nombreux enseignants, encore que la situation s'améliore. Les remarques ponctuelles qui nous sont parvenues ne correspondent sans doute pas à votre vision globale, que j'aurais donc besoin de connaître. Êtes-vous en mesure d'évaluer les enseignants sur leur connaissance du numérique, leur compréhension de la notion d'algorithme mais aussi leur utilisation des outils technologiques les plus courants, et ce, de manière à ce qu'ils y forment au mieux les enfants ?

Existe-t-il des formations professionnelles continues spécialisées dans ce domaine pour les enseignants, y compris ceux de matières *a priori* éloignées du numérique comme le dessin ou le latin ?

Enfin, quelles leçons tirez-vous de la pandémie et de l'enseignement à distance (EAD) ? Des questions que vous croyiez réglées se sont-elles imposées à votre attention ? À l'inverse, certaines difficultés que vous pensiez devoir affronter n'auraient-elles en fin de compte pas surgi ?

M. Édouard Geffray. Vos questions nous sont précieuses, car elles entrent en résonance avec celles que, nous-mêmes, nous nous posons.

Je vous livrerai une réaction spontanée fondée sur une impression d'ensemble. Nous avons relevé deux points intéressants.

D'abord, l'an dernier, la continuité pédagogique s'est immédiatement mise en place *via* l'enseignement à distance, alors même que, jamais encore, la totalité des écoles de France n'avait dû fermer. Mes homologues d'autres pays m'ont indiqué que deux à trois semaines de congés avaient été accordées aux professeurs et aux élèves avant d'envisager des mesures possibles. Il en a résulté un décrochage élevé chez certains de nos voisins européens. En France, de mémoire, l'annonce du confinement a eu lieu un vendredi et, le lundi matin suivant, les élèves ont continué l'école à domicile, malgré les quelques difficultés techniques qui ont surgi.

Ensuite, nous avons observé un mécanisme de conversion au numérique. Il s'est d'ailleurs traduit par les chiffres relevés la semaine du 6 avril. Le taux d'usage des outils éducatifs numériques a alors doublé par rapport au pic du mois de mai 2020. Chaque jour, au début d'avril 2021, 2 à 3 millions de visiteurs uniques se sont connectés à la plateforme du CNED, qui n'est pourtant pas le seul outil de classe virtuelle disponible. 200 000 professeurs, soit un sur quatre, ont par ailleurs, d'eux-mêmes, cherché à se former au numérique sur Canopé. Cette proportion témoigne d'une conversion massive au numérique, que nous étions certes en droit d'espérer, mais sur laquelle nous ne tablions pas pour autant, compte tenu de la diversité existant au sein du corps professoral. Des différences subsistent en effet entre générations, car si l'on trouve des professeurs férus de nouvelles technologies de tous âges, les plus jeunes s'avèrent dans l'ensemble plus à l'aise avec le numérique que leurs aînés. Notons que beaucoup se forment d'ailleurs auprès de leurs collègues.

Se pose dès lors la question de la consolidation des formations au numérique. Comment s'assurer que les professeurs acquièrent une culture numérique aboutie, adaptée à leur usage des nouvelles technologies et à ce qu'il leur revient de transmettre à leurs élèves ? L'Éducation nationale n'a pas besoin d'un million d'informaticiens mais d'enseignants forts d'une culture générale du numérique.

Un premier axe de travail a porté sur la formation initiale des professeurs, réorganisée depuis septembre 2020. Suite à la loi pour une école de la confiance et aux travaux parlementaires sur le numérique à l'école, le numérique, sujet désormais incontournable, figure dans le référentiel de formation des professeurs. Je m'occupe en ce moment des procédures d'accréditation des Instituts nationaux supérieurs du professorat et de l'éducation (INSPE). Tous dispensent des formations au numérique de qualité, des plus intéressantes à mon sens, adossées à un référentiel commun garantissant un certain niveau de compétences.

Concernant la formation continue, des dispositifs existent, pour l'heure essentiellement en ligne, du fait de la crise sanitaire, mais, dès que les circonstances le permettront, ils se dérouleront également en présentiel. Signalons que le numérique figure parmi les cinq priorités, aux côtés de l'école inclusive et de la promotion des valeurs de la République, du schéma directeur de la formation continue des personnels de l'Éducation nationale.

M. Jean-Marc Merriaux. Lors de la transformation numérique de tout secteur d'activité, prévaut la règle des trois tiers : pour un premier tiers, les acteurs s'impliquent et s'efforcent de saisir les enjeux, pour un autre tiers, ils peinent à se situer et s'interrogent, tandis qu'un dernier tiers se montre particulièrement réfractaire. Au sein de l'Éducation nationale, 25 % à 30 % d'enseignants, déjà très investis dans le numérique, possédaient d'importantes compétences en la matière, 50 % hésitaient à recourir aux nouvelles technologies dans la pratique de leur métier et 20 % à 25 % s'y disaient hostiles.

Dans la dynamique des états généraux du numérique pour l'éducation, le ministère a sollicité plusieurs laboratoires de recherche pour l'aider à analyser les changements apportés par la crise sanitaire. Une étude du laboratoire malouin de recherche, attaché à l'université de Rennes et spécialisé dans le numérique et l'éducation, a comparé des données recueillies avant et après le premier confinement. Au lendemain de celui-ci, plus de 50 % des enseignants se déclaraient prêts à utiliser le numérique dans leur classe. Il relève de notre mission d'accompagner ces professeurs qui y voient un levier dans leur pratique pédagogique.

De fait, le confinement a obligé à se saisir à bras-le-corps de la question du numérique. Il appartient au ministère de mettre en place tous les outils nécessaires à sa valorisation. Nous travaillons à la formation et à la certification des compétences numériques, outre des élèves, des enseignants. Nous avons ainsi développé, sur la plateforme Pix, des modules spécifiques proposant aux professeurs des tests autonomes de positionnement, dans l'idée d'encourager, tout en la suivant, l'évolution de leurs compétences numériques tout au long de leur carrière. Nous comptons aussi utiliser Pix pour certifier les compétences numériques des enseignants à l'issue de leur formation initiale. La plateforme M@gistère de formation à distance ambitionne enfin de former 250 000 enseignants chaque année, à la fois au numérique et par le numérique.

Nous avons déjà évoqué l'approche développée par Canopé et sa plateforme CanoTech durant le confinement. Le repositionnement de l'opérateur en matière de formation continue renforce l'accompagnement de l'enseignant à la pratique du numérique tout au long de sa carrière.

M. Philippe Latombe, rapporteur. Ma dernière question à propos des enseignants nous donnera l'occasion d'aborder plus directement l'institution que vous représentez. Les

établissements d'enseignement disposent-ils d'équipements numériques suffisants ou du moins assez récents pour permettre une bonne appropriation du numérique ? Qu'en est-il des enseignants eux-mêmes, à leur domicile ? Quelles leçons avez-vous tirées du confinement ? Je ne m'interroge pas seulement sur la disponibilité des ordinateurs mais aussi des tablettes ou des tableaux numériques. Les élèves doivent se familiariser avec les futures évolutions du numérique. Les enseignants vous semblent-ils capables de les anticiper ?

M. Jean-Marc Merriaux. La question de l'équipement numérique des collèges et lycées se pose avec beaucoup moins d'acuité depuis ces dernières années. La plupart des établissements disposent du matériel nécessaire, malgré des disparités entre territoires. Le projet « territoires numériques éducatifs » ambitionne d'ailleurs de cibler les établissements désavantagés afin de renforcer leur dotation, selon les trois axes évoqués tout à l'heure. Aux enjeux d'équipement proprement dit s'ajoutent en effet ceux de la formation et de l'accès aux ressources.

À la faveur du confinement, le primaire est apparu comme le parent pauvre de l'éducation en matière de numérique. Je songe ici à la disponibilité de tableaux blancs interactifs mais aussi à ce que tout le numérique peut apporter en termes de travail collaboratif ou d'évolution de ce que nous appelons la forme scolaire au sein des écoles. Les enjeux liés à l'enseignement du premier degré s'avèrent pourtant cruciaux, car structurants.

Dans le plan de relance, le ministère a lancé un appel à projets doté de 105 millions d'euros, accordant aux communes des subventions pour renforcer leur socle numérique de base, conformément à la recommandation émise par la Cour des comptes dans son rapport de 2019. Les collectivités territoriales se sont associées, ensemble, au ministère pour mener à bien ce travail. Lors des états généraux du numérique pour l'éducation, le ministère s'est appuyé sur l'idée de ce socle numérique de base, à établir en partenariat avec les communes ou regroupements de communes gérant les établissements de primaire, avant de lancer l'appel à projets du plan de relance. La mobilisation des communes a été garante du succès de cette démarche, par laquelle le ministère a démontré sa capacité d'améliorer l'équipement des établissements scolaires.

Notre stratégie s'est en réalité surtout concentrée, depuis trois ou quatre ans, sur l'enseignement du premier degré et les enjeux de l'équipement des écoles primaires. Nous avons réattribué, au bénéfice des territoires ruraux, les crédits subsistant du Deuxième programme d'investissements d'avenir (PIA2). Nous nous penchons maintenant sur le socle numérique de base du second degré en cherchant à identifier les établissements et collectivités territoriales qui accusent un retard dans leur équipement, en vue, bien sûr, d'y remédier. Le projet de « territoires numériques éducatifs » s'inscrit dans cette stratégie.

M. Philippe Latombe, rapporteur. Les professeurs de technologie, de mathématiques ou encore de sciences physiques tracent-ils, devant les lycéens des filières spécialisées dans le numérique, des perspectives sur l'avenir des nouvelles technologies ? Sont-ils capables d'anticiper leurs évolutions futures ? Parviennent-ils à répondre aux questions qui agitent notre mission, comme, à titre d'exemple, celles relatives aux usages d'une constellation de satellites en basse altitude ? Comment les enseignants intègrent-ils les réflexions qu'elles suscitent dans l'orientation de leurs élèves après le baccalauréat ? La continuité est-elle assurée entre enseignement secondaire et supérieur ?

M. Édouard Geffray. Vous nous interrogez en somme sur la dimension prospective de l'enseignement.

D'abord, des partenariats noués avec des entreprises permettent aux jeunes de se projeter dans un univers professionnel au fait des dernières évolutions du numérique. La filière numérique en général, et cybersécurité en particulier, connaît, parmi les formations professionnelles actuelles, une forte croissance. De nombreux jeunes réussissent brillamment leur baccalauréat professionnel numérique pour intégrer ensuite des formations de type Brevet de technicien supérieur (BTS) ou autre. Un projet comme celui des écoles P-tech, dont j'ai visité un exemple en région parisienne, crée un pont entre les entreprises du secteur industriel numérique et les lycées professionnels. Les élèves effectuent des stages dans les sociétés partenaires, sous la tutelle d'un mentor. Ils y découvrent les évolutions les plus récentes du numérique en l'abordant sous son versant « recherche et développement », entrant ainsi de plain-pied dans leur futur milieu professionnel.

À cette première dimension s'ajoute celle de l'actualisation des connaissances et de la formation de pointe. La formation continue s'avère d'autant plus indispensable dans des disciplines comme le numérique, à l'évolution rapide et incessante. Encore faut-il qu'elle enseigne l'usage des outils les plus récents pour garantir l'insertion sur le marché du travail.

Enfin, n'oublions pas les enseignants. Voici un an et demi, a été créé un dispositif de formation des professeurs déjà en poste, désireux d'enseigner la spécialité NSI, apparue dans les programmes en 2019, comme annoncé l'année précédente. Pour la première fois depuis 1980, me semble-t-il, un nouveau CAPES a été instauré dans une discipline autre que les langues : le NSI. Face à l'impossibilité manifeste de recruter 2 000 enseignants à l'issue d'une seule session de concours, nous avons décidé de préparer les personnels de l'Éducation nationale les plus férus d'informatique, qui le souhaitaient, à enseigner le NSI.

Deux options s'offraient dès lors au ministère. La première, traditionnelle, consistait en une formation interne. Nous avons finalement choisi la seconde en créant un diplôme interuniversitaire avec 22 établissements partenaires d'enseignement supérieur (universités et grandes écoles) spécialisés dans le numérique et l'informatique, selon la démarche prospective que vous évoquiez. La dissémination de ces établissements partenaires sur tout le territoire français garantit à tout professeur la possibilité de mener à bien sa formation, d'une durée de dix-huit mois, même en cas de mutation. Nous tablions sur 1 000 à 1 200 candidats, 2 400 se sont finalement présentés. Nous en avons formé 2 000 et ouvert une nouvelle session l'année suivante.

Les types de formations que je viens de décrire présentent l'intérêt de s'adosser à la recherche tout en transmettant des connaissances techniques fondamentales sans lesquelles la dimension prospective du numérique demeurerait inintelligible.

Un effort soutenu de formation doit être maintenu tout au long de la vie pour éviter que les compétences acquises perdent de leur valeur et, surtout, pour que l'éducation nationale dispose de professeurs à la pointe des évolutions technologiques et des interrogations que celles-ci suscitent.

Le programme de la spécialité NSI ne prévoit pas seulement l'acquisition de connaissances. Sa dimension proactive, en lien avec l'éthique du numérique, oblige l'élève à se poser des questions sur les évolutions technologiques encore à venir. Peu importe que nul ne soit pour l'heure capable d'y répondre, l'important reste la capacité du lycéen à mener une réflexion techniquement informée et à penser l'avenir du numérique.

M. Philippe Latombe, rapporteur. Passons aux questions concernant le ministère proprement dit. Je vais sans doute, là encore, manquer de diplomatie, mais un rapport de l'Inspection générale de l'éducation nationale (IGEN) a signalé des risques pesant sur les

données éducatives. Le rachat, par Docaposte, de la société en cause vous a visiblement rassurés.

On nous indique par ailleurs régulièrement que l'Éducation nationale a recours à des plateformes et des logiciels édités par Google, Amazon, Facebook, Apple ou Microsoft (les GAFAM). Compte tenu du mode de fonctionnement de ces entreprises, l'utilisation de leurs outils présente une menace pour notre souveraineté. Qu'en pense le ministère ? Quelles mesures comptez-vous prendre ?

Cette situation renvoie à la question des logiciels libres et à l'utilisation de données ouvertes. La présence des GAFAM au sein de l'Éducation nationale, dont j'aimerais que nous parlions, soulève des questions auprès des spécialistes du numérique, mais aussi des syndicats d'enseignants et des associations de parents.

M. Jean-Marc Merriaux. Le ministère a certes essuyé des critiques par rapport à certains marchés publics passés avec des entreprises comme Microsoft. Il convient de prendre en compte le contexte historique : à ce jour, la totalité des ordinateurs du ministère fonctionne grâce à des systèmes d'exploitation de la société Microsoft. La dimension administrative de la question que vous abordez repose en grande part sur ce socle numérique déjà en place.

Il me semble toutefois pertinent de distinguer ce versant administratif du problème de celui relatif à la continuité pédagogique. Celle-ci a été assurée entre autres grâce à des outils numériques conçus par les GAFAM. Cependant, le ministère a proposé quantité d'autres dispositifs, comme les ENT ou « ma classe à la maison », alors que, dans d'autres pays européens, ce n'était pas le cas. Nous estimions en effet de notre responsabilité d'offrir une alternative aux GAFAM, dans un environnement plus souverain garantissant le respect de certaines réglementations.

Vous avez insisté sur les logiciels libres. Lors des états généraux du numérique pour l'éducation, il a été proposé d'en généraliser l'usage. Nous comptons mettre en place un véritable plan d'action au service de cet objectif. Notons que les serveurs de l'Éducation nationale reposent essentiellement sur des logiciels libres. Nous nous engageons à promouvoir leur utilisation accrue dans un cadre pédagogique, de manière à renforcer notre souveraineté. Une feuille de route est en cours d'élaboration en ce sens.

M. Philippe Latombe, rapporteur. Cette feuille de route tiendra-t-elle compte des propositions du comité d'éthique au sujet des données éducatives et de la plateforme Education data-hub ?

M. Jean-Marc Merriaux. Je tiens à préciser que nous avons dû développer, à l'occasion du premier confinement, un service disponible à l'adresse apps.education.fr. Ce site met à la disposition de la communauté éducative un certain nombre d'outils sous licence libre, de partage de ressources, de plateforme de vidéos ou encore de microblogging. Il offre en somme un panel de solutions, surtout adaptées à l'enseignement du premier degré, qui ne disposait pas d'ENT. Nous avons notamment développé un outil de visioconférence du nom de BigBlueBotton, qui s'appuie lui aussi sur un logiciel libre. La feuille de route repose sur la mise à disposition de tels outils.

M. Philippe Latombe, rapporteur. Nous avons consacré beaucoup d'auditions aux données de santé, considérées comme sensibles, supposant que ce qui s'appliquait à ce type de données valait aussi, éventuellement, pour les données éducatives et scolaires, relatives à des enfants et donc à des mineurs au regard de la loi. Une polémique a surgi à propos de la plateforme des données de santé (ou *Health data hub*, HDH), confiée à un *cloud* étranger.

Revenons à la plateforme Education data-hub évoquée lors de vos propos liminaires. Sera-t-elle bien hébergée par GAIA-X et donc par un *cloud* souverain ?

M. Édouard Geffray. Nous allons héberger un certain nombre d'éléments de notre Education data-hub sur GAIA-X mais nous nous appuierons aussi sur une plateforme dédiée en tenant compte des questions que soulève l'hébergement des données. De tels enjeux relèvent de toute façon de la stratégie *cloud* portée par l'État et la Direction interministérielle du numérique (DINUM), loin de méconnaître leur dimension de souveraineté.

Concrètement, l'hébergement de notre Education data-hub sur GAIA-X ne semble pas envisageable avant deux ou trois ans, or nous souhaiterions que ce projet aboutisse plus tôt. Il n'est donc pas exclu que nous recourions à une autre option, éventuellement provisoire, et de toute façon en accord avec notre stratégie souveraine.

M. Philippe Latombe, rapporteur. J'attirerai votre attention sur deux points. D'abord, il faudra éviter qu'une polémique de même nature que celle qui a entouré la plateforme HDH n'atteigne l'Éducation nationale.

Ensuite, j'aimerais un éclaircissement sur les propos, qui ont beaucoup agité l'écosystème numérique, tenus par le ministre de l'Éducation nationale, la première semaine du confinement. À l'en croire, une partie des enseignements à distance n'a pu avoir lieu en raison de cyberattaques et de l'incendie de l'entreprise OVH à Strasbourg. Que s'est-il réellement passé ? Entreposez-vous aujourd'hui certaines de vos données dans un *cloud* et, si oui, lequel ? Les systèmes informatiques de l'Éducation nationale ont-ils été surpris par des cyberattaques d'ampleur supérieure à ce qu'ils prévoyaient ? Ces attaques ont-elles révélé des failles de sécurité dans les dispositifs d'enseignement à distance ?

M. Jean-Marc Merriaux. Votre question comporte de multiples dimensions. Comprenez d'abord que, dans une audition publique, nous ne pouvons apporter que des informations limitées sur les mesures de sécurisation des services informatiques du ministère, en tout état de cause confidentielles. Notre ministère dispose d'un réseau spécifique, le Réseau national de télécommunications pour la technologie, l'enseignement et la recherche (RENATER), équipé de dispositifs suffisants pour déjouer toutes les attaques par déni de service (ou DDoS) dont il a jusqu'ici fait l'objet.

Le ministère s'appuie par ailleurs sur un certain nombre de dispositifs portés par ses partenaires. Il nous est plus difficile d'obtenir une vision précise des menaces qui les visent. Nous pouvons malgré tout affirmer que d'authentiques attaques les ont touchés la première semaine du confinement. Nul ne saurait objecter que l'éducation est de plus en plus ciblée par les pirates informatiques.

Je citerai l'exemple récent du logiciel malveillant Emotet, auquel l'Éducation nationale n'a pas échappé. Aussi bien dans les rectorats qu'au sein de l'administration centrale, nous avons toutefois réussi à le contrer ou, du moins, à éviter qu'il n'endommage durablement nos systèmes d'information.

M. Philippe Latombe, rapporteur. Permettez-moi de revenir sur l'émoi de l'écosystème face à l'attribution à l'incendie d'OVH d'une partie des difficultés rencontrées par les dispositifs de l'Éducation nationale. Je me fais l'écho de ces réactions, ayant reçu de nombreux messages sur ce sujet, en lien avec les questions de souveraineté qui nous occupent. La question du soutien à une entreprise française du *cloud*, une rareté dans ce secteur dominé par les GAFAM, malgré les problèmes qu'elle affrontait, a été soulevée.

M. Jean-Marc Merriaux. L'incendie d'OVH n'a impacté qu'un outil spécifique des ENT parmi d'autres. Par ailleurs, nous avons essuyé quelques déconvenues à propos d'apps.education.fr, dont certains services étaient hébergés par OVH. Il nous a été très difficile de récupérer l'ensemble des données stockées sur ce *cloud*.

M. Philippe Latombe, rapporteur. Vous avez évoqué des partenariats avec des entreprises pour vous aider dans votre transformation numérique. Ces sociétés y trouvent-elles également leur intérêt ? Saisissent-elles ainsi une occasion de vérifier qu'elles ont développé leurs services à une échelle suffisante ? Réalisent-elles, ce faisant, une preuve de concept avant de se lancer à l'assaut du marché commercial ? Des laboratoires d'université vous apportent-ils de l'aide, en profitant en même temps pour s'aguerrir ? Des *start-up* vous démarchent-elles spontanément dans un but purement lucratif ? Travaillez-vous avec des *start-up* d'État, à savoir des émanations de l'administration visant à développer des outils à l'usage d'autres ministères aussi ?

M. Jean-Marc Merriaux. Il me semble que vous vous référez aux partenariats de l'innovation évoqués plus tôt. Il s'agit en réalité d'une nouvelle forme de marchés publics se déroulant en trois temps. Notre ministère a été parmi les premiers à y recourir.

Après une première étape de recherche et développement de plusieurs mois, passant par une sélection des sociétés, durant laquelle il convient de s'assurer que la solution envisagée répond à certaines attentes, celle-ci est ensuite déployée dans un grand nombre d'établissements qui la testent. Enfin, sans devoir passer de marché, et sous réserve que les deux précédentes phases aient été concluantes, la solution se généralise, sachant qu'à tout moment, le projet peut s'interrompre, puis reprendre ultérieurement. Cette procédure innovante permet d'accompagner durablement des sociétés, en particulier des *start-up*, amenées à travailler spécifiquement sur des enjeux d'Intelligence artificielle.

Nous réfléchissons, dans le Quatrième programme d'investissements d'avenir (PIA4), au lancement de nouveaux partenariats de l'innovation pour accompagner des sociétés amenées à mettre au point des outils répondant aux attentes des enseignants dans leur pratique pédagogique.

Nos relations avec les *start-up* respectent strictement les règles de passation des marchés publics. Plusieurs initiatives ont impliqué des *start-up* d'État. L'une d'elles a proposé une solution relative aux classes de CP à douze élèves. D'autres expériences n'ont pas abouti, du fait de la complexité de nos systèmes d'information, confrontés à des enjeux de transformation majeurs.

M. Philippe Latombe, rapporteur. Quelle place envisagez-vous pour le numérique dans l'Éducation nationale, à moyen et long terme, à la fois dans le contenu des enseignements, la manière d'enseigner et la gestion du ministère ?

M. Édouard Geffray. Nous assistons à une véritable recomposition du paysage de la pratique pédagogique des enseignants. Dans le même temps, il faut bien garder en tête que les outils numériques ne sauraient en aucun cas se substituer aux professeurs. La période que nous traversons l'a amplement montré. Tout le monde en a fait l'expérience, plus ou moins cruelle.

Néanmoins, nous n'en sommes encore qu'à l'orée des possibilités qui s'offrent aux enseignants d'utiliser des outils numériques en complément d'un cours au déroulement classique, aussi bien à des fins de ce que nous appelons la remédiation, autrement dit, pour aider un élève à surmonter des difficultés ou mieux comprendre un point spécifique d'une

leçon, que pour, tout simplement, lui proposer des révisions plus ludiques, *via* des dispositifs proches de l'environnement quotidien de ce même élève, comme calcul@TICE.

Par ailleurs, le numérique peut aider à surmonter certaines contraintes géographiques. Je songe au dispositif « devoirs faits », qui se heurte parfois aux horaires du transport scolaire des collégiens. Nous déployons des solutions innovantes comme « e-devoirs faits » (cette fois, à la maison et non plus dans l'établissement scolaire), selon des modèles pédagogiques différents. Ainsi, trois professeurs, dans une même salle, peuvent répondre aux questions posées par des élèves depuis leur domicile, voire à certaines interrogations des parents, ce qui crée avec eux une relation, autour des devoirs, complètement différente. Nous n'assistons pas là à une révolution technologique mais bien à une évolution des usages.

Les enseignants innovent en outre d'eux-mêmes, or nous souhaitons valoriser leurs initiatives, une fois leur efficacité prouvée, plutôt que de leur en imposer par la voie hiérarchique. Tout part en somme de la pratique pédagogique du professeur. Quoi qu'il en soit, il me semble probable que l'usage du numérique s'étende dans les champs que je viens d'indiquer.

M. Jean-Marc Merriaux. Revenons un instant aux enjeux liés à l'évolution du numérique. Nous avons constaté, pendant le confinement, que la technologie numérique servait surtout au transport de contenus, ainsi acheminés jusqu'à l'élève. Le potentiel pédagogique des nouvelles technologies, pour faciliter la mémorisation des leçons par leur répétition, notamment, reste encore à exploiter. Le numérique a certainement un rôle à jouer dans les enjeux de différenciation des apprentissages afin d'aider au mieux chaque élève.

Au-delà de ces questions, sur lesquelles ont porté les partenariats de l'innovation, le pilotage du ministère revêt une dimension numérique prégnante. Soulignons que nous utilisons des systèmes d'information grevés par de lourdes dettes techniques. Un travail de fond reste à mener pour améliorer la mise à disposition des données et la gestion des flux de données. Ce chantier considérable n'aboutira probablement pas avant un certain nombre d'années.

M. Philippe Latombe, rapporteur. Ma dernière question établira le lien avec l'enseignement professionnel, que vous évoquiez plus tôt. La plupart des entrepreneurs du numérique nous ont confirmé un besoin d'ingénieurs de haut niveau, dont la France dispose déjà, mais aussi de techniciens compétents, aux qualifications intermédiaires. Les jeunes issus de formations en apprentissage sont donc très attendus sur le marché du travail. Je vous confirme qu'ils ont suivi là une filière d'excellence et d'avenir.

Venons-en à l'enseignement supérieur. Comment se déroule la collaboration des établissements et du ministère ? Comment celui-ci s'assure-t-il de pourvoir en étudiants les universités et les grandes écoles ? Comment veille-t-il à la cohérence des apprentissages ? Nous poserons quoi qu'il en soit ces questions aux représentants de l'enseignement supérieur lorsque nous les auditionnerons. La confiance n'exclut pas le contrôle.

M. Édouard Geffray. Notons pour commencer qu'il existe un *continuum* de formations. Beaucoup de titulaires d'un baccalauréat professionnel « cyber » s'inscrivent ensuite en BTS « cyber ». Des lycéens ayant opté pour la spécialité NSI entreront dans des classes préparatoires aux grandes écoles également spécialisées dans le numérique. Nous menons un travail avec les universités et les grandes écoles autour des compétences acquises par les élèves du secondaire, dans les lycées professionnels aussi bien que généraux.

Un label « campus des métiers et des qualifications d'excellence » a été créé. Des campus se sont construits autour d'une logique territorialisée d'intégration étroite de

l'enseignement scolaire et supérieur. Même si aucun d'eux n'est exclusivement dédié au numérique, certains abordent ce domaine, comme le campus aéronautique à Toulouse, où est dispensé un enseignement, en informatique, de haut niveau.

L'élaboration des programmes de l'Éducation nationale et la formation des professeurs associent l'inspection générale, des enseignants eux-mêmes et, dans le cas des NSI, des universitaires, des ingénieurs et des chercheurs de grandes écoles. Ceux-ci contribuent ainsi à la construction d'un écosystème, dont ils connaîtront les tenants et les aboutissants.

Rappelons enfin que la formation des professeurs se déroule à l'université. Le fait qu'elle comporte des cours obligatoires de sciences numériques et d'informatique prouve bien la hauteur de notre niveau d'exigence.

M. Philippe Latombe, rapporteur. Souhaiteriez-vous aborder des sujets que nous aurions laissés de côté ?

M. Édouard Geffray. Nous venons de brosser un tour d'horizon qui me semble assez complet.

Audition commune, ouverte à la presse, de MM. Renaud Vedel, préfet, coordonnateur de la stratégie nationale pour l'Intelligence artificielle et Julien Chiaroni, directeur du « Grand défi » intitulé « Sécuriser, certifier et fiabiliser les systèmes fondés sur l'Intelligence artificielle » *(6 mai 2021)*

Présidence de M. Philippe Latombe, rapporteur.

M. Philippe Latombe, président et rapporteur. Nous auditionnons M. Renaud Vedel, préfet et coordonnateur de la stratégie nationale pour l'Intelligence artificielle (IA), ainsi que M. Julien Chiaroni, directeur du Grand défi « Sécuriser, certifier et fiabiliser les systèmes fondés sur l'Intelligence artificielle ».

La stratégie nationale pour l'Intelligence artificielle a été présentée par le Président de la République le 29 mars 2018 et prend appui sur le rapport de M. Cédric Villani, rendu public la veille. Cette stratégie vise à faire de la France l'un des pays leaders en la matière. Elle s'appuie sur quatre axes, à savoir : conforter l'écosystème de l'IA en France et en Europe, engager une politique d'ouverture des données, adapter le cadre règlementaire et financier, national et européen, ainsi que définir les enjeux éthiques et politiques de l'IA. Cette stratégie nationale dispose d'un investissement d'1,5 milliard d'euros sur la période 2018-2022.

Dans nos réflexions sur les enjeux de souveraineté numérique, la recherche en matière d'IA ainsi que son déploiement nous apparaissent comme majeurs du point de vue de la compétitivité de nos industries et de la maîtrise technologique. À titre d'introduction, je vous invite à réagir aux trois points.

Premièrement, quelle est votre approche de la souveraineté numérique ? Cette question est maintenant récurrente pour chacune de nos auditions et découle de la grande diversité des définitions. Aussi, quelle en est votre définition, et quelles sont ses interactions avec l'IA, du point de vue de l'application de cette technologie ? En France et en Europe, quels sont les enjeux de souveraineté en ce qui concerne la recherche et le déploiement de l'IA ?

Deuxièmement, dans la mesure où vous occupez la fonction de coordonnateur national de la stratégie pour l'IA, M. Renaud Vedel, je vous propose de procéder à un état des lieux de son avancement à l'approche de l'horizon fixé, à savoir 2022. Plus précisément, je souhaite que nous évoquions les progrès réalisés en la matière, par exemple avec les instituts interdisciplinaires d'intelligence artificielle (3IA). Jugez-vous que, du fait de la crise sanitaire, la stratégie nécessite une relance particulière ? Comment considérez-vous les efforts de mise en œuvre d'un cadre commun à l'échelle européenne ? Sur ce point, je fais référence à l'annonce récente de la Commission européenne d'un Règlement européen spécifique à l'IA.

Troisièmement, du point de vue du développement d'une culture de l'IA et du numérique, comment appréciez-vous l'intérêt des entreprises pour l'IA, y compris de la part de celles qui ne sont pas spécialisées ? Comment évaluez-vous notre capacité à former nos élèves en matière d'IA et de numérique ?

M. Renaud Vedel, préfet et coordonnateur de la stratégie nationale pour l'Intelligence artificielle. En réponse à votre question portant sur la définition de la souveraineté numérique, un nombre croissant d'économistes considère que les technologies d'IA pourraient devenir des technologies d'usage général, comme cela a été le cas pour le

moteur électrique et les transports au cours des révolutions industrielles, ou ensuite avec les technologies numériques dites classiques.

Si cette hypothèse venait à se vérifier dans le futur, les systèmes basés sur l'IA constitueraient un mode d'information se généralisant à l'entièreté du tissu économique. Une nation maîtrisant ces technologies se trouveraient bien positionnée dans la course économique mondiale. D'ailleurs, les grandes capitalisations internationales en attestent puisqu'en dix ans, de grandes entreprises utilisant des algorithmes d'IA ont réussi à s'imposer.

Le projet de Règlement européen pourrait prochainement fournir une définition juridique de l'IA, incluant la mention de « logiciels développés à l'aide de techniques définies par l'homme, générant des résultats tels que des contenus, prédictions et décisions, interagissant avec l'environnement ». Le terme « automatisation » peut résumer cette idée.

L'Intelligence artificielle est utilisée dans les traitements de signaux de l'industrie, du langage naturel, de la vision de l'image par ordinateur, de données de grandes dimensions, ainsi que dans la robotique. Il apparaît que la matrice de l'IA est à même de réaliser de plus en plus de tâches. Le fait qu'une machine, un robot ou un logiciel devienne capable de voir ou d'entendre va nécessairement changer notre rapport à l'autonomie.

L'IA comporte la capacité de calcul, des algorithmes, des données, et des talents. Concernant la capacité de calcul, la France, dans sa stratégie sur la base du rapport de M. Cédric Villani, a souhaité limiter les inégalités d'accès à la puissance de calculateur, passant du *petascale* à l'*exascale*, avec la création du supercalculateur Jean Zay pour GENCI (Grand équipement national de calcul intensif). Ce supercalculateur voit ses usages augmenter, avec une nouvelle tâche lui parvenant chaque jour. Des initiatives complémentaires sont à souligner, comme le *cloud* d'État, la filière microélectronique dans le cadre d'un IPCE, projet commun européen, ou les travaux originaires d'Allemagne et désormais européanisés, de GAIA-X, offrant une filière européenne au calcul de haute performance. L'enjeu majeur des années à venir consistera à embrasser le développement de l'Internet des objets. Nous estimons à 80% de la puissance de calcul la part qui sera distribuée en périphérie.

Concernant la formation, la stratégie de l'IA vise, en France, à multiplier par deux, puis par quatre, le nombre de personnes formées, incluant des experts tels que des ingénieurs et des docteurs, mais pas seulement. Au cœur de la bataille mondiale sur cet enjeu de souveraineté de l'IA, nous nous apercevons de l'existence d'un goulot d'étranglement, malgré la qualité de nos écoles d'ingénieurs, amenant à une tension en ce qui concerne le nombre de profils. En ce sens, un double cursus doit s'appliquer, par exemple l'IA et la santé, l'IA et l'agriculture, l'IA et l'industrie 4.0, l'IA et la culture, etc. De même, nous aurons besoin de techniciens d'un niveau DUT ou licence, car une fois qu'un système d'IA est développé, il convient d'en comprendre les limites, les règles éthiques de fonctionnement, les alertes et être capable de préparer les données. Ces tâches ne nécessitent pas en elles-mêmes un haut niveau d'expertise, mais requièrent cependant une formation particulière.

Pour le reste, nous faisons état du point le plus difficile, à savoir l'intégration de l'IA à l'ensemble du mouvement numérique à l'échelle du marché du travail. En effet, l'IA est un objet avancé sans être à part, et elle s'intègre dans l'ensemble de la transformation numérique. Un produit d'IA n'est jamais exclusivement composé d'IA. Ce produit disposera de fonctionnalités d'IA mais interviendra dans un système où l'humain aura sa part de décision et de contrôle, comprenant l'usage de techniques numériques plus classiques. Dans cette optique, la population active, comme les Français ensuite, devront pouvoir interagir et comprendre l'IA, sans pour autant en être experts. L'IA s'utilise alors par la commande vocale ou par les gestes, impliquant l'apprentissage d'interfaces.

Sur la question des 3IA, il découlait effectivement d'une volonté du Président de la République et du gouvernement de concentrer l'activité sur des pôles de taille internationale. Pour autant, une répartition des rôles s'opère à l'échelle nationale au sein des centres de recherche ou des universités, sachant que les quatre 3IA de Paris PRAIRIE (PaRis Artificial Intelligence Research Institute), Toulouse ANITI (Artificial and Natural Intelligence Toulouse Institute), Nice 3IA Côte d'Azur et MIAI@Grenoble-Alpes (Multidisciplinary Institute in Artificial Intelligence) de Grenoble concentrent 137 des chaires sur les 180 existantes. Une ville ne disposant pas d'un institut pourra cependant travailler autour de l'IA, comme en attestent les seize chaires du plateau de Saclay. De même, un soutien accru est apporté à la recherche partenariale et au transfert de technologie, en direction des instituts de recherche technologique (IRT), des instituts pour la transition énergétique, des instituts Carnot et des pôles de compétitivité. Le plan de relance européen comprend également des mesures de sauvegarde pour la recherche.

Concernant la diffusion de l'IA dans l'économie, cette technologie bénéficie des outils transversaux habituels de l'économie numérique. Bpifrance a porté le plan Deeptech, et des challenges d'IA ont été organisés afin de faire travailler ensemble des *start-up* ou PME avec de grands acteurs économiques, dans un équivalent de parrainage. Dans le même ordre d'idée, des concours d'innovation ont eu lieu, ciblés sur des mono-porteurs de projets. Aussi, une part croissante des projets structurants des pôles de compétitivité – qui existent depuis quinze ans – a concerné les technologies d'IA.

Enfin, l'approche de l'IA hérite de trois « Grands défis », dont l'un « Sécuriser, certifier et fiabiliser les systèmes fondés sur l'Intelligence artificielle » est dirigé par M. Julien Chiaroni. Le deuxième des « Grands défis » de l'IA est conduit par M. Olivier Clatz et s'intitule « Améliorer les diagnostics médicaux à l'aide de l'Intelligence artificielle ». Il sera par ailleurs intégré à la stratégie du ministère de la santé sous le volet de la santé numérique. Le dernier « Grand défi » en matière d'IA porte sur la cybersécurité, afin de « rendre nos systèmes durablement résilients aux cyber-attaques ». Au cours de nos échanges, ce matin, je pourrai également vous présenter l'écosystème de l'IA de façon plus précise, ainsi que son état de maturation.

M. Julien Chiaroni, directeur du Grand défi « Sécuriser, certifier et fiabiliser les systèmes fondés sur l'Intelligence artificielle ». Je fais miens l'ensemble des propos de M. Renaud Vedel et veux ajouter deux précisions.

En premier lieu, pour l'ensemble de ses éléments génériques dans l'espace numérique, l'IA relève d'infrastructures logicielles, qui se trouvent être fondamentales car, d'une part, elles génèrent du *business*, et, d'autre part, elles permettent de créer un écosystème innovant autour de cette infrastructure. À ce titre, vous connaissez sans doute la loi de Metcalfe selon laquelle la valeur d'un écosystème est fonction du nombre de participants à son réseau. Ces infrastructures logicielles me semblent essentielles en vue de construire un socle, soit pour du *business* applicatif, soit pour de nouveaux services généralisés à l'ensemble des filières. Ces infrastructures nécessitent des investissements très importants, autant du point de vue de la structure technique que d'un écosystème d'innovation. Nécessairement, des tensions apparaissent entre les secteurs applicatifs et les infrastructures génériques, que survienne, soit un partage, soit une captation, de la valeur par les infrastructures numériques, à l'égard des filières sectorielles. Ces infrastructures étendent leur portée à l'égard du *business* comme de la souveraineté.

En second lieu, l'IA intervient fortement dans le *business to consumer (B to C)* mais bien moins dans le *business to business (B to B)*. D'importants enjeux d'industrialisation de l'IA existent, impliquant ensuite une *compliance* et une règlementation spécifique autour de

l'IA. Cette conformité de l'IA a trait aux enjeux de souveraineté, qui se généralisent alors à l'ensemble des secteurs. Ce phénomène devrait s'opérer dans les années à venir.

M. Philippe Latombe, rapporteur. En écho à vos propos introductifs, je me souviens que, lors de leurs auditions, les spécialistes et industriels du *cloud* nous indiquaient que la France et l'Europe avaient perdu la bataille de l'IA dans le *cloud* mais qu'elles possédaient une longueur d'avance concernant l'IA des objets. Partagez-vous ce point de vue ?

M. Renaud Vedel. Ce propos doit être nuancé. Il est vrai que le *cloud* s'est développé à partir de grandes applications à destination des consommateurs, c'est-à-dire des applications de service, se basant sur la localisation, des algorithmes comme ceux des réseaux sociaux. Ces technologies ont été utilisées par les GAFAM et les NATU.

Pour autant notre base industrielle diffère et commence à incorporer de l'IA dans les objets. Nous parlons alors de périphérie ou *Edge AI* en anglais. De ce point de vue, l'élaboration des standards et la compétition ne sont pas encore achevés. Ce type d'IA intervient davantage pour des systèmes de grands réseaux, tels que la distribution d'eau, l'éclairage urbain, et, en ce sens, sont plutôt rattachés aux territoires. Je souligne que la France et l'Europe se montrent performants dans le domaine spatial, l'automobile ou le ferroviaire.

Bien que cette IA embarquée intervienne à la périphérie, un partage des tâches s'opère entre l'IA du *cloud*, et l'IA de périphérie. Une complémentarité s'articule et je ne pense pas que le *cloud* soit amené à disparaître face à la périphérie. Simplement, comme l'affirme M. Thierry Breton, l'ordre de grandeur actuel de 80% pour le *cloud* et 20% pour la périphérie pourrait s'inverser à l'avenir.

M. Julien Chiaroni. J'ajoute que du point de vue de l'automatisation, il va être cherché davantage encore à intégrer l'IA dans l'ensemble des objets connectés. Je confirme cette forte tendance du *edge*, sachant qu'il existe deux types de *edge* à mon sens. D'un côté, nous trouvons un *cloud at the edge*, comme en promeut Atos par exemple, c'est-à-dire à la périphérie, au plus près d'une usine, à titre d'illustration. D'un autre côté, il existe un *edge* plus proche de l'objet et de l'Internet de l'objet. Dans tous les cas, les deux sont complémentaires.

Quoiqu'il en soit, il apparaît que la maîtrise technique, la maîtrise du marché et la maîtrise de la souveraineté passent par la compréhension d'une addition de *stack* (empilement de données) techniques et règlementaires portant sur l'ensemble de la chaîne de valeur. En somme, une décomposition s'opère, de la donnée jusqu'au capteur et il convient de prêter attention aux éléments adéquats de la chaîne de valeur.

M. Philippe Latombe, rapporteur. Vous avez évoqué la règlementation portant sur l'IA et le projet actuel à l'échelle européenne. Hormis ces dispositions que l'Union européenne envisage, estimez-vous qu'il existe une urgence à adapter une règlementation, ou à en proposer de nouvelles, afin de fluidifier l'utilisation de l'IA ? Par extension, avez-vous connaissance de règlementations provenant d'autres acteurs, comme la Chine ou les États-Unis, susceptibles de faire naître un risque d'extraterritorialité, qui nous pousserait à nous adapter au lieu d'être pleinement décideurs des règlementations en vigueur en matière d'IA ?

M. Renaud Vedel. Nous constatons un changement de paradigme technique. Il est vrai que l'IA a vu le jour avec l'informatique, sachant que le premier article l'incluant date de 1950, mais depuis une décennie, tant les capacités de calcul que l'algorithmie ou la combinaison des données du fait de la numérisation généralisée, nous permettent de mettre en

œuvre des IA d'ordre statistique et multi-échelle. La façon de concevoir et de programmer diffère de celle relevant de l'informatique classique.

Du point de vue des domaines règlementés, comme la sécurité, la sûreté ou le risque, les modélisations réalisées à partir des données sont plus puissantes, mais aussi plus fragiles, du fait de l'existence de risques de divergence. Après une mise sur le marché du produit, les circonstances peuvent évoluer, voyant naître des données nouvelles ou des phénomènes nouveaux. Pour cette raison, il convient d'opérer une surveillance post-marché intense. C'est d'ailleurs l'un des points centraux de la future règlementation européenne. Ainsi, les anciennes règlementations n'auront pas à être abandonnées, mais devront être revisitées.

M. Julien Chiaroni évoquera sûrement les systèmes d'IA critiques. Pour prendre l'exemple de la santé, qui est un domaine critique, les autorisations préalables de mise sur le marché d'un médicament, conçues à l'aide d'un dispositif d'IA médical, devront faire l'objet d'une surveillance post-marché en continu. Formulé autrement, les données ayant servi à façonner l'outil doivent être vérifiées en permanence, afin de s'assurer qu'elles soient toujours représentatives. Ce paramètre produit un mouvement bien plus complexe à maîtriser, mais dont les résultats peuvent être significatifs, car la modélisation humaine peut présenter des limites face aux capacités d'un outil d'IA.

M. Julien Chiaroni. Il faut rappeler que la voie du Règlement, choisie par l'Union européenne, va se décliner en standards et normes dans chacun des États membres, dans une logique d'harmonisation. Les acteurs de l'IA seront impliqués, en vue de déployer ces éléments règlementaires au sein de l'écosystème et du marché.

En revanche, d'autres acteurs agissent par le biais de la normalisation et de la standardisation, comme le font les États-Unis ou la Chine, qui montrent une grande implication sur ces sujets et dans les instances concernées, dans le but d'imposer leur vision des spécifications à respecter en matière d'IA. Ainsi, l'approche américaine semble comporter l'élément de la confiance dans l'IA, qui fera partie de la *compliance* au sens large. Cette confiance constituera donc par la suite une barrière, créant des difficultés à l'entrée pour les acteurs n'en remplissant pas les conditions.

Il convient également de rappeler que la règlementation européenne portera sur des applications à hauts risques, comme la mobilité ou des applications étatiques. Elles seront ainsi peu nombreuses mais importantes en valeur. Or, cette volonté de règlementer va avoir pour conséquence la nécessité de développer un socle technique permettant aux acteurs industriels d'y répondre. Cet enjeu d'envergure est d'ailleurs envisagé dans le « Grand défi ». Ces importantes barrières techniques que nous poserons à l'entrée permettront ensuite de développer des applications et des *business* sur les marchés, offrant un avantage compétitif aux acteurs en disposant, face à ceux ne répondant pas aux critères.

M. Philippe Latombe, rapporteur. L'histoire industrielle montre que l'acteur capable d'imposer ses standards dispose d'une avance importante sur ses concurrents dans l'utilisation commerciale du système. La France et l'Europe se trouvent-elles en pointe quant à la définition des standards relatifs à l'IA ou, au contraire, considérez-vous que les États-Unis, ou d'autres acteurs, sont en passe de nous imposer les leurs ? Les standards semblent en cours d'élaboration mais comportent des technologies non encore parvenues à maturité ou susceptibles d'évoluer à nouveau.

M. Renaud Vedel. La proposition de Règlement de la Commission européenne est inédite et constitue une tentative en vue d'établir une forme de règlementation pour l'IA. Il ne faut toutefois pas sous-estimer la dimension processuelle de cette règlementation, dans son

volet horizontal, car chaque fournisseur d'IA sera soumis à des obligations lourdes, incluant un système de maîtrise des risques, une surveillance post-commercialisation ou des déclarations d'incidents.

Aussi, des règlementations interviendront de manière complémentaire, secteur par secteur. En ce sens, les règles du marché communautaire devront être révisées. La Commission précise que les standards adéquats, comprenant la documentation technique, devront s'appliquer. Et si ces standards n'existent pas, la Commission se réservera le droit d'adopter des spécifications communes. La volonté d'agir de l'Union européenne sur la standardisation intervient par exemple par le Comité européen de normalisation (CEN) et le Comité européen de normalisation en électronique et en électrotechnique (CENELEC). En France, le « Grand défi » comprend un volet portant sur la normalisation.

M. Julien Chiaroni. Nous sommes conscients de la portée fondamentale des normes et standards. À ce titre, le « Grand défi » finance un projet à hauteur d'1,6 million d'euros, ce qui constitue une première, en termes de méthodologie et d'investissement de l'État.

L'approche règlementaire de la Commission européenne va se décliner sous la forme de normes et de standards, qui ne pourront pas être découplés des éléments techniques. Les normes relèvent d'un même *framework* que la technique et la standardisation. Quand bien même l'Union européenne parviendrait à développer ses standards, le chemin ne serait qu'à moitié parcouru, car il faudrait encore façonner les éléments techniques capables d'y répondre. Or, c'est à ce stade que naîtront les dimensions de souveraineté et de création de valeurs. L'architecture à façonner semble particulièrement complexe et nécessite de nombreux *stack* depuis le *cloud* jusqu'aux applications. Les standards constituent une clef, qui devra être déclinée dans le processus technique afin de déboucher sur les applications. L'ensemble que je présente se devra d'être maîtrisé, en vue de couvrir l'intégralité de la chaîne de valeurs.

M. Philippe Latombe, rapporteur. Sur le plan de la formation, proposons-nous des filières définies et claires, visant à former des spécialistes du domaine de l'IA et à même de prendre le relais des actions menées aujourd'hui ? Ainsi, je constate que nous sommes trois hommes dans cette conversation. Vos collègues sont-ils aussi des femmes ? Et si tel n'est pas le cas, quels sont les moyens qui permettraient de féminiser l'ensemble du milieu de l'IA ?

M. Renaud Vedel. En ce qui concerne la formation, nous n'avons encore parcouru qu'entre un tiers et la moitié du chemin, au regard de la transformation et de l'émergence des formations qu'exige la vague technologique. La formation ne doit pas reposer uniquement sur la formation initiale, bien que de très importants efforts sont à fournir sur ce plan. Nous devons également revitaliser les connaissances ou procéder à l'entraînement de certains acteurs qui n'opèrent pas directement sur l'IA mais qui auraient la capacité d'investir le sujet. Dans le monde professionnel, il faut également que les fonctions comme les ressources humaines, le *marketing*, le *business* deviennent capables de comprendre et d'intégrer les systèmes d'IA dans leurs façons de raisonner. Nous constatons un important effort de ce point de vue et l'offre de formation s'étoffe grandement. L'État, par le biais des 3IA, cherche à contractualiser en nombre en matière de formation.

Concernant la féminisation, nous nous devons d'admettre que l'informatique présente un très net manque de diversité et cet enjeu constitue un défi. Il serait par exemple intéressant, dès le plus jeune âge, à l'école, dans l'approche des sciences et de l'informatique, d'expliquer que la matière ne se limite pas à être le domaine de jeunes garçons adeptes des jeux vidéo. En ce sens, le tissu des *start-up* cherche à bousculer les codes, à prendre des initiatives pour diversifier, et atteindre des publics différents.

M. Philippe Latombe, rapporteur. La question de la diversité n'est-elle pas d'autant plus importante du fait de l'existence de biais ? Au regard de ces derniers, comment appréhendez-vous la faible féminisation du domaine, et comment envisagez-vous de corriger ou réduire ces biais ?

M. Renaud Vedel. Du point de vue de la conceptualisation, un travail a été mené depuis deux ans, se traduisant par la multiplication de documents internationaux, dont il apparaît qu'ils convergent quant au recensement des biais.

Les biais peuvent survenir à différents niveaux, de l'humain à la machine. Par exemple, un humain pourrait sélectionner des données qui ne seraient pas représentatives vis-à-vis de l'ensemble à modéliser. Outre les biais de modélisation, des biais techniques peuvent survenir et donner lieu à un débat comme en France, en Europe et aux États-Unis, quant à déterminer la portée des corrections à apporter, par exemple en matière de prescription.

Deux illustrations peuvent éclairer ces situations. La première est celle de capteurs photographiques dans l'industrie du cinéma, dont on s'est aperçu que les focales ou les réglages techniques favorisaient certains types de peau, au contraire d'autres types de peau. La seconde illustration porte sur les modèles géants pré-entraînés du langage aux États-Unis. Entre le jeu d'apprentissage non supervisé et le langage de la société, des biais – bien qu'ils puissent également exister dans la société – peuvent être incorporés et perpétués dans la machine. Ces biais doivent être corrigés, mais s'ouvrent alors des débats éthiques.

À l'heure actuelle, les documents sont établis et commencent d'être déclinés sous la forme de processus opératoires et *check list*. Mais il convient de les déployer secteur par secteur et différemment selon chaque machine. Il est bon de rappeler que, pour la première fois, l'Union européenne, par son projet de Règlement, envisage de mettre en place une obligation de tester les appareils sur ces biais à tous les stades, allant de la conception, en passant par la validation et jusqu'à la surveillance post-validation.

M. Julien Chiaroni. Les problèmes de biais doivent être considérés comme des éléments de spécification, dans la mesure où les systèmes doivent comporter des spécifications claires au sujet des biais, de la robustesse, etc. La difficulté tient alors au fait de prendre en compte l'intégralité des biais et demande ainsi une excellente définition des éléments à sélectionner. L'*AI Index* de l'université de Stanford rend compte d'un important travail de spécification réalisé par de nombreuses instances, nationales comme internationales.

Le véritable enjeu tient dans la capacité à décliner les exigences en matière de sûreté, d'éthique et de confiance dans ces systèmes, prouvant ainsi que ces derniers respectent les spécifications. De grandes exigences peuvent être fixées, mais s'il n'est pas possible de les démontrer, par exemple pour un véhicule autonome, l'ensemble de la chaîne n'est pas couvert et il ne pourra pas être répondu aux enjeux socioéconomiques.

M. Philippe Latombe, rapporteur. Vous l'avez dit, la formation fait partie du plan 2018-2022. De manière générale, la crise sanitaire a-t-elle produit un effet de freinage quant à la réalisation des objectifs de 2022 ? Seront-ils atteints ou devront-ils être réajustés ?

M. Renaud Vedel. La crise sanitaire a produit divers effets hétérogènes mais aussi bien dans le domaine du numérique que celui de l'IA plus spécifiquement, elle n'a pas été un obstacle majeur produisant un ralentissement. Par exemple, les importants investissements dans les *start-up* en France en attestent, avec cinq milliards de dollars investis en France, bien qu'il soit difficile d'isoler le sujet de l'IA des autres technologies du numérique. À l'échelle européenne, la position de la France est bonne, bien que Londres demeure de loin le principal

centre de compétences. Pour autant, Paris constitue le premier écosystème en Union européenne.

En revanche, des risques ont rapidement été identifiés quant à la fuite des talents ou au sous-investissement dans l'IA. En effet, les systèmes d'IA étant encore des technologies en voie de maturation, les grands industriels, comme les *start-up* réalisant de la R&D, peuvent mener des arbitrages entre le court et le long terme, et ainsi juger que l'IA n'offre pas de retour sur investissement immédiat. Du point de vue des profils rares, une compétition intense a lieu, incluant des acteurs puissants qui profitent de ce que d'autres rencontrent des difficultés conjoncturelles, pour recruter les ressources.

Afin de favoriser le transfert de technologie, le modèle des 3IA connaissait une indexation sur les participations collaboratives privées, avec trois parts de financement dont une pour le standard de base, puis un euro versé par l'État pour chaque euro récupéré auprès de l'industrie dans les marchés collaboratifs. Devant la menace d'un écroulement du modèle, l'État a temporairement suspendu cette condition.

En réponse à la crise, il convient aussi de noter que le plan de relance, dans son volet portant sur la recherche privée, permet la mise à disposition de chercheurs privés pour les laboratoires publics, avec une prise en charge de 80% par l'État. De même, l'État cherche à protéger la génération des chercheurs en IA, en offrant la possibilité d'un accueil temporaire dans les laboratoires publics pour des projets de recherche avec un contrat de travail qui, au bout de deux ans, sera pris en charge par une entreprise, ou entrera dans un financement de post-doctorat.

Je termine en ajoutant que des approches par filière et multi-filières devront être adoptées, afin du mutualiser les charges comme les risques à investir dans les systèmes d'IA encore en voie de lancement.

M. Julien Chiaroni. Au sujet de l'approche multi-filières, nous constatons que l'IA va atteindre l'ensemble de la chaîne des acteurs industriels, depuis l'ingénierie et l'industrie 4.0 jusqu'aux produits et services. Pour autant, dans l'arbitrage que ces acteurs mènent, les applications choisies relèvent davantage du *business* traditionnel.

De ce fait, les investissements dans les socles d'infrastructure, ou de plateforme, baissent. Or, ces socles sont fondamentaux et stratégiques en ce qu'ils permettent aux écosystèmes et aux applications de monter en compétences. Des plateformes comme *TensorFlow*, par exemple, soutiennent les chaînes de développement et cherchent à maintenir les niveaux d'investissement.

Nous essayons de contrebalancer cette baisse des investissements dans les socles d'infrastructure par le développement d'approches multi-sectorielles, dont je peux vous citer un exemple avec le « Grand défi », car l'un de nos plus importants programmes implique jusqu'à six filières partageant un même problème et mutualisant les risques et les investissements. Elles œuvrent ainsi pour une approche générique, c'est-à-dire des socles de plateforme bénéficiant à l'ensemble de l'écosystème.

M. Philippe Latombe, rapporteur. Estimez-vous que le Parlement français pourrait modifier les paramètres financiers et les investissements en matière d'IA ?

M. Renaud Vedel. À l'échelle nationale, le programme des investissements d'avenir (PIA) 3 et ensuite le PIA 4 comprennent la stratégie de l'IA. Ces fonds devront être combinés avec ceux hérités du fonds de relance européen, dont 20% sera consacré au numérique incluant

l'IA. En résumé, le plan européen coordonné va articuler et cofinancer les actions nationales. En cela, la stratégie nationale doit être révisée pour la période 2021-2027, avec les outils fournis par la Commission européenne. Par exemple, des appels à projets auront lieu pour des plateformes de test et d'expérimentation. Des pôles d'innovation numérique seront mis en place et certains pôles de compétitivité se spécialiseront dans l'IA. Il existe aussi l'action lancée par M. Thierry Breton portant sur les espaces de données, qui devra être transposée en France.

À ce titre, en France, le domaine de l'agriculture est en train de prendre le virage du numérique et de l'IA, bien que les outils aient encore besoin de monter en puissance. D'une part, il existe un volet à tendance associative, avec le Agdatahub, qui est une plateforme de données souveraines et de services associés, cofinancée dans le cadre de la stratégie. D'autre part, il existe un acteur plus commercial, qu'est API-AGRO, place de marché et de données d'algorithmes disposant d'une licence et soumise au régime de liberté du commerce et de l'industrie. Enfin, l'association NumAlim cherche à standardiser les données de l'agriculture française.

En conclusion, l'écosystème se développe, permettant d'espérer échapper à la situation où les grands semenciers et fournisseurs de machines agricoles possèderaient un monopole sur les données. Nous pourrions transmettre à l'agriculture française les moyens de maîtriser ses données et de les valoriser, comme nous ambitionnons de le faire pour les neuf premiers secteurs identifiés par les États membres et la Commission européenne.

M. Philippe Latombe, rapporteur. Selon vous, voir figurer la mention de 20% des fonds européens à destination du numérique est-il suffisamment précis pour que l'IA en bénéficie également ?

M. Renaud Vedel. Il ne s'agit encore que d'une phase de démarrage. Pour autant, DigitalEurope et Horizon Europe offrent de l'espace à l'IA, puisque tel est le vœu de la Commission européenne. Tout financement serait le bienvenu, mais nous jugeons que l'effort est engagé. À l'échelle nationale, le PIA 3 inclut favorablement l'IA et nous attendons maintenant les annonces des ministres pour le PIA 4. Il faut aussi accepter l'idée selon laquelle tous les investissements ne porteront pas précisément sur l'IA mais que l'IA s'y diffusera, comme dans le cadre du programme d'éducation numérique.

M. Julien Chiaroni. Sous un angle différent, qui n'engage que ma personne, j'estime que les investissements dans l'IA, en France ou à l'échelle de l'Union européenne, posent la question de la méthodologie d'intervention et de l'accompagnement, ainsi que de leur degré, sur divers sujets. Une analogie peut être posée entre les aspects de plateforme et les questions d'infrastructure. À mon sens, la méthodologie d'approche de l'intervention publique et des mécanismes financiers d'intervention par les États membres ou l'Union européenne pourraient être étudiés, en vue de renforcer le positionnement des acteurs sur ces chaînons des plateformes, essentiels en termes de souveraineté. Je peux préciser mon propos.

M. Philippe Latombe, rapporteur. Je ne suis pas certain d'avoir perçu le sens de chacun des éléments.

M. Julien Chiaroni. Comme le mentionnait M. Renaud Vedel à propos de l'agriculture, certains applicatifs se rapprochent d'applications usuelles, bien que de l'IA soit introduite dans le *business*. En revanche, pour les éléments génériques de socle, qui supportent l'ensemble, nous pourrions envisager une intervention différenciée, afin de fédérer les acteurs, mutualiser et créer un écosystème. Si l'État avait une attitude plus directive et plus récurrente, il serait possible de développer ces socles techniques. Actuellement, qu'il s'agisse d'une

plateforme stratégique du point de vue de la souveraineté, ou d'une autre plateforme qui ne l'est pas, le taux d'intervention est le même. C'est sur ce point que je suggère d'adopter une approche différente.

M. Philippe Latombe, rapporteur. Les entreprises, amenées à devenir clientes et utilisatrices des systèmes d'IA, ont-elles suffisamment connaissance de la teneur de ces technologies, et, à ce titre, sont-elles en mesure de les intégrer à leur stratégie ? L'écosystème de l'IA communique-t-il suffisamment sur les possibilités offertes aux entreprises par cette branche du numérique ?

M. Renaud Vedel. D'abord, la plupart des organisations et entreprises ne se situent qu'en phase d'expérimentation, voire de découverte.

Ensuite, la Commission européenne a évalué le taux de maturité des entreprises vis-à-vis de l'IA : sur un panel de 10 000 entreprises, dont 550 françaises, seules 42% ont adopté une technologie et 25% utilisent au moins deux technologies.

Pour autant, même si la France compte parmi les pays les plus en retard, elle est également le pays qui compte le plus de projets. La phase actuelle consiste encore à recueillir les investissements des clients, en vue de rendre l'écosystème national solvable. Ce paramètre suppose de l'apprentissage, de la découverte et une « évangélisation », bien que je n'affectionne pas ce terme.

Enfin, quant aux processus utilisés, la sphère industrielle fait déjà usage de la détection d'anomalies, de l'automatisation des processus de production ou de la chaîne de montage, même si des progrès restent à réaliser.

M. Julien Chiaroni. Une forte hétérogénéité entre les acteurs se doit d'être soulignée, en termes de compétences et d'appréhension de l'IA. L'un des principaux problèmes tient au passage de la *Proof of concept* (POC, preuve de concept) au véritable produit ou service industriel.

Des plateformes comme *TensorFlow* ou les modèles pré-entraînés permettent de façonner rapidement une POC, avec des coûts acceptables. Mais la phase d'industrialisation et de déploiement étant très coûteuse, ce sont sept POC sur huit qui ne sont pas déployées ensuite.

M. Philippe Latombe, rapporteur. Ces observations valent-elles également pour la sphère publique ? De nombreuses collectivités territoriales souhaitant réaliser la transition vers les villes intelligentes auront besoin de l'IA. S'y projettent-elles au travers des technologies, ou, comme pour les entreprises, en sont-elles encore à la découverte ?

M. Renaud Vedel. D'un point de vue global, il n'y a pas de différence entre la sphère publique et les entreprises : elles se situent aux prémices. Pour autant, les services régaliens se dotent de véritables programmes d'IA, par exemple pour les ministères des armées ou des finances.

Il est vrai qu'en comparant une petite à une grande structure, l'utilisation de l'Intelligence artificielle peut aller du simple au double mais les types de produits ou d'Intelligence artificielle peuvent également différer. Nous concédons qu'il existe un retard.

Au compte des freins à l'adoption des technologies d'Intelligence artificielle, nous pouvons pointer, d'une part, la difficulté d'embauche de salariés ayant la compétence

nécessaire, avec le goulot d'étranglement que je mentionnais plus tôt, et d'autre part, le fait que les technologies peuvent être difficiles à « prendre en main ». Si une organisation se trouve en retard, elle ne doit pas utiliser de l'Intelligence artificielle pour le principe, mais plutôt engager une véritable transformation numérique.

Selon le cabinet de conseil Boston Consulting Group, les investissements technologiques en IA se décomposent en 10% pour l'algorithme, 20% pour la chaîne complète de technologie et 70% pour la transformation du processus opérationnel. Ainsi, ces investissements s'avèrent lourds. À cela s'ajoutent les obstacles règlementaires, dont le Règlement général pour la protection des données (RGPD), les études d'impact. Il nous faudrait faciliter ou simplifier l'accès à l'Intelligence artificielle, par l'utilisation de références et de standards.

M. Philippe Latombe, rapporteur. Bpifrance n'a-t-elle pas pour rôle « d'évangéliser » ? Participe-t-elle à vos travaux et met-elle en place des passerelles avec les entreprises ?

M. Renaud Vedel. Nous avons de réguliers entretiens avec Bpifrance, d'autant qu'elle est l'opérateur pour la plupart des appels d'offres. Des événements ont lieu chaque année, comme le Bpifrance Inno Generation (BIG), forum au cours duquel des présentations de technologies sont faites aux industriels. Bpifrance réalise un important travail d'animation dans l'écosystème, y compris avec les pôles d'activité comme Cap digital.

L'ensemble doit encore gagner en maturité et se structurer en ce qui concerne l'Intelligence artificielle. Peut-être devrions-nous recourir à des démonstrateurs secteur par secteur.

M. Philippe Latombe, rapporteur. Quelle est l'activité, en matière d'Intelligence artificielle, des grands ensembles tels que les États-Unis, la Chine ou la Russie ? Pourrions-nous intégrer certaines de leurs réussites dans nos stratégies ?

M. Renaud Vedel. Concernant les États-Unis, l'une de leurs grandes forces repose sur la R&D, suivie de la commercialisation, en s'appuyant sur des universités, telles que dans la Silicon Valley, à New-York, Seattle ou Boston. Cette puissance, s'ajoutant à la capacité d'un certain nombre d'acteurs à racheter leurs concurrents, fait encore défaut à l'Europe.

À ce titre, à chacune de mes rencontres avec des entrepreneurs de *start-up*, je m'aperçois que, dans leur stratégie, figure toujours l'étape au cours de laquelle elles iront s'implanter aux États-Unis. En ce sens, le rapport remis par M. Philippe Tibi sur le financement des entreprises technologiques françaises constitue une réponse, invitant à accompagner la montée en maturité des entreprises et leur donner les moyens de rester en Europe, si elles le désirent. Mais le marché américain définit souvent le standard de commercialisation, puisque nous évoluons dans un monde global, comprenant un net tropisme états-unien. Sans les réseaux et les appuis d'envergure qui proviennent des États-Unis, les projets voient leurs chances de réussir se réduire.

L'Union européenne se doit d'être plus offensive et de créer une unité entre les parlements nationaux, car l'Europe représente un marché de 450 millions d'âmes contre 330 millions aux États-Unis.

Concernant la Chine, la problématique est différente car le marché est gigantesque, relativement homogène et guidé par une puissance publique, bien que l'organisation soit capitalistique, avec des équipes nationales réparties autour de domaines et de secteurs clefs.

Leur plan de 2007 avait vexé les États-Unis, puisque la Chine ambitionne de devenir leader en Intelligence artificielle d'ici à 2030. Les États-Unis avaient répondu dès 2008 par un plan intitulé « Rester les meilleurs ».

Il est indéniable que la concurrence existe mais en investissant et en développant, nous pouvons mener une stratégie de rattrapage, comme le fait la Chine à l'égard des États-Unis.

M. Julien Chiaroni. Un rapport de la commission nationale de défense sur l'Intelligence artificielle vient de paraître aux États-Unis, et son contenu montre la volonté de ce pays de demeurer leader dans le domaine, avec une approche à la fois civile et de défense, mais en l'élargissant au-delà de ces deux volets, par exemple avec la microélectronique. L'alliance du matériel et du logiciel est une des clefs de la réussite, d'où l'importance de diversifier les domaines d'investissement, afin de développer les systèmes adéquats.

J'appuie les propos de M. Renaud Vedel quant au constat selon lequel l'Europe a les capacités, humaines et d'entreprise, pour répondre aux exigences de la situation. De nombreuses opportunités se présentent et l'alliance de la règlementation et de la *compliance*, que je mentionnais tout à l'heure, ainsi que le soutien au développement technologique, peuvent procurer un avantage compétitif aux acteurs européens. Une double approche, règlementaire et d'investissement, permettrait de verrouiller certains marchés et de leur assurer une avance certaine.

M. Philippe Latombe, rapporteur. Au regard de notre échange de ce jour, voulez-vous porter à notre attention de législateur l'existence d'autres sujets sur lesquels l'État pourrait intervenir ?

M. Renaud Vedel. Il convient de s'assurer que les normes qui seront appliquées laisseront la place à l'interprétation et à des « bacs à sable » d'expérimentation, car ces technologies évoluent très vite. Nous en avons la preuve dans le domaine du langage, avec les *transformers*, ou dans le domaine de l'image, il y a dix ans.

Par ailleurs, nous nous apercevons que le RGPD, rédigé entre 2014 et 2016 et adopté en 2016, ne comportait pas la question du *big data* et de l'Intelligence artificielle. Par exemple, la réutilisation des données avec un lien connexe n'a pas été abordée, montrant que le comité européen de protection des données n'a pas pris position sur certains points. De tels textes doivent être compatibles avec une finalité d'usage.

Or nos concurrents européens, à savoir les Britanniques, usent de cette pratique du « bac à sable », avec pas moins de 700 personnes pour assurer la régulation. C'est pourquoi la règlementation européenne présentera un intérêt, à condition de ne pas trop restreindre, et de laisser une place à l'innovation et à la nouveauté, afin que nos acteurs disposent de deux à trois ans pour expérimenter. Il serait dommageable de se lancer avec un handicap dans une course, dans laquelle nos concurrents sont pleinement libres d'agir.

M. Julien Chiaroni. Parmi les sujets que nous n'avons que peu abordés, il y a, en premier lieu, la combinaison des sujets d'Intelligence artificielle et des autres sujets numériques, comme le *cloud* ou le *computing*, sans lesquels il n'existe pas d'apprentissage, ou encore la microélectronique. Le virage est opéré en direction du *edge* et nous aurons besoin d'architectures matérielles et logicielles performantes afin de développer des produits et services.

En second lieu, le déploiement des plateformes présente un coût relativement marginal. En ce sens, il serait souvent plus intéressant d'initier des projets globaux, de tailles plus

importantes, avec des investissements à proportions égales, que de multiplier les petits projets visant à tester des applications. En effet, la généricité offre l'atout de l'élargissement du *business*. En résumé, une intervention publique en la matière pourrait être intéressante, du fait des coûts marginaux faibles et de la capacité d'investissement.

M. Philippe Latombe, rapporteur. La pénurie des semi-conducteurs ralentira-t-elle le développement des programmes et le déploiement des technologies à l'échelle des objets ?

M. Julien Chiaroni. Un impact très fort se fait sentir, notamment au sein de la filière automobile, qui compte de nombreux microcontrôleurs, dont la conséquence est une baisse des capacités de production.

À l'échelle de l'Intelligence artificielle, la maîtrise des semi-conducteurs constitue un élément important de la chaîne des valeurs, puisqu'une compétition existe déjà à cet égard. Par exemple, Nvidia propose des architectures matérielles avec son GPU. De tels acteurs ont l'intention d'entrer dans des marchés comme l'autonomie des véhicules, et ainsi concurrencer les intégrateurs français ou européens du secteur de l'automobile, alors que ces pans de l'activité sont historiquement pris en charge par des acteurs des rang 1 ou rang 2. À ce titre, une véritable transformation de la chaîne industrielle pourrait s'opérer, d'où la nécessité d'adopter une vision globale de l'empilement, allant du semi-conducteur au *cloud*, en passant par l'Intelligence artificielle. Le chevauchement des domaines se fait de plus en plus important, et cette tendance ne fera que s'accroître.

M. Philippe Latombe, rapporteur. L'Europe devrait-elle réinvestir dans la production des semi-conducteurs et créer ses propres fonderies ? La pénurie n'est-elle pas plutôt ponctuelle et amenée à se résorber avec les investissements opérés par Intel à hauteur de 20 milliards de dollars sur deux ans, ou du leader taïwanais TMSC pour 100 milliards en trois ans ? Est-il nécessaire d'investir, ou bien ne pouvons-nous pas plutôt recourir à différents acteurs à travers le monde ?

M. Julien Chiaroni. Premièrement, vous mentionnez les fonderies, les fabrications de composants électroniques, mais la chaîne de valeur du semi-conducteur s'avère bien plus étendue. Le détail de l'empilement inclut les fondeurs, les IDM, mais aussi les EDA – acteurs du design dont la majorité se trouve aux États-Unis – et donc un ensemble complet à maîtriser, depuis le silicium jusqu'au composant final.

Deuxièmement, sur le fait d'investir dans le semi-conducteur, je dois d'abord préciser que je pourrais manquer d'objectivité, puisque j'ai travaillé dans le domaine. Pour autant, je considère qu'il faut investir, car dans le semi-conducteur réside un fort élément de souveraineté. À propos de TSMC, j'ajoute tout de même qu'il s'agit du plus grand investissement au monde dans le domaine des technologies avancées.

Troisièmement, déterminer si l'Europe doit se doter de fonderies demanderait une discussion plus spécifique mais à mon sens, elle doit investir dans des capacités pour cette filière.

M. Philippe Latombe, rapporteur. À propos des semi-conducteurs, mon intervention concernait bien l'ensemble de la filière, mais je n'y mentionnais que la fonderie car le Commissaire européen, M. Thierry Breton, annonçait vouloir recréer une fonderie européenne.

M. Renaud Vedel. Pour ma part, je ne suis pas un spécialiste du domaine mais je rappelle qu'il existait un projet européen d'intérêt commun, auquel les annonces de la Commission européenne du 21 avril laissent présager un deuxième volet d'importance.

Plusieurs acteurs travaillent déjà à faire le lien entre le calcul, les processeurs, les algorithmes et les logiciels, afin de créer une émulation et acquérir un statut d'envergure.

J'ajoute qu'il convient bien de raisonner du point de vue européen, puisque les Pays-Bas hébergent par exemple l'acteur de référence internationale pour les machines de fabrication. De même, les pays nordiques comptent en leur sein de nombreux experts. Additionnées à l'échelle européenne, ces capacités et compétences peuvent faire la différence à l'échelle mondiale.

Enfin, pour revenir à votre question initiale visant à définir la souveraineté, à mon sens, la souveraineté et l'autonomie stratégique ne consistent pas à maîtriser tous les éléments d'un ensemble mais plutôt à posséder des forces relatives par l'intermédiaire de certains maillons, afin de négocier d'égal à égal et de disposer d'une capacité de rétorsion, dans le cas où un acteur abuserait de son pouvoir de marché.

M. Julien Chiaroni. Nous mentionnions les importants investissements mondiaux dans le semi-conducteur, mais il ne faut oublier les milliards de dollars investis dans le secteur de l'IA, comme ceux réalisés par Palantir. Certes, les investissements dans l'Intelligence artificielle sont inférieurs à ceux du semi-conducteur, mais la compétition coûte malgré tout très cher. À mon sens, l'articulation du semi-conducteur et de l'Intelligence artificielle est fondamentale pour l'avenir.

L'audition s'achève à dix heures cinquante.

Audition commune, ouverte à la presse, de Mme Françoise Mercadal-Delasalles, co-présidente du conseil national du numérique et directrice générale du Crédit du Nord, et de M. Gilles Babinet, co-président du conseil national du numérique et *digital champion* auprès de la Commission européenne
(6 mai 2021)

Présidence de M. Philippe Latombe, rapporteur.

M. Philippe Latombe, président et rapporteur. Nous avons le plaisir d'auditionner Mme Françoise Mercadal-Delassales, directrice générale du Crédit du Nord et co-présidente du conseil national du numérique (CNNUM) et M. Gilles Babinet, également co-président du CNNUM et *digital champion* auprès de la Commission européenne.

Le CNNUM est une commission consultative indépendante, créée en 2011, chargée de conduire une réflexion ouverte sur la relation des humains au numérique. Son collège pluridisciplinaire se compose de dix-sept membres nommés pour deux ans par le Premier ministre, ainsi que de quatre parlementaires nommés par les présidents de l'Assemblée nationale et du Sénat. Le CNNUM est placé auprès du secrétaire d'État chargé de la transition du numérique et des communications électroniques.

Le CNNUM ne s'est pas encore saisi du sujet de la souveraineté numérique dans sa mandature actuelle, puisque ses membres ont été renouvelés au début de 2021. Nous vous remercions tous les deux pour cet échange qui ne préjugera évidemment pas du contenu de vos travaux à venir.

A titre liminaire, je souhaite vous interroger sur trois points.

Premièrement, quelle est votre approche de la souveraineté numérique et comment la définissez-vous ? Cette question est récurrente au cours de nos auditions, du fait de la grande diversité d'approches à cet égard. Comment jugez-vous la montée en puissance de la notion de souveraineté numérique dans le débat public ? Enfin, quel regard portez-vous sur le rôle qu'a joué le numérique durant la crise sanitaire, par exemple avec l'application TousAntiCovid ou l'éventualité d'un pass sanitaire ?

Deuxièmement, au cours des auditions, nous avons relevé que le fait pour l'État de rester souverain dans le numérique implique, à la fois, de conserver une indépendance vis-à-vis des choix technologiques et de réguler l'activité des acteurs du numérique. De quelle manière peuvent cohabiter les trois rouages de la souveraineté numérique, à savoir l'État, les entreprises et les citoyens ? Quel jugement portez-vous sur les initiatives européennes visant à réguler le service numérique, le marché de la donnée ou encore l'Intelligence artificielle (IA) ?

Troisièmement, je souhaite vous entendre au sujet du développement d'une culture du numérique dans la société. Quel est selon vous le degré d'intention des entreprises, même non spécialisées, à s'approprier la matière du numérique ? Comment jugez-vous la capacité à former les plus jeunes au numérique, en France comme en Europe ?

Mme Françoise Mercadal-Delassales, directrice générale du Crédit du Nord et co-présidente du CNNUM. Le CNNUM n'a pas encore abordé le sujet de la souveraineté numérique. Avant de répondre, je souhaite préciser les missions et le fonctionnement du

CNNUM, tout en montrant comment les sujets que vous introduisez sont traités et quel est notre niveau de réflexion.

Depuis une quinzaine d'années, les membres qui composent actuellement le CNNUM participent au déploiement du numérique dans leurs entreprises respectives. Comme au sein de l'État, les outils numériques y ont été déployés très rapidement, sur la base de ce qu'a observé et conseillé le CNNUM.

Pour cette période de deux ans, nous souhaitons faire un « pas de côté » dans cette course effrénée au déploiement du numérique, alors que nous avons plongé dans la grande transition anthropologique – pour citer Michel Serres – qui modifie considérablement nos comportements individuels, sociaux et économiques. Nous chercherons à déterminer les impacts de cette grande transition sur les humains et le fonctionnement du monde.

Je vous avertis d'ores et déjà que les productions et informations que le CNNUM diffusera ne répondront pas frontalement au fait de déterminer ce qu'est la souveraineté numérique et sur la manière de réguler les plateformes. L'État dispose déjà d'experts tout à fait à même de mener ces réflexions.

Le collège du CNNUM se compose de quatre parlementaires et dix-sept membres, qu'ils soient philosophes, sociologues, anthropologues, psychologues, économistes, journalistes, dirigeants d'entreprise, juristes, linguistes ou informaticiens. Cette composition vise à modeler une pensée interdisciplinaire sur cinq grands thèmes, à savoir la relation des humains au savoir, la relation à la vérité, la relation aux institutions – où la souveraineté pourrait être abordée sous un angle sociologique ou philosophique – la relation au collectif social et la relation avec l'ensemble du vivant.

À mon sens, cet échange, ce matin, autour de la souveraineté, pourrait être fidèle à la démarche du « pas de côté » voulue par le CNNUM et chercher à préciser comment être souverain de soi-même au cœur de la civilisation numérique, tout en en restant acteur et en donnant au citoyen la capacité d'opérer ses choix propres, alors même que tout un chacun est assailli par les informations et les outils que le monde actuel impose. En résumé, la question de la souveraineté numérique ne se limite pas à l'État, mais tient aussi au fait de savoir comment être souverain de soi-même.

M. Gilles Babinet, *digital champion* auprès de la Commission européenne et co-président du CNNUM. Je souscris pleinement à ce propos liminaire et propose donc de passer aux questions de la mission d'information.

M. Philippe Latombe, rapporteur. Comment donner une perspective commune aux trois entités de la souveraineté numérique, c'est-à-dire l'État, les entreprises et les citoyens, qui sont aussi des usagers ?

M. Gilles Babinet. En écho aux propos de Mme Françoise Mercadal-Delassales, j'affirme que nous devons recréer un projet collectif et politique. Cette question a d'ailleurs nourri l'orientation des travaux du CNNUM. Nous sommes tous conscients des menaces géopolitiques que peut véhiculer le numérique et, en ce sens, nous devons faire des choix. En effet, les natures des projets numériques diffèrent dans le monde, avec un axe économique aux États-Unis, une vision militaire en Israël et une visée expansionniste pour la Chine. L'Europe cherche, quant à elle, à développer un projet numérique davantage inclusif, bien que ce point demande à être détaillé.

Pour répondre à votre question à propos de la souveraineté, il y a quatre ans, j'ai rédigé à ce sujet un dossier pour l'Institut Montaigne. Aussi, le CNNUM ne s'étant pas encore positionné sur ce point, je propose de m'exprimer à titre personnel.

D'une part, il existe, à mon sens, un enjeu de court terme, avec la proportionnalité de l'usage du numérique et la mise en balance des avantages et des risques à y recourir. Dans votre propos liminaire, vous évoquiez les sujets de santé, comme le Health Data Hub, et je me déclare en désaccord avec les positions communément adoptées, par exemple, par la commission nationale de l'informatique et des libertés (CNIL) et le Conseil d'État. En effet, le risque doit être pesé, mais tout un chacun doit pouvoir utiliser les outils appartenant à l'*hyperscale*. Cependant, les données pourraient être utilisées, y compris à des fins de renseignement, et ces problèmes doivent être abordés.

D'autre part, il existe les enjeux de long terme, imposant de posséder une vision forte du numérique, pour la politique industrielle, la cybersécurité, les microprocesseurs ou encore les enjeux d'éducation. La Chine est un pays dont nous parlons peu en la matière, mais elle mène une politique spécifique au numérique pour l'éducation, notamment pour l'IA, employant des logiques de « silo » difficiles à mettre en place. À l'inverse, il est complexe de percevoir les effets consécutifs aux déclarations de nos autorités en la matière. L'organisation structurelle de nos institutions est-elle compatible avec le monde numérique ? Poser la question est commencer d'y répondre.

M. Philippe Latombe, rapporteur. L'Union européenne cherche actuellement à règlementer le numérique, s'étant aperçue, après le Règlement général sur la protection des sonnées (RGPD), qu'il fallait réguler davantage comme avec les projets *Digital Services Act (DSA)* et *Digital Market Act (DMA).* Cette méthode est-elle efficace ou devrions-nous plutôt entrer dans la compétition du numérique pour imposer nos standards sur le marché, sans passer par la règlementation ?

M. Gilles Babinet. Nombreux sont ceux, et j'en fais partie comme le Commissaire européen, M. Thierry Breton, à constater que les outils institutionnels européens sont insuffisants. Ce problème s'accentue dès lors qu'il faut parvenir à un consensus recueillant l'unanimité pour mettre en œuvre des budgets européens d'investissement.

Dans le plan de relance, je déplore que des affectations de budget préexistantes à la crise ont été remises en cause en matière d'innovation ou de numérique.

Je m'exprime encore une fois à titre personnel, pour affirmer que nous devons nous doter d'un outil de défense européen, indépendant de l'OTAN, comprenant une forte part cyber. Ce projet n'a pas encore pris corps. Pour le reste, nous devons adopter une logique applicative de recherche et de transfert, comme le fait l'agence américaine *Defense Advanced Research Projects Agency* (DARPA). Comme tout le monde, j'ai entendu parler d'un budget de dix milliards d'euros en faveur du numérique, portant sur une durée inconnue, dont il faudrait dans tous les cas que la gouvernance soit dotée d'agilité.

En somme, la logique européenne devrait se tisser autour d'axes tels que ceux définis par le processus de Bologne. De même, l'Union européenne devrait consacrer une part importante du plan de relance au programme Erasmus, l'un de ceux ayant connu le plus de succès, et tendre à un Erasmus digital. Une telle dynamique ferait probablement montre de son efficacité, et produirait un effet très positif du point de vue du sentiment européen.

Mme Françoise Mercadal-Delassales. La nécessité de réguler est une évidence absolue, mais réguler ne sera jamais suffisant, car les modes de régulation traditionnels, hérités

du XIXe siècle, n'interviennent plus dans un monde pyramidal, et se heurtent à des résistances sociales et sociétales.

Il convient de réaliser que nous serons bientôt huit milliards d'individus sur la planète, ayant tous l'information à portée de main. L'absence de traitement de l'information peut avoir des effets délétères mais, à l'inverse, il est possible de produire des effets fabuleux, en se dotant effectivement d'une vision politique dans l'utilisation de ces outils, à des fins collectives.

En marge de la règlementation, il nous semble nécessaire de développer une culture du numérique. Il y a longtemps maintenant que les entreprises en France, y compris les PME, se sont lancées dans la compétition du numérique, mais nous n'y avançons qu'à l'aveugle, car les individus qui mettent en place ces systèmes, au sein des entreprises, n'ont pas reçu d'éducation à l'école, quant à l'influence de ces outils sur l'humanité. À titre personnel, je considère que cette éducation numérique manque au secteur public comme au secteur privé, pour opérer les choix allant dans le sens de l'intérêt général.

La culture du numérique constitue un enjeu politique et social majeur et elle inclut la compréhension ou l'apprentissage des aspects techniques de l'outil, des algorithmes, de la signification d'une donnée, et du point de savoir où ces données sont stockées, ou encore du fonctionnement du *pagerank* de Google.

D'un point de vue politique et civique, il est important de comprendre les enjeux de la collecte des données, en matière de surveillance, de libertés et de protection de la vie privée. L'aspect économique s'ajoute à ces enjeux, mais également un aspect psychosocial avec l'impact des écrans sur le développement cérébral, le changement des rapports intergénérationnels, la communication et le collectif. Nous pouvons regretter que l'histoire des sciences ne soit pas enseignée à l'école, car ne pas comprendre comment une révolution technologique transforme l'humanité mène à être utilisé, soi-même, par les outils.

Nous comprenons cette course au développement du numérique et que l'Europe, face aux États-Unis, à la Chine, se trouve saisie d'un sentiment d'urgence l'incitant à réguler. En ce sens, un malaise profond se déploie dans notre société, et un décalage très important apparaît entre la vitesse de développement de la société du numérique et la compréhension que nous en avons.

Peut-être ces sujets s'éloignent-ils du thème de la mission d'information, mais pour avoir évolué au sein d'une grande entreprise bancaire dix ans durant, en tant que dirigeante des services informatiques, je sais que les choix technologiques que nous opérions étaient guidés par l'efficacité économique et l'immédiateté. Cette efficacité était évidemment une réponse à la puissance des *majors* états-uniennes, auxquelles, demain, s'ajouteront des *majors* chinoises. Mais j'affirme que dépendre complètement des outils fabriqués par ces acteurs ne traduirait qu'une vision de court de terme de notre part, quant à la viabilité de nos entreprises. Il est nécessaire d'amener les citoyens à vivre la transition digitale de manière positive, en leur donnant les moyens de la comprendre. Atteindre cet état de compréhension relève de la souveraineté individuelle et collective, et amène à prendre des décisions différentes, selon qu'il s'agit d'un acteur public ou privé.

M. Philippe Latombe, rapporteur. Vos développements correspondent tout à fait au volet de la formation, enjeu de souveraineté, de notre mission et il est bon que vous l'ayez abordé.

À propos de la culture du numérique, le thème de la fracture numérique apparaît récurrent. Cette fracture est-elle désormais autant sociologique que physique, c'est-à-dire que les territoires ruraux et éloignés des réseaux à haut débit ne sont plus les seuls à être concernés par le problème ? Je suis bien conscient que votre mandature du CNNUM n'a pas encore travaillé sur ces sujets, mais, selon vous, comment pourrions-nous amener ces citoyens à ne plus être effrayés ou subir la transformation numérique ? L'exemple de la digitalisation des services publics peut être pertinent.

M. Gilles Babinet. J'appuie les propos de Mme Françoise Mercadal-Delassales et tiens à signaler que la création d'un imaginaire collectif est déterminante pour effectuer la transition du numérique. C'est notamment ce qui ressort de l'ouvrage *The Code* de Margaret O'Mara à propos de l'émergence de la *Silicon Valley* aux États-Unis. L'environnement s'y est imprégné de littérature, de cursus universitaires, ayant amené à faire émerger la puissance de cet écosystème. En somme, nous devons bâtir une culture qui nous soit propre, et non pas importée, afin d'être maîtres de notre destin.

Concernant la fracture numérique, je me souviens d'un débat à propos des populations migrantes, au cours duquel il était expliqué que la capacité d'intégration dépendait du fait de posséder un référentiel culturel permettant d'avoir un sentiment d'appartenance à l'ensemble. Au même titre que ces mouvements dans l'espace, l'accélération technologique a produit un sentiment de déracinement dans le temps. C'est alors qu'intervient le besoin de posséder une culture collective nous portant au changement, plutôt que de nous en rendre victime.

À de nombreuses reprises, j'ai encore été surpris qu'il faille convaincre des journalistes, chercheurs et politiciens du fait que mettre en œuvre la technologie ne revient pas à se soumettre à des modèles importés. Nous pouvons imprimer de fortes inflexions, tant sur la technologie pure qu'au sein des humanités numériques et faire prévaloir nos façons de penser ou de réguler la technologie.

Mme Françoise Mercadal-Delassales. La fracture numérique n'est pas seulement territoriale, d'autant que les pouvoirs publics, centraux ou locaux, déploient des dispositifs afin d'atteindre les populations les plus isolées.

À mon sens, la fracture numérique est essentiellement sociale. Le fait que les outils en soient massivement utilisés, et par toutes les tranches d'âge, amène à reproduire, tant le négatif que le positif de nos vies hors du numérique. L'outil numérique ne fait alors qu'accentuer les tendances préexistantes. Au sein du CNNUM, nous comptons Mme Dominique Pasquier, sociologue, dont les travaux démontrent que l'usage de l'outil digital diffère d'une classe sociale à l'autre. Quand les enfants des cadres l'utiliseront afin d'apprendre et se renforcer, les enfants de classes plus défavorisées en useront d'une manière non enrichissante, voire appauvrissante et amenant à désapprendre. Les pouvoirs publics se doivent d'être extrêmement vigilants à cet égard.

Dès l'école primaire, l'enfant doit commencer à comprendre la portée de l'utilisation de l'outil digital, et cet apprentissage importe autant que le fait de lire, écrire ou compter. Dans le cas contraire, la société ne s'en fragmentera que davantage, exposée en permanence aux bulles des réseaux, qui nous diviseront. Cet apprentissage correspond au travail sur la vérité qu'ambitionne de mener le CNNUM.

Dans la mesure où les outils numériques existent et que nous devons composer avec eux, le CNNUM souhaite suggérer des pistes afin de lutter contre leurs effets négatifs. Par exemple, il s'agirait de déterminer comment utiliser l'IA pour nous protéger des bulles informationnelles et des *fake news*. À ce sujet, le CNRS compte en son sein l'institut des

systèmes complexes, qui a mis en place un *politoscope* visant, par exemple en période d'élections, à apurer l'information des manipulations malveillantes. En d'autres termes, il faut utiliser la technologie pour protéger notre capacité de choix, c'est-à-dire notre souveraineté.

Cette transition numérique équivaut à l'invention des premiers outils ou à la découverte de l'atome. Pour ma part, j'ai été pionnière et chantre du digital au moment où nos entreprises se devaient d'effectuer cette évolution. Pour autant, l'année écoulée de crise sanitaire nous a montré que seuls, face à nos ordinateurs, nous avions besoin de contact social, d'échanger et d'être ensemble. De ce point de vue, l'école doit jouer un rôle fondamental.

Le CNNUM désire contribuer à ce débat et fournir des éléments et ressources afin d'affiner la pensée au sujet du numérique. D'ailleurs, au-delà de nos productions écrites, nous avons commencé d'interviewer des chercheurs et penseurs sur notre plateforme en vue d'amener à réfléchir et pourquoi pas, s'il le faut, susciter des controverses constructives.

M. Philippe Latombe, rapporteur. La crise sanitaire a eu pour conséquence de lever le voile sur de nombreux effets, positifs comme négatifs, du numérique. L'école, à titre d'illustration, s'est beaucoup numérisée du fait des circonstances. Comment mettez-vous en balance la nécessité d'enseigner le numérique à l'école, et le fait que l'école a été dispensée à distance pendant la période ? Quelles conclusions tirez-vous de cette phase pour la dimension éducative ?

M. Gilles Babinet. L'école est un bon exemple d'une institution lourde, qui a « subi » le numérique du fait, d'une part, de son impréparation, et, d'autre part, d'une opportunité non saisie de repenser le projet pédagogique. Je n'ai pas connaissance d'un débat autour du protocole pédagogique, alors même qu'injecter le numérique de cette manière aurait présenté des vertus éducatives, mais également celle de permettre la réappropriation de la technologie, que je mentionnais plus tôt. L'une des dernières enquêtes PISA montre que la France est l'un des pays ayant le plus faible taux de mobilité sociale par le biais de l'éducation. Je considère vraiment dommageable que nous n'ayons pas mené d'action en vue de repenser la dimension pédagogique.

En résumé, la crise du Covid-19 n'a fait qu'exacerber les disparités sociales, puisque selon les foyers il était, ou non, possible de s'isoler chez soi ou d'accéder aux supports et plateformes adéquats. L'analyse post-crise pourrait être sévère à ce titre, et elle souligne une difficulté à prendre du recul et à considérer le numérique autrement que comme un outil strictement technique.

Mme Françoise Mercadal-Delassales. Le système scolaire français recueille en effet de nombreuses critiques, mais je ne souhaite pas ajouter de commentaire à ce sujet, même si d'autres pays ont su mieux tirer parti de la crise de ce point de vue.

Le CNNUM, par son groupe de travail portant sur le savoir, introduit l'idée de la complémentarité entre l'enseignement physique dit classique, et l'utilisation des outils numériques. Nous avons récemment interviewé Mme Daphné Bavelier, neuroscientifique, qui étudie l'influence des jeux vidéo. Elle met en avant le fait que les jeux vidéo ou certains supports peuvent permettre un renouveau du plaisir d'apprendre pour certains élèves ne pouvant plus être ramenés au système scolaire classique. De même, l'outil digital pourrait être utilisé face à la dyslexie et aux troubles de l'attention.

Je rejoins M. Gilles Babinet sur le fait que, tant que les enseignants n'auront pas également fait un « pas de côté » dans leur cheminement à propos des outils numériques, et qu'ils n'auront pas abandonné une vision manichéenne pour une approche rationnelle du

numérique, le débat demeurera stérile. Nous maintenons qu'il faut jouer de cette complémentarité entre les deux modèles d'éducation.

D'ailleurs, l'un des membres du CNNUM, M. Alexandre Lacroix, philosophe et directeur de la revue *Philosophie magazine*, évoquait avec nous la nécessité de faire jouer la pensée complexe, prenant en compte les oppositions comme le *yin* et le *yang*, le blanc et le noir. Il convient de dépasser le bien et le mal vis-à-vis de l'usage du numérique et de se pencher sur l'usage que chacun en fait.

M. Philippe Latombe, rapporteur. Le monde du numérique est encore majoritairement masculin. L'outil numérique peut-il promouvoir la diversité des sexes ?

Mme Françoise Mercadal-Delassales. Tout dépendra de l'usage qui sera fait de l'outil numérique.

M. Philippe Latombe, rapporteur. Que devons-nous faire pour que le numérique produise des effets vertueux, et non pas destructeurs, au sein de la société ? Comment pouvons-nous mobiliser les citoyens, autrement que par l'action publique ?

M. Gilles Babinet. Les débuts d'Internet promettaient des effets vertueux, par exemple via l'*open source*, l'*open data* ou des plateformes comme Wikipédia avec une massification du savoir. Puis les méta-plateformes sont apparues, débordant les vues préexistantes.

Lors de chaque élection présidentielle, je déplore le fait que, dans des échanges avec les personnalités politiques, lorsque nous mentionnons l'existence d'une révolution technologique, le scepticisme prévale et que l'idée selon laquelle nous vivons une accélération notable ne soit pas comprise. Le numérique permettrait pourtant de refonder un projet collectif, et de travailler sur des enjeux d'« encapacitation » et d'éducation.

De même, je n'apprécie pas du tout le terme de dématérialisation, qui donne la sensation qu'il ne s'agit que de transposer les outils d'avant dans une version digitalisée. Sans repenser les pratiques sociales et économiques, nous n'adoptons qu'une vision très partielle de la situation.

De nombreux exemples de projets politiques existent, à l'international avec les écrits de M. Salman Kahn ou l'université de Bologne, et au niveau national avec les expérimentations en réseau d'éducation prioritaire (REP) que mène le mouvement *Agir pour l'école*. Intégrer le numérique ne constitue pas une lubie, mais bien une idée concrète pouvant déboucher sur des succès. Cependant, même si j'interviens à ce sujet depuis des années et dans différentes sphères, jusqu'à la sphère politique, je constate qu'il est encore difficile de faire « bouger les lignes ».

C'est la raison pour laquelle le CNNUM adopte la stratégie du « pas de côté », pour poser des questions de fond et interroger le sens que nous voulons donner à la société, car nous n'en sommes pas encore à la situation où un véritable projet collectif émerge et grandit de manière exponentielle.

M. Philippe Latombe, rapporteur. Comment percevez-vous le rôle du CNNUM dans la situation globale que nous décrivons ?

Mme Françoise Mercadal-Delassales. D'abord, le numérique ne doit pas être perçu comme un simple fait technique mais comme un fait social et total.

Ensuite, notre humble ambition consiste à donner matière à penser sur les grandes questions que pose le déploiement massif du numérique. Ces questions rejoignent celles que je mentionnais en début d'audition, sur lesquelles le CNNUM a l'intention de se pencher, et qui pourraient être amenées à évoluer.

Enfin, nous souhaitons faire du CNNUM un lieu riche en ressources, où échanger des points de vue et construire une pensée collective. Pour y parvenir, nous souhaitons partager la pensée que nous produirons sur la plateforme du CNNUM et au-delà, éventuellement publier un ouvrage pour porter notre vision. Dans cette optique, nous espérons susciter l'intérêt des médias, des parlementaires et nous envisageons également de nous rendre dans les régions pour présenter nos réflexions, et jusque dans les écoles. En conclusion, notre intention est d'allumer une mèche dans la réflexion publique, en commençant par pointer le fait que le numérique ne doit pas se limiter à l'usage d'un outil.

M. Philippe Latombe, rapporteur. De vos développements, nous comprenons que les chantiers que vous listez porteront sur des réflexions longues. Cette stratégie du « pas de côté » vous mènera-t-elle à participer à des débats pouvant survenir ponctuellement, comme la reconnaissance faciale dans l'espace public, ou bien vous abstiendrez-vous d'intervenir ?

Mme Françoise Mercadal-Delassales. Dans son agenda, le CNNUM n'a pas prévu de répondre ponctuellement aux sujets mais, dans la mesure où nous sommes au service de l'État, si le gouvernement nous le demande, nous aborderons certains sujets en particulier.

Aussi, bien que nous abordions des réflexions de fond, nous avons l'intention de « produire de la pensée » de manière régulière et continue. En ce sens, faire part de nos travaux à l'orée d'une élection présidentielle ou de la présidence française de l'Union européenne nous apparaît potentiellement très profitable.

M. Philippe Latombe, rapporteur. Considérant la trajectoire actuelle du numérique, quelle place lui attribuez-vous à moyen et long terme ?

M. Gilles Babinet. Cette question est très ouverte. Toutefois, je considère que le numérique aura une place équivalente, si ce n'est supérieure, à celle de l'électricité. Michel Serres parlait à juste titre d'une révolution anthropologique, qui nous amènera à penser différemment, à avoir d'autres connexions avec nos amis, nos familles, la transmission aux enfants. Le numérique relève d'un modèle productif et d'enjeux de souveraineté. En réalité, cette révolution totale me semble être de première importance et unique.

Michel Serres déclarait également que pour trouver trace d'un événement modifiant notre psyché autant que le fait le numérique, il fallait remonter à la civilisation de Sumer et le passage d'un vocabulaire de quelques centaines à plusieurs milliers de mots. Le numérique modifiera notre rapport à la connaissance, davantage encore que l'imprimerie de Johannes Gutenberg.

Mme Françoise Mercadal-Delassales. Parler de moyen ou de long terme est dépassé, puisque le numérique produit déjà pleinement ses effets et l'entrée dans cette nouvelle ère a eu lieu, peut-être même si rapidement que nous ne nous en sommes pas tout à fait rendu compte. L'année écoulée de crise sanitaire nous a peut-être ouvert les yeux sur cette fulgurance, mais les effets surviennent déjà et nous devons nous emparer des réflexions et les porter dans le débat public.

M. Philippe Latombe, rapporteur. Quel usage de l'IA projetez-vous à l'échelle de la société ? Est-ce que le CNNUM interviendra sur des débats, comme celui, apparu il y a quelques années, d'une personnalité juridique de l'IA ?

M. Gilles Babinet. Si nous possédions une véritable culture collective de l'IA, ce débat serait déjà dépassé. Pour le reste, j'avais suivi cette question et m'en étais agacé, car selon moi, doter l'IA d'une personnalité juridique n'est qu'un débat propre aux juristes, faisant état d'un transfert. Cette réflexion révèle en fait une peur du potentiel de la technologie, et était d'ailleurs portée par des futurologues dystopiques n'ayant jamais pris la peine de pratiquer le code.

Pour autant, le débat sur l'IA est passionnant et nous cherchons les points d'appui pour le généraliser.

Mme Françoise Mercadal-Delassales. Pour ma part, je ne vois qu'une déresponsabilisation totale des humains dans ce débat, comme si nous parlions des machines envisagées par Aldous Huxley ou dans le film Matrix. Alors qu'en réalité, derrière chaque machine, chaque algorithme, chaque IA de nos entreprises, il existe des hommes qui cherchent à s'enrichir. Les robots ne peuvent pas être tenus responsables de nos actions et de l'univers que nous avons fabriqué de bout en bout, quand bien même certaines IA mimeraient approximativement nos comportements.

En réponse, le sujet de l'IA fera partie des réflexions du CNNUM, mais au même degré et suivant la même méthodologie que les autres sujets que nous envisageons d'aborder.

M. Philippe Latombe, rapporteur. Je citais l'exemple de l'IA car il revêt une forte dimension sociologique et psychologique, jusque dans les biais qu'il génère et les reflets de la diversité des sexes, par exemple entre les manières féminines et masculines de penser. Ce sujet fait-il partie des réflexions que le CNNUM souhaite amener dans le débat public ?

Mme Françoise Mercadal-Delassales. L'institut des systèmes complexes, dépendant du CNRS, que je mentionnais plus tôt, travaille sur ces sujets.

Concernant le CNNUM, notre premier livret évoquera la manière d'utiliser l'IA, non pas contre elle-même, mais afin de débusquer en son sein les biais de genre, les biais sociaux ou éducatifs.

Je répète que nous sommes absolument responsables des systèmes que nous créons, et des algorithmes que nous bâtissons. Parfois, je crains que certains ne cherchent à se cacher derrière les machines pour agir. Mais ce point nous fait revenir au projet politique et social.

M. Philippe Latombe, rapporteur. Ne pensez-vous pas justement qu'il existe, comme il y en a eu un avec le *green washing*, un phénomène de *« sovereignty washing »* sans que le terme de souveraineté n'ait véritablement été défini, et qu'il soit ensuite utilisé comme slogan ? Au-delà du numérique, le terme de souveraineté revient dans de nombreux discours. Aussi, comment le définiriez-vous ?

M. Gilles Babinet. Je vous remercie pour cette question à laquelle j'apprécie répondre car la souveraineté se trouve souvent associée à des pensées antimondialistes ou anti-atlantistes.

À mon sens, la souveraineté ne peut découler que d'un projet politique, et passe désormais par la technologie. Dans ce monde où l'ubiquité numérique remet partiellement en

cause les frontières géographiques, nous devons définir ce qui nous lie et nous permet d'exister ensemble. Pour autant, il est difficile de parvenir à une définition claire, y compris dans les discours politiques, dont le contenu est souvent incomplet ou discutable, car mal précisé vis-à-vis de la révolution technologique que nous traversons.

Mme Françoise Mercadal-Delassales. Pour ma part, je lie les sujets de la souveraineté et de la durabilité. La souveraineté tient dans notre désir de faire survivre des valeurs, qu'à certains égards il faudrait encore définir. Un parallèle peut être effectué avec une entreprise qui, par les décisions qu'elle prend, cherche à faire perdurer ses valeurs managériales, éthiques et, de manière générale, ses codes.

Il semble évident qu'un acteur économique qui sous-traite une partie de ses activités vitales à d'autres entreprises ou entités étatiques se place dans une situation de dépendance vis-à-vis de ces dernières. Je considère que la souveraineté relève de la limite en-dessous de laquelle un acteur ne confie pas à d'autres les éléments vitaux qui le caractérise. Or, désormais, le numérique et la donnée sont devenus des éléments vitaux du corps social que nous formons. Dans le domaine bancaire, nous avons pour habitude de conseiller de diversifier les placements et de même, un acteur du numérique doit diversifier les entreprises ou entités étatiques auxquelles il confie ses éléments vitaux.

Le paramètre qui me semble fondamental est de conserver la capacité, l'intelligence et la compréhension des systèmes que nous utilisons, pour préserver la possibilité de fabriquer nous-mêmes par la suite. Si nous perdions cette faculté de compréhension, nous nous exposerions aux caprices d'entités ne partageant pas nos valeurs et nos façons de penser.

En conclusion, la souveraineté est un terme dépassant la matière économique, qui doit être combiné avec la durabilité et la survie de nos valeurs.

M. Philippe Latombe, rapporteur. Voyez-vous, dans l'émergence de la notion de souveraineté au sein du débat public, une opportunité de développer la pensée et la réflexion, ou plutôt à l'inverse, un faux-semblant ne pouvant que parasiter les échanges et réflexions que vous pourriez formuler dans le domaine numérique ?

Mme Françoise Mercadal-Delassales. Nous sommes bien conscients des distorsions qui peuvent s'opérer dans les discours incluant la notion de souveraineté. Notre intention consiste à poursuivre nos réflexions, alimenter le débat et les controverses constructives avec des arguments de tous les horizons, afin de permettre aux citoyens de se forger leurs propres opinions.

M. Gilles Babinet. Quant à moi, je regrette qu'en France, le monde de la recherche ne fasse pas partie du débat public. Je compare cette situation à celles de pays que je connais bien également, comme les États-Unis ou le Royaume-Uni, l'Irlande et les pays scandinaves, où le débat public se nourrit des informations provenant du monde de la recherche.

J'estime qu'une démocratie en bonne santé inclut ses chercheurs dans le débat public. C'est d'ailleurs précisément ce que nous essayons de faire au sein du CNNUM, en ayant intégré des membres ayant un parcours académique. Rendre au monde de la recherche la part qui lui est due dans le débat public fait aussi partie du travail que le CNNUM a l'intention d'effectuer.

M. Philippe Latombe, rapporteur. J'entends que vous citiez des pays anglo-saxons mais, en Europe continentale, voyez-vous émerger des réflexions identiques à celles que vous ambitionnez pour le CNNUM ? Avez-vous des homologues en Europe ?

M. Gilles Babinet. Bien qu'ayant voyagé dans de nombreux pays d'Europe par le passé, je ne les connais pas tous. Pour autant, je sais que l'Allemagne s'appuie beaucoup sur la science dans ses prises de décision, portant la participation du corps scientifique aux institutions administratives et politique à un degré bien supérieur à celui qui est le nôtre en France. D'ailleurs, la chancelière, Mme Angela Merkel, est elle-même une scientifique et le rappelle régulièrement. Aussi, la crise sanitaire a illustré cet état de fait en Allemagne, où l'institut Robert Koch a fréquemment été associé aux décisions prises.

En Suisse, je connais l'excellence du domaine universitaire et son importante capacité à nourrir le débat public. De ce que je sais, la Pologne ou l'Autriche sont également dans la ligne de l'Allemagne et de la Suisse pour cette manière de procéder, incluant le monde des sciences.

La France, qui possède pourtant une grande culture et une grande histoire scientifiques, est en train de décrocher. Je ne peux pas utiliser un autre terme, car telle est la réalité des indicateurs. Des conséquences apparaissent sur le plan de la compétitivité, la qualité de la pensée et du débat. Une nouvelle fois, je considère qu'il faut replacer le travail scientifique et la recherche académique au centre du débat public.

M. Philippe Latombe, rapporteur. Reste-t-il des points que nous n'avons pas abordé au cours de cet échange ?

Mme Françoise Mercadal-Delassales. Nous avons développé de nombreux sujets et le travail du CNNUM ne fait que commencer.

M. Philippe Latombe, rapporteur. C'est la raison pour laquelle je vous posais la question, car le rapport de la mission d'information doit être remis d'ici un mois et demi. En ce sens, il est important que nous ayons l'ensemble de vos réflexions, afin de ne pas occulter des sujets d'importance.

M. Gilles Babinet. Je pense également être intervenu sur les éléments que nous souhaitions développer.

M. Philippe Latombe, rapporteur. Sachez que je lirai avec intérêt les écrits émanant du CNNUM.

Audition de M. le général de corps aérien Jean-François Ferlet, directeur du renseignement militaire (DRM) (ministère des armées)
(20 mai 2021)

Présidence de M. Jean-Luc Warsmann, président.

(Les propos tenus au cours de l'audition à huis clos n'ont pas fait l'objet d'un compte rendu.)

Audition de M. le général de division aérienne Didier Tisseyre, officier général commandant de la cyberdéfense (état-major des armées) (ministère des armées) et de l'ASC Sébastien bombal, chef du pôle stratégie
(21 mai 2021)

Présidence de M. Philippe Latombe, rapporteur.

(Les propos tenus au cours de l'audition à huis clos n'ont pas fait l'objet d'un compte rendu.)

Audition, ouverte à la presse, de M. Mehdi Gharsallah, conseiller stratégique pour le numérique auprès de la directrice de l'enseignement supérieur et de l'insertion professionnelle (ministère de l'enseignement supérieur, de la recherche et de l'innovation)
(25 mai 2021)

Présidence de M. Philippe Latombe, rapporteur.

M. Philippe Latombe, président et rapporteur. L'importance cruciale de la formation ressort fréquemment de nos auditions de différents acteurs du numérique, aussi bien des entreprises que des instituts de recherche ou l'agence nationale de la recherche. Nous n'avons pas manqué d'entendre le directeur général de l'enseignement scolaire du ministère de l'éducation nationale. Il convenait de porter une attention à l'autre extrémité de la chaîne en nous attachant à l'enseignement supérieur. Aussi avons-nous le plaisir d'auditionner ce matin M. Mehdi Gharsallah, conseiller stratégique pour le numérique auprès de la directrice générale de l'enseignement supérieur et de l'insertion professionnelle.

Rappelons que la direction générale de l'enseignement supérieur et de l'insertion professionnelle (DGESIP) élabore et met en œuvre la politique relative à l'ensemble des formations supérieures, initiales et tout au long de la vie, relevant du ministre en charge de l'enseignement supérieur. Elle veille à la mise en œuvre, par les établissements relevant de sa compétence, de leur mission d'orientation et d'insertion professionnelle. Elle exerce la tutelle des établissements publics relevant du ministre chargé de l'enseignement supérieur et élabore le cadre juridique de leur organisation et de leur fonctionnement. Elle répartit également les moyens entre ces établissements, à partir d'une analyse de leurs activités et de leurs performances. Elle fixe enfin le cadre national des formations et des niveaux de diplômes, et elle met en œuvre une politique active d'orientation et de préparation à l'insertion professionnelle. En outre, elle participe à la définition et à la mise en œuvre de la stratégie numérique pour l'enseignement supérieur, visant à utiliser le numérique comme levier de rénovation pédagogique afin d'accroître l'attractivité de l'enseignement supérieur français dans le monde et, en particulier, les pays francophones.

Je commencerai par vous poser une question devenue rituelle lors de nos auditions, procédant de la grande diversité des définitions données à la souveraineté numérique. Comment concevez-vous cette notion ? Comment l'enseignement supérieur tient-il compte des préoccupations qu'elle inspire ?

Un pays ne peut se prétendre souverain en matière numérique qu'à condition de susciter durablement le flux de talents indispensables pour lui assurer des compétences dans ce domaine en renouvellement constant. Je reprendrai l'image de la pyramide utilisée par le président-directeur général de l'institut national de recherche en informatique et en automatique (Inria) lors de son audition. Les élèves de l'enseignement secondaire intéressés par les sciences et technologies en forment la base. Nous les avons évoqués avec le directeur de l'enseignement scolaire. Quelle appréciation portez-vous sur ce vivier ? Comment garantir qu'un nombre suffisant de diplômés d'un master en mathématiques appliquées ou en informatique s'engagent dans la recherche, alors que les entreprises en pleine transformation numérique et donc, en demande de talents, s'évertuent à les attirer ? Comment, enfin, maintenir au sommet de la pyramide, pour y attirer des spécialistes de haut niveau, une puissance académique de taille à concurrencer, voire dépasser, celle des grands acteurs internationaux des nouvelles technologies, dont les moyens rivalisent désormais avec

l'excellence académique publique ? En somme, comment maintenir une telle pyramide en lui évitant de se déformer excessivement à moyen et long terme ?

Lors de son audition, l'agence nationale de la recherche a attiré notre attention sur le manque d'enseignants chercheurs en informatique et en mathématiques appliquées face à la demande croissante dans les domaines de l'Intelligence artificielle ou de l'informatique quantique. Partagez-vous ce constat ? Le cas échéant, quelles actions préconisez-vous pour y remédier ?

Mon deuxième point portera sur l'impact de la crise sanitaire sur l'enseignement supérieur. Le ministère avait déjà, auparavant, inscrit le numérique au cœur de son projet stratégique. Comment cette démarche a-t-elle permis d'accroître la résilience de l'enseignement supérieur face aux bouleversements liés au Covid, aussi bien en termes de production de contenus et de services numériques que d'accompagnement des enseignants à l'utilisation du numérique ? J'aimerais revenir sur le sujet particulièrement prégnant du recours au numérique dans l'enseignement supérieur en vue d'assurer une continuité pédagogique au bénéfice des étudiants.

Pour terminer mon propos liminaire, je souhaiterais prendre du champ afin d'évoquer la souveraineté numérique d'un point de vue comparatif. Comment notre enseignement supérieur se positionne-t-il par rapport à celui des pays voisins dans les domaines relatifs aux compétences numériques ? Comment le développement de formations en ligne peut-il renforcer la visibilité et l'attractivité de l'enseignement supérieur français afin de cibler les talents et de les attirer vers notre pays ?

M. Mehdi Gharsallah, conseiller stratégique pour le numérique auprès de la directrice de l'enseignement supérieur et de l'insertion professionnelle. Je vous approuve entièrement de poser de manière rituelle la question de ce que recouvre la notion de souveraineté, en particulier numérique.

Le concept de souveraineté fait aujourd'hui figure de paradigme. Son usage polysémique s'avère toutefois problématique. Le terme recouvre en effet des notions aussi différentes que le patriotisme économique, la sécurité informatique, la confiance ou encore l'indépendance.

Je la considère pour ma part comme l'ensemble des actions grâce auxquelles un État et une nation limitent leur dépendance vis-à-vis de puissances extérieures. Une souveraineté numérique française ou européenne devrait ainsi permettre à l'administration et aux citoyens d'utiliser des services numériques sans dépendre d'entreprises ou d'États étrangers, ou même d'organisations non gouvernementales.

Force est de constater que ce n'est pas le cas, comme le montre par exemple notre utilisation de la plateforme par le biais de laquelle nous échangeons. J'avoue que l'invitation que j'ai reçue à m'y connecter m'a fait sourire.

M. Philippe Latombe, rapporteur. Nous nous apprêtons à en changer. Un véritable problème se pose à nous.

M. Mehdi Gharsallah. Votre recours à cette plateforme m'apparaît en tout cas révélateur, d'abord par la réaction qu'il suscite. Il y a lieu de se demander s'il est normal et souhaitable de s'en servir. Il me semble que non.

La France et l'Europe sont encore loin d'être souveraines sur des nombreuses strates du numérique. Un rééquilibrage, d'ailleurs probablement en cours, se révèle souhaitable, partout où il reste encore possible.

La notion de souveraineté numérique implique un double problème, car elle associe deux termes recouvrant des réalités très différentes. Leur combinaison multiplie les possibilités d'interprétation.

Les batailles qui se livrent autour du numérique et de la notion même de souveraineté n'en sont pas toutes au même point, que ce soit en France ou en Europe. En ce qui concerne les terminaux et les composants des ordinateurs et des téléphones, cette bataille me semble déjà perdue. Bien peu en France tentent en tout cas encore de la livrer. La perspective de disposer d'un ordinateur souverain a certes été maintes fois évoquée, mais l'alignement actuel des planètes n'y semble pas propice.

La bataille concernant les systèmes d'exploitation me semble elle aussi globalement perdue, sauf, peut-être, à la marge. Heureusement, il existe Unix et Linux, mais leur usage dans un cadre quotidien ne se répand pas tant que cela. Si une alternative libre aux systèmes d'exploitation mobiles Android ou iOS venait à surgir, il y aurait « un coup à jouer ». Sinon, dans l'ensemble, peu nombreux sont ceux qui s'engagent encore dans cette compétition.

Je me permets d'entrer dans le détail des différentes strates du numérique, car il me semble important de ne pas percevoir ce domaine comme un ensemble monolithique, ce qu'il n'est d'ailleurs pas.

Nous disposons d'un ancrage territorial tellement fort dans le domaine des infrastructures « réseaux » qu'il vient de nous sauver. Des opérateurs nationaux ou européens, en particulier dans l'enseignement supérieur et la recherche, comme le Réseau national de télécommunications pour la technologie, l'enseignement et la recherche (RENATER), garantissent notre souveraineté. Détenir des canaux de communication et d'échanges n'est pas anodin. De nombreux changements peuvent en découler.

La puissance d'Amazon web services (AWS) et de Microsoft dans le champ des centres de données, à l'extrémité de ces réseaux que nous venons d'évoquer, apparaît évidente. Cependant, nous pouvons encore leur opposer une résistance grâce à des acteurs européens comme OVHCloud ou des centres de données de recherche universitaires, labélisés par le ministère de l'enseignement supérieur, de la recherche et de l'innovation (MESRI). Ces acteurs peuvent et doivent permettre de rééquilibrer les forces en présence.

La strate des services et des usages est souvent celle qui se présente le plus spontanément à l'esprit, quand il est question du numérique. Nous sommes peut-être sur le point de perdre la bataille sur ce front, bien qu'il soit encore possible de résister et même d'anticiper les évolutions, grâce aux logiciels libres ou à la règlementation, et notamment au Règlement général sur la protection des données (RGPD). La digue qu'ils constituent me semble capable de résister, quoique pas forcément longtemps, en l'absence de services numériques en mesure de remporter pour de bon la bataille des usages.

Je reviens, sans malice, sur notre utilisation de Zoom dans cette audition. La force de cette plateforme repose en grande part sur l'expérience quasiment parfaite qu'elle offre à ses utilisateurs. La concurrence en a d'ailleurs beaucoup souffert depuis un an. Une fois habitué à son ergonomie et à la qualité des services qu'elle rend, un utilisateur hésitera à la délaisser au profit d'une plateforme, certes hébergée en Europe, mais dont il doute qu'elle fonctionnera de manière aussi optimale.

En somme, j'estime qu'il ne faut pas envisager la souveraineté numérique de façon monolithique.

Nous assistons en ce moment, et l'existence même de la mission le démontre, à « un alignement des planètes » inédit, qui permettra probablement un rééquilibrage des forces en présence, grâce auquel l'Europe pourrait imposer sa propre vision du numérique et de ses usages, face aux deux grandes puissances que représentent les États-Unis et la Chine. Cette conjoncture favorable est liée, à la fois, bien sûr, à la crise sanitaire que nous traversons et à ses impacts, entre autres économiques, sur les deux puissances que je viens de nommer.

Une prise de conscience a eu lieu, y compris aux États-Unis, de la position hégémonique, désormais sujette à débat, d'acteurs du numérique tels que Google, Amazon ou Microsoft. Elle s'accompagne d'une prise de conscience, de la part de l'ensemble des acteurs, en particulier politiques, que la protection de la vie privée ou des données personnelles ne consiste pas seulement à protéger l'identité des utilisateurs, mais aussi leur libre arbitre et leur autonomie comportementale et décisionnelle. La menace ne vient pas simplement d'un éventuel piratage d'une messagerie électronique ou d'une perte d'anonymat mais d'algorithmes massivement capables de modifier les modes de pensée. Un besoin crucial de s'en protéger surgit dès lors.

Un alignement des planètes, tel que nous l'observons actuellement, ne s'était plus présenté depuis les années 1980. Il y a donc « un coup à jouer » maintenant.

Nous devons continuer à tout mettre en œuvre pour ne pas dépendre de puissances étrangères, qu'il s'agisse d'entreprises géantes du numérique ou d'États, d'autant plus quand il existe entre eux des collusions d'ordre militaire, tout autant que politique. Leurs positions dominantes créent une forme d'hégémonie économique malsaine pour l'économie elle-même et comportent un sérieux risque de prise de contrôle de nos vies privées et même de notre libre arbitre. Un manque de confiance en résulte envers ces puissances étrangères qui se nourrissent de nos données en se réservant la possibilité de changer les règles et de couper les services à tout moment, comme cela s'est produit, lors du choc pétrolier de 1973, qui a déstabilisé l'économie mondiale. Si, demain, Google devenait payant ou privait de ses services des utilisateurs refusant de communiquer l'intégralité des éléments constitutifs de leur identité, l'économie mondiale entière en pâtirait.

Il faut veiller à ne pas réduire la place du numérique dans l'enseignement supérieur à son rôle dans l'enseignement à distance, d'autant qu'il en a beaucoup été question depuis un an, étant donné que le numérique apparaissait comme le seul moyen de poursuivre les formations pendant la fermeture des établissements. En somme, bien que le numérique ait dernièrement beaucoup servi d'outil, il ne se résume pas à cette dimension en dehors de la période très particulière que nous venons de traverser

Vous avez cité à la fin de vos propos introductifs ce en quoi consiste principalement le numérique dans l'enseignement supérieur : la création de contenus et de ressources pédagogiques. La France aujourd'hui, et la remarque vaut un peu moins pour l'Europe, fait figure de très bon élève en matière de production de ressources éducatives numériques libres. Nous avons commencé très tôt, voici une dizaine d'années, à investir ce domaine. Dans notre pays, on recense à ce jour entre 35 000 et 40 000 ressources éducatives libres, totalement accessibles à quiconque souhaite se former en ligne. S'y ajoutent évidemment les ressources propres à certains enseignants ou établissements, qui ne les partagent pas. Ces chiffres éloquents résultent d'une succession de politiques incitatives. Nous pouvons donc affirmer sans rougir notre souveraineté en termes de ressources pédagogiques. Malgré notre autonomie et notre indépendance actuelles, il n'est toutefois pas exclu que, demain, des acteurs privés

tels que des géants américains se mettent en tête d'intervenir dans ce champ. Quoi qu'il en soit, nous sommes pour l'heure loin de dépendre de quiconque en la matière.

Il est apparu, à la faveur de la crise, que l'accès à ces contenus, *via* un ordinateur ou un smartphone, équipé d'une connexion Internet, posait problème pour 1 à 3% d'étudiants. Cette proportion, en aucun cas insignifiante, prouve bien l'existence d'une fracture numérique, due, soit à l'impossibilité d'accéder au réseau, soit à sa qualité insuffisante ou encore à l'absence ou au partage d'un terminal de connexion à domicile. Beaucoup d'actions continuent d'être menées pour pallier cette difficulté, déjà connue, mais qui nous a sauté aux yeux dès le mois de mars 2020. Jusque-là, les établissements ouverts mettaient à disposition des étudiants des connexions sans fil, des ordinateurs dans des salles en libre-service et des tablettes, prêtées par les bibliothèques. Leur fermeture a mis en lumière des situations critiques.

Dans l'ensemble, l'équipement numérique des enseignants n'a pas posé de problème. Tous ne disposaient certes pas de micros, mais la plupart des établissements en ont fourni à ceux qui en avaient besoin. Des appels à projets financés par l'État continuent de permettre aux établissements qui le souhaitent d'équiper leurs enseignants. En général, cette démarche s'accompagne d'une formation de ces mêmes enseignants. Celle-ci constitue selon moi le principal enjeu actuel de la transformation numérique de l'enseignement supérieur. Cette réalité nous a sauté aux yeux pendant la période que nous venons de traverser.

Nous sommes tous, et moi le premier, victimes d'un biais : en tant que conseiller pour le numérique, je ne vois que des personnes à l'aise avec le numérique. Or elles s'apparentent à l'arbre qui cache la forêt. Entre un dixième et un cinquième des enseignants ont transformé leurs pratiques pédagogiques en instaurant des classes inversées, en produisant des *Massive open online course* (MOOC) ou encore en recourant à la remédiation. Nous nous sommes rendu compte, pendant la crise, qu'ils ne représentaient pas la majorité et qu'une part significative de la population enseignante nécessitait un équipement numérique et une formation à son utilisation, mais surtout à la transformation de la pédagogie.

Depuis un an, à quelques exceptions près, nous avons assisté à une volonté de transposer à distance les cours en amphithéâtre. Cette volonté me semble compréhensible, étant donné que le basculement du présentiel vers le distanciel est intervenu du jour au lendemain. Chacun s'est débrouillé comme il a pu, avec souvent beaucoup d'énergie et de conviction, ce que j'estime positif. Toutefois, nous nous sommes rendu compte que cette évolution ne correspondait pas à celle que nous œuvrions depuis des années à mettre en place. Il fallait en réalité remettre en question les pratiques pédagogiques pour les adapter au canal de communication utilisé. On ne travaille pas de la même façon en ligne qu'en classe. La plupart des établissements se chargent du nécessaire accompagnement des enseignants. Des appels à projets financés par l'État permettent de développer leur formation aux pratiques numériques. L'accélération des mesures en ce sens doit continuer. À ce jour, certains établissements ont déjà formé près de 80 % de leurs enseignants.

J'aborde volontairement en dernier les plateformes, car c'est souvent à elles que l'on songe en premier quand on traite du numérique dans l'enseignement. Nous avons remarqué à propos de ces plateformes, aussi bien de classe virtuelle, de webinaires, d'examens à distance que de *Learning management system* (LMS), c'est-à-dire d'administration de la classe, une assez grande hétérogénéité au sein des établissements, qui sont autonomes de toute manière. Certains étaient prêts à affronter la crise, alors qu'elle en a mis d'autres en difficulté. Aujourd'hui, des financements publics, à travers le plan de relance, subventionnent le développement de plateformes souveraines.

Les enjeux actuels de souveraineté portent principalement sur ces plateformes. L'objectif est de rééquilibrer les rapports de force avec les géants américains, dont nos données nourrissent les algorithmes, encore que la remarque s'applique assez peu aux données de l'enseignement supérieur. Nous continuons en somme de développer notre indépendance par rapport à ces acteurs majeurs sur l'ensemble des strates du numérique.

Vous m'interrogiez sur la formation, non plus par le numérique, mais au numérique, intimement liée, d'ailleurs, à la notion de souveraineté, ainsi que sur la place de la France par rapport à d'autres pays d'Europe. La France peut se targuer d'une très belle réussite dont nous sommes d'ailleurs fiers : la plateforme Pix d'autoévaluation, de formation et de certification des compétences numériques, accessible à tous gratuitement. Largement diffusée, elle accompagne l'ensemble des élèves en leur proposant des certifications à deux ou trois reprises au cours de leur scolarité dans le primaire et le secondaire. Les étudiants de la plupart des établissements d'enseignement supérieur y obtiennent au moins une certification en licence et une autre en master. Pix mériterait de se généraliser. Nous comptons créer à partir des certifications qu'elle propose un standard équivalent au *Test of English for international communication* (TOEIC) ou au *Test of English as a foreign language* (TOEFL). Pix s'appuie sur le référentiel européen de compétences numériques Digcomp, co-construit par l'ensemble des pays d'Europe. Il répertorie huit niveaux dans cinq domaines. Pix en constitue la première application concrète. Nous disposons, en France, d'une longueur d'avance dans ce champ, où nous venons de franchir une étape, suscitant l'envie de nos voisins européens. Des discussions sur Pix se déroulent avec l'Organisation des Nations unies pour l'éducation, la science et la culture (UNESCO) et la Commission européenne. Nous présentons régulièrement cet outil dans sa version internationale. Il marque une indéniable réussite pour former le plus grand nombre aux compétences et aux enjeux du numérique.

Pour en revenir aux propos du président-directeur général de l'Inria, nous nous heurtons à une difficulté de recrutement des étudiants dans les formations supérieures de très haut niveau, orientées vers le numérique. Nous avons identifié le problème et travaillons à le résoudre, notamment avec une association baptisée Talents du numérique. Elle nous a aidés à mieux cerner la perception des métiers et des formations du numérique par les élèves, en prenant pour échantillon ceux de l'Académie de Rennes. Ces professions souffrent d'un déficit d'image considérable. Sans doute les entreprises de services numériques n'ont-elles pas su dissiper le cliché du *geek* ou du *nerd* amateur de hard-rock et qui passe ses journées à coder. Certains discours présentant les développeurs comme les ouvriers du XXI^{e} siècle n'ont rien arrangé non plus. Nous sommes en tout cas certains que les représentations mentales des métiers du numérique se figent dès le lycée, amenant à considérer ces professions, qui ne font pas rêver, comme réservées à une certaine catégorie de population.

La réalité apparaît évidemment fort différente. Ceux qui veulent changer le monde devront en passer par le numérique. Il faut retravailler sur l'image des métiers du numérique et des formations à ces métiers, telle qu'elle se met en place dès un très jeune âge. En terminale, il est déjà presque trop tard. Les idées reçues, selon lesquelles le numérique ne conviendrait pas aux filles, par exemple, se construisent à compter des premières années de collège.

Si nous voulons qu'augmente le nombre de professionnels du numérique issus de nos formations, de très bon niveau, il faut y attirer plus de candidats. Seules les formations les plus sélectives n'en manquent pas. Résoudre ce problème répondrait à la question des moyens à mettre en œuvre pour s'assurer qu'un plus grand nombre d'étudiants en master s'orienteront vers la recherche. La difficulté ne vient pas seulement de l'attractivité du secteur privé. Les candidats ne sont tout simplement pas assez nombreux. Il ne servirait à rien de créer plus d'écoles ou de formations. Il faut d'abord remplir et rendre plus attractives celles qui existent

déjà. Sans doute conviendrait-il de réviser la manière dont nous les présentons et la place qu'y occupent les mathématiques ou leur aspect technique. Avant tout, nous devons quand même œuvrer à transformer les représentations des métiers du numérique.

M. Philippe Latombe, rapporteur. Vous avez parlé d'« alignement des planètes » favorable à la notion de souveraineté. Je vous poserai une question conjoncturelle et délibérément polémique : ne vous semble-t-il pas que ce concept, en ce moment à la mode, du fait, entre autres, de la pandémie, et utilisé à propos de tout et n'importe quoi, est brandi à propos du numérique parce que nous avons affaire à des entreprises aussi puissantes que des États ? Autrement dit, la notion de souveraineté numérique recouvre-t-elle au fond quoi que ce soit de substantiel ?

M. Mehdi Gharsallah. Je ne sais si le terme est à la mode. Il est en tout cas d'actualité. Il me semble donc normal que nous soyons nombreux à en parler et que les pouvoirs publics prennent conscience de la nécessité de reprendre la main, maintenant ou jamais. Je n'exclus pas que la mise en avant de la notion de souveraineté résulte d'une forme d'opportunisme mais, à la limite, peu importe.

Les discours sur l'écologie d'il y a vingt ans, au-delà du *greenwashing* (ou écoblanchiment), accordaient déjà une place considérable aux questions environnementales qui nous occupent aujourd'hui et qui ne sont d'ailleurs pas sans lien avec celles que soulève le numérique. Le constat, depuis quelques mois voire un an, qu'un État, une nation, leurs entreprises et leurs pouvoirs publics, et même la survie de leur économie dépendaient d'une puissance étrangère et de sociétés hégémoniques étrangères a frappé tout le monde. La revendication de ne plus utiliser que Linux n'émanait jusqu'à récemment encore que d'une bande de pirates informatiques. Ce n'est plus le cas aujourd'hui. L'affaire Edward Snowden ou le scandale lié à Cambridge Analytica ont conduit à une prise de conscience un peu brutale : nous sommes à la merci de puissances étrangères. La France et l'Europe ont voulu y mettre le holà. Telle est la réalité à laquelle nous sommes confrontés, au-delà de l'effet de mode. J'en suis en tout cas convaincu.

M. Philippe Latombe, rapporteur. Quelle place le logiciel libre occupe-t-il dans l'enseignement supérieur ? Le rapport présenté par M. Éric Bothorel sur la politique publique de la donnée a conduit à des prises de position du gouvernement. Où en sont aujourd'hui l'utilisation et l'enseignement du logiciel libre et des codes ouverts, non propriétaires ? Représentent-ils une piste d'avenir pour concurrencer les systèmes d'exploitation Android et iOS ?

M. Mehdi Gharsallah. Votre question comporte différents aspects, dont certains que je ne m'estime pas le mieux placé pour évoquer. Je ne cherche pas à botter en touche. Je vous renverrai, au besoin, vers un ou deux interlocuteurs au MESRI en mesure de répondre précisément à vos interrogations sur la production de code source, dont s'occupent principalement les chercheurs.

L'enseignement supérieur recourt en majorité à des plateformes libres. Ainsi, 98 % des universités utilisent Moodle. Le plan de relance finance des plateformes de dimension nationale, reposant soit sur BigBlueBotton, soit sur Jitsi, permettant à tout établissement qui le souhaite d'accéder à des solutions de classe virtuelle. RENATER ou le consortium ESUP-Portail produisent des outils logiciels 100 % libres à destination des universités. Notre approche se construit autour des logiciels libres, que nous ne nous contentons pas d'utiliser, puisque nous donnons à la communauté accès à nos contributions. L'enseignement supérieur et la recherche ont pris de ce point de vue des engagements forts, découlant de leur ADN.

La situation que nous vivons a poussé certains établissements à se servir de Zoom pour répondre à leurs besoins temporaires. Je m'attends à ce qu'ils y renoncent en grand nombre, dès que possible. Nos étudiants utilisent tout au long de leur journée des logiciels libres, pour y récupérer leurs cours et déposer leurs travaux.

Il existe des formations de niveau master, destinées aux futurs chercheurs, sur le dépôt de code source et les licences *creative commons.* Nous ne partons pas de rien. Une véritable culture du logiciel libre s'est implantée dans l'enseignement supérieur et la recherche. Peut-être ne l'avons-nous pas assez bien formalisée. Une amélioration en ce sens figure parmi nos engagements suite au rapport présenté par M. Éric Bothorel. Nous produirons à la fin de l'été notre feuille de route sur le logiciel libre. À vrai dire, nous utilisons sans cesse ce type de logiciels, aussi ne nous posons-nous même plus la question. La plateforme Pix, entièrement libre, est ainsi accessible à tous. N'importe qui peut la télécharger en vue de la modifier.

M. Philippe Latombe, rapporteur. Pensez-vous que pourraient, à terme, voir le jour des formations européennes fondées sur du logiciel libre et susceptibles de constituer la base d'un système d'exploitation européen souverain ?

Le RGPD a favorisé l'éclosion d'un certain nombre de solutions technologiques numériques. Le code et son enseignement, en vue d'en faire un langage commun en Europe, pourrait-il jouer le même rôle ? Pourrait-on structurer une filière de formation européenne autour du code ?

M. Mehdi Gharsallah. Je doute de ma capacité à répondre à votre excellente question. Bon nombre de nos formations, de qualité, sur le code possèdent déjà une dimension européenne, souvent par le biais de partenariats bilatéraux. Les liens entre les institutions existent d'ores et déjà, à l'échelle européenne. Les échanges et coopérations entre universités en fournissent le meilleur exemple.

L'Europe est réellement capable de produire des solutions qui pèsent dans la balance, c'est-à-dire, qui contribuent à un rééquilibrage. Il ne s'agit pas de battre Google, Amazon, FaceBook, Apple ou Microsoft (les GAFAM) mais d'échapper à une complète dépendance. Linux, sauf erreur de ma part, a été mis au point par un Européen. Nous sommes en mesure d'investir dans cette voie pour peu que nous le souhaitions.

J'attirerai votre attention sur un point, que je perçois comme une difficulté. J'ai noté que certains s'attendent parfois à ce que les initiatives européennes émanent de la Commission ou du Parlement en tant qu'institutions. Ces dernières ont certes beaucoup produit, et notamment le référentiel de compétences numérique, mais il vaudrait mieux percevoir toute solution conçue dans un pays d'Europe comme européenne. Sinon, autant considérer une solution née au Texas comme texane plutôt qu'américaine. Nous devons changer d'échelle. Une solution de classe virtuelle mise au point par les Allemands est par nature européenne. Il ne faut pas forcément attendre que les initiatives viennent des institutions, sous peine de ne parvenir à rien. Les pays membres de l'Union sont des parties constituantes de l'Europe.

M. Philippe Latombe, rapporteur. Les États-Unis constituent un État fédéral à l'histoire fort différente de celle de l'Europe.

M. Mehdi Gharsallah. Vous avez entièrement raison. Toutefois, nous devrions, lorsque les Allemands nous annoncent avoir mis au point une solution de classe virtuelle, nous autoriser à considérer celle-ci comme une solution européenne. Nous devrions également nous doter du cadre contractuel nécessaire et réviser le code des marchés.

M. Philippe Latombe, rapporteur. Nombre de nos auditions ont porté sur le code des marchés publics. L'impression vient malgré tout qu'en France, plutôt que d'adopter d'entrée de jeu les solutions développées dans d'autres pays, nous les reprenons à notre compte en vue de procéder à des expérimentations ultérieures, alors que nous pourrions plus simplement les transposer.

J'en reviens à la formation, non pas des ingénieurs de pointe mais des métiers intermédiaires, comme celui de développeur, assez mal perçus et trop peu féminisés. Existe-t-il des initiatives, dans d'autres pays voisins, que nous pourrions reproduire sans, justement, réinventer la roue ?

M. Mehdi Gharsallah. À vrai dire, je ne sais pas. Les initiatives françaises dans ce domaine viennent surtout de la société civile. Peut-être manquons-nous d'actions en ce sens à l'échelle de l'État. Il me semble que les autres pays d'Europe connaissent à peu près la même situation que nous. Il faut probablement aller plus loin. En Inde, à titre d'exemple, les métiers de l'informatique sont plutôt considérés comme féminins, car ils ne nécessitent pas de force physique et il est possible de les exercer à domicile. Je conviens que ces arguments trahissent un certain sexisme. En tout cas, les professions liées au numérique y sont perçues autrement.

Je note, quoi qu'il en soit, qu'il serait bon de mener une étude comparative des initiatives européennes, afin de mettre en évidence les mieux à même d'ouvrir les métiers du numérique au plus grand nombre et, surtout, à une plus grande diversité de profils.

M. Philippe Latombe, rapporteur. Le moment est venu de vous poser ma question rituelle de conclusion : souhaiteriez-vous aborder encore un autre point ou que notre mission approfondisse un sujet en particulier ?

M. Mehdi Gharsallah. Nous pourrions, à court terme, mettre en œuvre des solutions pour rééquilibrer le rapport de forces. Je ne reviendrai pas sur le code des marchés. Néanmoins, nous devons renforcer la préférence européenne dans ce cadre. Peut-être devrions-nous accorder aux lanceurs d'appels d'offres plus de liberté ou de latitude. J'ai vu se dérouler des procédures de marchés publics dans le domaine de l'informatique en nuage (ou *cloud*). Un marché a été déclaré infructueux parce que la meilleure offre émanait d'AWS. La volonté de camper sur une position défensive a finalement conduit à ne pas passer de marché du tout. J'estime impossible de continuer ainsi. Un changement s'impose.

M. Philippe Latombe, rapporteur. La stratégie *cloud* du gouvernement, diffusée voici quelques jours, vous satisfait-elle ?

M. Mehdi Gharsallah. Son existence même va considérablement nous aider. Cette doctrine claire a en outre été largement co-construite. Elle traduit un consensus et permet de nous protéger sans pour autant nous isoler. Nous n'avons aucun intérêt à cesser d'employer les solutions nord-américaines. Nous ne visons pas l'autarcie. Simplement, notre dépendance doit cesser. Cette stratégie de l'État me paraît aller dans le bon sens. J'espère que nous réussirons à l'appliquer comme il se doit.

Pour ce qui est des autres solutions à mettre en œuvre à court terme, la pierre est dans mon jardin. Le besoin se manifeste d'une meilleure formation encore des jeunes, plus malléables du fait de leur âge, afin de modifier leurs usages du numérique. Nous devons remporter la bataille des usages. Il n'est plus admissible que nous cédions à la facilité de poursuivre certaines pratiques en sachant pourtant pertinemment que nous ne le devrions pas. Il me paraît crucial de gagner cette bataille, au moins sur le front des étudiants, les plus jeunes ne relevant pas de la compétence de mon ministère.

M. Philippe Latombe, rapporteur. Comment voyez-vous la place du numérique dans l'enseignement à moyen terme ? Vous avez établi la distinction entre l'usage du numérique pour enseigner et les formations au numérique. Ma question porte sur ces dernières.

M. Mehdi Gharsallah. Pour peu que nous parvenions à relever le défi de la diversification des profils et de leur féminisation, notamment, de formidables possibilités se présenteront à nous. Nous disposons de formations de très bon niveau en France, en Intelligence artificielle ou en informatique quantique. Certains organismes se plaignent du manque de spécialistes dans ces domaines, mais il n'est pas imputable à un éventuel défaut de qualité de ces formations. D'ailleurs, beaucoup d'étudiants les ayant suivies alimentent les grandes sociétés américaines. Nous avons surtout besoin de remplir ces formations. Une fois relevé le défi de leur massification, encore que ce terme soit un peu fort, un bel avenir attendra la France. Nous avons de l'or entre les mains.

Audition, ouverte à la presse, de M. Jean-Luc Sauron, professeur associé à l'université de Paris-Dauphine
(25 mai 2021)

Présidence de M. Philippe Latombe, rapporteur.

M. Philippe Latombe, président et rapporteur. M. Jean-Luc Sauron, vous êtes professeur associé en charge du diplôme de délégué à la protection des données de l'université de Paris-Dauphine.

Nos auditions ont souvent traité du modèle européen du numérique, parfois qualifié d'humaniste et en tout cas distinct tant du modèle américain marqué par la prévalence de l'absence d'entraves à l'activité économique que d'un modèle autoritaire donnant à la souveraineté numérique l'aspect d'un suivi très attentif, voire soupçonneux, de l'usage d'Internet par les citoyens. Il a été question de convertir ce modèle européen en un outil, d'abord de puissance et de régulation au service du *soft power*, puis, un temps, d'une volonté de rééquilibrage de la compétition industrielle et économique. Nous comptons sur votre éminente connaissance des arcanes de la construction européenne pour nous éclairer à cet égard.

Je vous poserai trois questions liminaires.

Ma première concerne votre approche de la notion de souveraineté numérique. Il s'agit là d'une question rituelle lors de nos auditions, procédant de la grande diversité des définitions données à cette notion. Comment vous-même la concevez-vous ? Ne tendons-nous pas à présumer que les autres États de l'Union européenne (UE) partagent une vision de la souveraineté numérique européenne alignée sur la nôtre ? Les États voisins de la France en nourrissent-ils une conception proche ou divergente ?

Mon deuxième point portera sur l'évolution du droit européen des données personnelles. Comment évaluez-vous la portée de la jurisprudence récente, dont l'arrêt de la Cour de justice de l'Union européenne dit « Schrems II », du point de vue, tant de la garantie des droits de la personne, que de la réponse la plus efficace possible aux prétentions de certaines institutions publiques américaines d'user de leurs prérogatives hors du territoire des États-Unis ? Que répondre aux inquiétudes qui s'expriment parfois d'un risque induit de désavantage relatif dans la compétition scientifique et industrielle en matière, par exemple, d'Intelligence artificielle ? Comment pourrions-nous, en Europe, réguler sans entraver l'innovation ?

Je m'attacherai en troisième lieu aux initiatives de la Commission européenne en vue d'encadrer juridiquement l'espace numérique européen. Le *Digital Services Act (DSA)* portant sur les services numériques tend surtout à renforcer le processus de contrôle des contenus, tandis que le *Digital Markets Act (DMA)* visant les entreprises du numérique veut instaurer une nouvelle régulation du comportement des grandes plateformes sur le marché européen. Enfin, le *Data Governance Act (DGA)* s'efforce de consolider le cadre juridique du marché européen de la donnée. Comment jugez-vous ces initiatives en l'état, sachant que les trilogues où l'on en débattra n'ont pas encore commencé ?

M. Jean-Luc Sauron, professeur associé à l'université de Paris-Dauphine. En préparant cette audition, j'ai été frappé par la multiplicité des définitions données à la souveraineté numérique. Cette multiplicité montre bien l'extrême difficulté qui surgit pour qui tente de cerner cette notion, d'autant que certains refusent d'en considérer la polyvalence.

Sa meilleure définition reposerait encore, à mon sens, sur celle du cadre dans lequel elle s'exerce. M. Thierry Breton, en 2019, a évoqué le sujet lors d'une audition devant le Sénat. Il a très justement choisi de définir la souveraineté numérique comme un espace informationnel, de même qu'il existe un espace territorial, maritime ou encore aérien. Cette notion, extrêmement mouvante, d'espace informationnel recouvre l'ensemble considérable et sans cesse croissant des informations que les citoyens, les administrations et le secteur économique produisent et traitent.

La notion de souveraineté, appliquée à un État ou une nation, suppose en principe celle de frontières, qui me paraît difficile à transposer dans le domaine du numérique, encore qu'il ne faille pas écarter cette possibilité. La souveraineté repose aussi sur l'idée d'un pouvoir détenu par l'autorité publique dans un espace, en l'occurrence informationnel, pour organiser celui-ci, le structurer et le défendre. Il me semble en tout cas qu'il ne saurait exister de souveraineté numérique de l'espace informationnel sans stratégie nationale ou européenne pour le construire, sans anticipation de son devenir et sans outils pour le transformer. L'anticipation doit constituer un préalable à la stratégie, dont la mise en œuvre passera par des outils adaptés.

Je ne parviens pas, ce qui ne laisse d'ailleurs pas de me frapper, à discerner de stratégie numérique réelle en Europe, sauf depuis la récente nomination de M. Thierry Breton au poste de commissaire chargé, entre autres, du numérique. Nous nous contentons, jusqu'ici, en Europe, de naviguer à vue, en réaction à la conjoncture.

Nous avons d'abord réagi à notre environnement numérique par la convention 108 (pour la protection des données à caractère personnel) sous l'égide du Conseil de l'Europe, puis par la directive 95/46/CE (sur la protection des données). Le délai de transposition de cette directive courait jusqu'à octobre 1998. Or Google a été créée en septembre 1998. Nous constatons donc un décalage entre la réalité du monde numérique et notre législation européenne. Il a fallu attendre près de dix ans la mise en œuvre d'un outil, certes considérable, mieux adapté au contexte économique réel, tel que le Règlement général pour la protection des données (RGPD).

Il nous manque, selon moi, tant en France que dans l'Union européenne, la capacité d'anticiper. Avant de construire une stratégie et de concevoir les outils utiles à sa mise en œuvre, il faut réfléchir à ce que nous réserve l'avenir. Nous devons, à mon avis, nous appuyer sur ces trois piliers que constituent l'anticipation, la stratégie et les outils, pour viser un objectif de souveraineté numérique.

Vous m'avez interrogé sur l'existence d'une politique commune à l'Union européenne. Les 27 États qui la composent ne disposent pas tous d'une stratégie nationale de la donnée vraiment définie. La Grande-Bretagne, qui en avait une, a malheureusement quitté l'Union européenne. La France, l'Allemagne, l'Espagne et l'Italie en ont une également, mais l'on ne saurait en dire autant de tous les pays d'Europe. La seule limite que l'on constate, depuis près de vingt ans, aux politiques de la donnée vient de leur concrétisation industrielle.

En 2008, le programme Quaero ambitionnait de créer ce que l'on présentait alors comme un Google européen. Le partenaire allemand de ce projet franco-allemand s'en est retiré en 2013 et l'aventure s'est soldée par un échec. L'actuel projet GAIA-X, franco-allemand à l'origine, a depuis intégré certains opérateurs issus de géants américains du numérique et même une société chinoise. Faute, là encore, de stratégie industrielle claire, cette initiative est devenue illisible. Faut-il s'appuyer sur les grands acteurs étrangers, quitte à nouer avec eux des partenariats ? L'Europe peut-elle encore rattraper son retard ? Ces questions

méritent d'être tranchées. J'estime l'Union européenne capable de combler son retard, encore faut-il qu'elle s'en donne les moyens intellectuels.

Votre application du terme « humaniste » au modèle numérique européen m'a frappé tout à l'heure. Le RGPD veille avant tout à ce que la valeur que représentent les données reste là où elle est produite. Ne rejouons pas un combat humaniste. Ce RGPD répond au défi que devait relever l'Europe d'associer la capacité de nourrir notre économie de données avec un souci de la protection de ces mêmes données et du respect de la vie privée. Les États-Unis partagent ces mêmes préoccupations. Il me semblerait excessif de prétendre que les États-Unis foulent aux pieds les droits de l'homme. La remarque ne vaut certes pas pour d'autres systèmes, dictatoriaux.

Il me paraît tout de même étonnant de qualifier d'humaniste la protection des données en Europe. Une telle assertion revient à se tromper sur l'essence même du RGPD et de tout ce que nous avons construit depuis quarante ans.

M. Philippe Latombe, rapporteur. Cette assimilation erronée de la volonté de légiférer à un souci d'humanisme ne vient-elle pas du fait que la Cour de justice de l'Union européenne a rendu ses arrêts *Schrems* I, *Schrems* II et Tele2 dans un sens de protection des libertés individuelles et publiques ?

M. Jean-Luc Sauron. Il ne faut pas mettre sur le même plan les arrêts *Schrems* I et II, Tele2 ou même Quadrature du net, qui n'ont rien à voir. Ces arrêts s'inscrivent dans l'histoire des institutions européennes.

L'arrêt *Schrems* I a été rendu en 2015, c'est-à-dire avant l'entrée en vigueur du RGPD. L'activiste Max Schrems a en réalité attaqué le monopole de la Commission sur la définition d'une législation congruente. L'accord *Safe Harbor* de 2015*,* premier texte de relation entre les États-Unis et l'Union européenne, portait sur la protection des données lors de leurs échanges. En principe, une fois que la Commission européenne, à l'issue d'un long processus, prend une décision d'adéquation, selon laquelle un État tiers dispose d'une législation essentiellement convergente avec la nôtre en matière de données, il devient possible d'échanger celles-ci sans contrôle. Par son arrêt *Schrems* I, la Cour de justice européenne a remis ce principe en cause. Si jamais l'autorité de contrôle saisie par un citoyen prouve qu'en réalité, la législation de l'État tiers ne comporte pas les mêmes garanties de protection des données que notre législation, alors il revient à la Cour de justice de trancher la question. L'arrêt *Schrems* I a ainsi annulé l'accord *Safe Harbor*. Je vous rappelle que les législateurs, dont vous faites partie, ont intégré cette disposition à la révision de 2003 de la loi Informatique et libertés.

Le chapitre 5 du RGPD interdit clairement tout transfert de données vers un État extérieur à l'Union européenne, sauf, en vertu de son article 44, quand ces données bénéficient de la même protection hors du territoire de l'Union européenne. L'article 45 porte sur les décisions d'adéquation, l'article 46, sur les conventions internationales et autres outils garantissant la conformité de la protection des données, l'article 48 sur l'interdiction de communiquer des données à des administrations de pays tiers et l'article 49, sur les cas dérogatoires. De fait, cet article 49 compte parmi ceux qui suscitent le plus de débats. Il se voulait une porte de sortie. En réalité, il ne concerne pas de flux importants de données mais uniquement des cas exceptionnels limités.

Pour qui l'arrêt *Schrems* II a-t-il des conséquences ? Pour n'importe quel utilisateur de FaceBook, de WhatsApp, ou encore de Zoom, comme vous et moi en ce moment, mais également pour l'ensemble des entreprises. À l'heure actuelle, il n'existe pas de solution qui

permette de surmonter les difficultés soulevées par l'arrêt *Schrems* II. Les lignes directrices du comité européen de la protection des données (CEPD) ne répondent pas à la question fondamentale, qui porte sur la possibilité d'un recours juridictionnel pour assurer l'opposabilité des droits. La législation américaine n'est pas compatible avec la règlementation européenne. Comment des clauses contractuelles pourraient-elles aller à l'encontre de textes législatifs ? C'est impossible. Seul un nouvel accord entre les États-Unis et l'Union européenne serait en mesure de répondre à l'arrêt *Schrems* II.

L'arrêt Quadrature du net, relatif aux libertés publiques, met en lumière un problème de compatibilité avec un certain nombre de problématiques nationales. J'aimerais y revenir plus tard. Quoi qu'il en soit, il ne faut pas tout confondre.

L'arrêt *Schrems* II importe surtout par ses conséquences. Il n'existe pas aujourd'hui de société commerciale échangeant des données avec les États-Unis qui respecte le droit. La remarque s'applique à tous les secteurs, dont celui des banques. Y a-t-il lieu de le regretter ? Je ne le pense pas. Le juge de l'Union européenne a fait son travail. Il en a conclu qu'en l'état, le RGPD est inapplicable. Si les juridictions européennes ne parviennent pas à répondre aux difficultés que pose l'arrêt *Schrems* II, alors à quoi sert le RGPD ? En l'absence de réponse politique et juridique à l'arrêt *Schrems* II, je n'aurai plus qu'à mettre un terme à la formation diplômante que j'encadre pour me remettre au droit canonique.

M. Philippe Latombe, rapporteur. Justement, quelle solution opérationnelle pourrait être apportée à l'arrêt *Schrems* II ? Les équivalents, dans les autres pays européens, de la commission nationale de l'informatique et des libertés (CNIL) ont pris position sur le sujet, notamment son homologue irlandaise, qui en a tiré des conséquences assez strictes.

M. Jean-Luc Sauron. Je ne vois qu'une seule solution : un accord entre les États-Unis et l'Union européenne. Des négociations suivent d'ailleurs leur cours. Un tel accord devrait reconnaître la possibilité pour les ressortissants européens d'accéder aux juridictions américaines afin de faire valoir l'opposabilité de leur droit. Un tel accord interfèrerait avec les principes américains mais aussi avec le *Foreign Intelligence Surveillance Act (FISA)* et le *Patriot Act*.

Cela m'agace particulièrement que, parmi les décisions, articles et commentaires qui me tombent entre les mains, je n'aie pas encore trouvé une seule analyse vraiment pertinente et complète de la législation américaine, qui bloque l'exercice de nos droits et a suscité l'arrêt *Schrems* II.

Le mémoire de la CNIL relatif à l'ordonnance Health Data Hub indique clairement que l'entreprise qui reçoit une demande de communication de données émanant d'une agence de sécurité américaine ne peut pas en faire état à un tiers. Or cela ne dérange apparemment personne.

Vous avez auditionné les représentants d'Amazon Web Services (AWS). Que vous ont-ils dit ? Ils ont affirmé qu'au cas où une administration américaine leur adresserait une demande de communication de données, ils minimiseraient les données transmises. Il subsiste sur ce sujet beaucoup d'à-peu-près et de zones d'ombre, dont il faut sortir pour que se mobilise l'ensemble des juristes et de la communauté légale, composée des parlementaires et du gouvernement. Pourriez-vous me citer un seul gouvernement européen qui ait pris position sur l'arrêt *Schrems* II et ses conséquences ? L'attitude générale pourrait se résumer ainsi : « Cachez cet arrêt que je ne saurais voir. »

M. Philippe Latombe, rapporteur. Comment percevez-vous, à la lumière de l'arrêt *Schrems* II, les positionnements récents du gouvernement sur le Health Data Hub (HDH) et la doctrine du *cloud*, publiée voici quelques jours ?

M. Jean-Luc Sauron. Je serai franc : si seulement il n'y avait que le HDH à être hébergé par un *cloud* américain ! Demandez plutôt au gouvernement quels sont, en dehors de quelques opérateurs régaliens, les partenaires *cloud* de l'administration française.

Au lendemain de l'ordonnance de référé du Conseil d'État, très précisément la semaine suivante, l'Union des groupements d'achats publics (UGAP) claironnait un partenariat avec Microsoft Azure. Les quantités de données économiques, financières et d'organisations qui transitent par l'UGAP, centrale d'achat de l'administration, ne présentent-elles pas, à votre avis, un intérêt pour des tiers ?

Je n'ai pas compris, à la lecture des documents publiés par le gouvernement, en quoi notre *cloud* souverain assurerait notre souveraineté. Une demande de partenariat a été lancée dans l'idée de bénéficier des avancées technologiques des géants du numérique américains. Le problème du *cloud* souverain vient d'un défaut d'anticipation. Lors de son audition devant le Sénat en 2019, M. Thierry Breton, à l'époque, président-directeur général d'Atos, a déclaré que, pour l'heure, 80% des données se trouvent dans le *cloud*. Le développement de l'Internet des objets, grâce auquel les objets connectés passeront, d'ici dix ans, de 23 milliards à 75 milliards, soit une moyenne de 10 par habitant, et plus encore dans les pays développés, entraînera une modification de la répartition des données. Le *cloud* n'en hébergera plus, alors, que 20%. Qu'est-ce qui prendra de l'importance ? L'*edge computing* (informatique en périphérie), basé sur l'utilisation de la puissance de calcul là où se trouvent les données, c'est-à-dire, non plus dans le *cloud*, mais dans les objets connectés eux-mêmes. L'enjeu portera donc sur les algorithmes et, marginalement, la 5G (cinquième génération des standards pour la téléphonie mobile). Or les annonces de l'État concernent aujourd'hui le *cloud* souverain.

Je ne sais ce qu'il en est pour vous, mais j'ai, quant à moi, le sentiment très français que nous accusons systématiquement un retard. Il ne sert à rien de construire un *cloud* souverain, sorte de ligne Maginot numérique, alors que la bataille se jouera sur la maîtrise des algorithmes.

Comment les Américains et les Chinois ont-il construit leur avancée technologique ? À partir du bassin de données à leur disposition. Ces deux puissances vont développer grâce à ce bassin des algorithmes utilisés par l'Intelligence artificielle. Je suis bien sûr attaché aux droits fondamentaux et aux libertés individuelles et je défends le RGPD mais, faute d'un espace européen de la donnée, nous n'aboutirons à rien. Les différents pays de l'Union européenne n'utilisent même pas les mêmes applications de contrôle du Covid. Si nous voulons rattraper notre retard et devenir autonomes, technologiquement, nous devrons, une fois établi le bassin de données qui nous manque, produire des systèmes d'Intelligence artificielle.

Ce que nous avons connu à propos de la 5G, au développement de laquelle n'a participé qu'un malheureux opérateur européen, se reproduira à une échelle dix fois supérieure dans le domaine de l'Intelligence artificielle et des algorithmes. Nous en revenons au défaut d'anticipation. Que ferons-nous dans cinq ans ? Où en serons-nous dans dix ans ? Nous devons accélérer et nous fixer des objectifs.

La réponse opérationnelle à la circulation des données comporte deux volets. Tout d'abord, il faut résoudre le problème soulevé par l'arrêt *Schrems* II. En 2019, le Conseil de l'Union a été mandaté pour discuter avec les États-Unis des relations entre nos autorités

publiques respectives. Par le *Clarifying Lawful Overseas Use of Data Act* (*Cloud Act*), le gouvernement américain s'est arrogé le droit de consulter les fichiers d'entreprises soumises à la législation américaine, y compris à l'étranger.

Le deuxième volet du *Clourd Act*, tout aussi important, bien qu'il en soit peu question, prévoit des négociations internationales avec des États tiers pour assurer, dans un cadre légal, des relations entre autorités publiques. En somme, le *Cloud Act* n'est qu'une façon de contourner les traités d'entraide judiciaire. Une fois que certains pays se seront mis d'accord avec les États-Unis, ceux-ci iront piocher dans les données traitées par les opérateurs pour obtenir celles que nécessitent certaines enquêtes policières ou judiciaires.

Comment est né le *Cloud Act* ? Il ne vient pas d'un projet américain de domination du monde. Il a vu le jour parce que, dans le cadre d'une enquête policière, il a été demandé à Microsoft de fouiller dans des fichiers en Irlande. L'entreprise a objecté au gouvernement américain qu'elle n'y était pas autorisée à moins de méconnaître la souveraineté irlandaise. Quelques mois plus tard, le vote du *Cloud Act* a donné à Microsoft le droit de fournir au gouvernement les données nécessaires à une enquête relative à la sécurité nationale.

La réponse à l'arrêt *Schrems* II réside en un accord entre l'Union européenne et les États-Unis, qui apporte des garanties essentielles, communes aux deux espaces, en matière d'échange de données. Comment faciliter sa mise en œuvre ? Une loi française de 1968 interdit la communication à des États de données économiques, financières ou administratives. Les sanctions en cas de contravention sont aujourd'hui inexistantes, alors que les géants américains du numérique ne sont pas toujours en adéquation avec le gouvernement américain. Ils pourraient très bien objecter à un juge américain qu'au cas où ils communiqueraient aux États-Unis des données au mépris de lois étrangères, ils subiraient telle ou telle sanction. Ce juge, estimant ces sanctions trop pénalisantes, admettrait alors le refus de l'entreprise de transmettre les données demandées. En 1987, la Cour suprême américaine a clairement déclaré qu'en l'absence de sanctions effectives en cas de contravention à la loi de blocage française de 1968, celle-ci n'avait pas à être prise en compte. Pour faciliter les négociations avec les États-Unis, nous pourrions durcir les sanctions à l'encontre des grands opérateurs numériques. Rappelons que, depuis 2018, une seule condamnation a été prononcée en Europe contre un opérateur, par la CNIL. L'autorité italienne de régulation de la concurrence vient de lancer une procédure contre Google. Nous disposons d'outils, mais le plus efficace reste la négociation d'un accord international avec les États-Unis afin de définir les garanties essentielles qui nous permettraient d'avancer sur le sujet.

Il faut garder à l'esprit que la possibilité pour n'importe quel ressortissant européen ou étranger de défendre ses droits devant le juge est propre à notre culture européenne. Il n'en va pas de même aux États-Unis, en matière de traitement des données, ou alors très difficilement. Jusqu'à la décision d'adéquation entre l'Union européenne et le Japon, ce n'était pas possible non plus au Japon. Désormais, un ressortissant européen sollicitant une protection contre l'utilisation de ses données au Japon peut enfin, par le biais d'un mécanisme, certes assez lourd, mais qui a le mérite d'exister, obtenir une décision d'une juridiction japonaise. L'accès au juge, typiquement européen, n'est pas reconnu sur l'ensemble de la planète.

M. Philippe Latombe, rapporteur. Sur le plan opérationnel, ou plus exactement technique, que penser de GAIA-X, présenté comme l'une des réponses possibles à l'arrêt *Schrems* II ?

M. Jean-Luc Sauron. Pour le moment, GAIA-X a donné naissance à un partenariat entre OVHcloud et Deutsche Post. D'autres partenariats devront suivre. Rappelons que GAIA-X n'est pas un projet de *cloud* européen mais de moteur de recherche, censé fournir les

références d'entreprises européennes répondant à un cahier des charges relatif à certains droits, aujourd'hui impossibles à appliquer, dans la pratique, par un opérateur européen de *cloud*. Ces droits concernent entre autres la portabilité ou la possibilité de transférer des données.

Aujourd'hui, le seul secteur où la portabilité des données s'est imposée reste celui des opérateurs téléphoniques, alors même que ceux-ci prétendaient une telle exigence impossible à mettre en œuvre. Un usager d'Orange peut ainsi migrer vers Bouygues tout en conservant son numéro de téléphone et ses données.

À ce jour, GAIA-X se résume à un cahier des charges, voire à une liste d'opérateurs. Le plus étonnant reste que, malgré l'arrivée récente de certains géants américains du numérique et d'opérateurs chinois dans l'initiative GAIA-X, ceux-ci ne bénéficieront pas du label GAIA-X, ce que je peine à comprendre.

J'ai bien saisi, en revanche, que deux campagnes se déroulent en ce moment au sujet du *DMA*. La rapporteure du Parlement européen, Mme Stéphanie Yon-Courtin, estime qu'il ne faut pas infléchir le *DMA* pour cibler les géants américains du numérique, alors qu'en réalité, si. Comment permettre à des plateformes européennes de monter en puissance, sinon en les protégeant de la concurrence des puissants acteurs américains ? Il ne sert à rien d'imposer un Règlement européen tant que les portes de l'Europe restent ouvertes à la concurrence étrangère.

J'y vois là une tare européenne. Il n'y a qu'en Europe qu'une société est considérée comme européenne, bénéficiant ainsi d'aides européennes, pour la simple raison qu'elle a établi une filiale sur le territoire de l'Union européenne. Les acteurs américains du numérique participent aux marchés publics européens. Pour qu'une entreprise européenne participe à un marché public au Canada, alors même que les opérateurs canadiens tels que Bombardier répondent déjà aux appels publics d'offres en Europe, il faudra attendre l'entrée en vigueur d'un accord commercial bilatéral de libre-échange (le *Comprehensive Economic and Trade Agreement* ou *CETA*).

La position défendue par cette rapporteure m'agace au plus haut point. Nous ne pouvons pas continuer comme cela. À quoi songe-t-elle ? Un problème de lutte se pose. L'un des points majeurs du *DMA* porte sur la possibilité de laisser à des plateformes européennes le temps de monter en puissance. Ensuite seulement, les règles de concurrence pourront changer, sans quoi aucune plateforme européenne n'émergera jamais. La fable de La Fontaine sur le lièvre et la tortue ne s'applique pas dans le monde économique.

Les autorités de concurrence nationales devraient en outre jouer leur rôle. Se sont-elles montrées capables d'une confrontation avec les géants américains du numérique ? Non. Il faut une force aussi importante que la Commission européenne pour intervenir sur le champ de bataille, où doivent être mobilisés bien plus que de petits régiments.

Le texte du *DGA* est d'une extrême importance, bien qu'il en soit peu question. Là encore, on note un manque de réflexion nationale et européenne sur ce que recouvre la notion de données ouvertes. Aujourd'hui, si vous me pardonnez la familiarité de cette expression, l'*open data*, c'est l'*open bar*. Les données ouvertes sont produites par les administrations, qui ne disposent ni de la réglementation ni des spécialistes seuls à même d'éviter que des tiers étrangers s'approprient leurs données économiquement utiles. Il aurait fallu, une fois de plus, anticiper l'usage de ces données ouvertes, source de richesse et de production de valeur. Qui en tire profit aujourd'hui ? Le secteur souffre d'une mauvaise structuration.

M. Philippe Latombe, rapporteur. Que devrions-nous, en tant que législateurs français, voire européens, mettre en œuvre pour améliorer la situation ? Que préconisez-vous, dans l'immédiat ?

M. Jean-Luc Sauron. Je n'ai jamais songé à dicter des lois, même dans mes rêves les plus fous. Différents secteurs sont à considérer.

D'abord, je réfléchirais à l'ensemble des autorités qui interviennent en France dans le domaine du numérique. Nous constatons dans notre pays une accumulation d'autorités administratives indépendantes. Dès qu'il s'en crée une, une autre s'y ajoute, aux compétences proches. Il faudrait remettre à plat ce champ et se donner les moyens d'agir. La CNIL accomplit un travail remarquable, mais elle n'emploie que 225 personnes. Vous n'imaginez bien évidemment pas qu'elle puisse, avec ce faible effectif, mener un travail de fond sur l'ensemble du territoire. Malgré la forte mobilisation de ses équipes, elle n'en a tout bonnement pas les moyens.

L'émission *Cash investigation* sur la carte vitale et l'utilisation des données de santé a suscité grand bruit, à juste titre. J'ai consulté la délibération afférente de la CNIL. On y lit en page 4 : *« Il est prévu que les personnes soient informées individuellement* [du traitement des données les concernant] *par la remise d'une notice d'information. »* Des délibérations dont nul ne vérifie l'application ne servent à rien. Il faudrait que la CNIL s'appuie sur un maillage du territoire comparable à celui de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

M. Philippe Latombe, rapporteur. Faudrait-il aller jusqu'à grossir le budget de la CNIL d'une partie des amendes qu'elle inflige ? Ou une telle proposition reviendrait-elle à tordre son modèle économique au risque de générer des effets de bord trop importants ?

M. Jean-Luc Sauron. Le système de la CNIL commence à dater. L'État pourrait se donner les moyens financiers d'assurer une régulation, dont l'importance économique n'est pas négligeable. Reconnaissons que ce serait contraire au mode de fonctionnement français et même européen. Le maillage du territoire revêt une importance considérable. L'acculturation au RGPD, et donc son application, ne progresseront qu'à condition d'y sensibiliser et d'y former les citoyens.

Le ministre actuel de l'éducation nationale effectue un travail considérable. Je ne le chargerai donc pas. J'estime toutefois aberrant de ne pas considérer l'éducation numérique comme un enjeu fondamental, au même titre que la capacité de lire, écrire et compter. La maîtrise des enjeux du numérique participe de la modification des modes de sélection dans l'administration et même l'emploi privé. Lors de mes études en droit, mes condisciples et moi-même devions acquérir des bases communes avant de nous spécialiser. J'estime impératif que des cours en université prolongent l'enseignement du numérique dans le primaire et le secondaire. Ces cours porteraient sur le RGPD et les grands principes du numérique, qui font désormais partie de la culture de tout honnête homme au XXI^{e} siècle.

Nous n'avons pas évoqué la Cour européenne des droits de l'Homme, dont la jurisprudence encadre pourtant aujourd'hui des pans entiers du domaine économique, concernant la protection des données.

Le fait, que des décisions prises dans un État de l'Union européenne ne s'appliquent pas dans les autres, me chagrine et choque quelque peu les opérateurs. En voici un exemple. L'autorité berlinoise de contrôle de la protection des données, suivie de ses homologues dans chacun des *Länder* allemands, a estimé, voici près de six mois la suite Microsoft 365 non

conforme au RGPD. Il est inconcevable que des décisions portant sur des systèmes qui opèrent dans l'ensemble d'un espace de données, où celles-ci circulent sans frontières, jugent ceux-ci dangereux sur un territoire, alors que dans le territoire voisin, nul ne s'en émeut.

M. Philippe Latombe, rapporteur. Le problème de la cohérence entre les États européens vous semble-t-il le plus prégnant aujourd'hui ?

M. Jean-Luc Sauron. Sans conteste. La position des autorités de concurrence nationales, qui souhaitent aujourd'hui jouer un rôle dans l'application du *DMA*, relève selon moi d'un contresens historique.

M. Philippe Latombe, rapporteur. Je vous poserai maintenant la question rituelle qui conclut nos auditions. Souhaiteriez-vous aborder un sujet que nous aurions omis d'évoquer, ou insister sur un point particulier ?

M. Jean-Luc Sauron. D'abord, il me semble important de relever que certains droits n'existent pas dans la pratique. Je songe ici au droit à la portabilité, garanti par le RGPD, ou encore au droit au transfert de données, heureusement bloqué par l'arrêt *Schrems* II. Le droit à la portabilité garantit la liberté de choix du consommateur. Pour l'instant, il ne trouve d'application que chez les opérateurs de téléphonie mobile.

Ensuite, j'insisterai sur le problème de cohérence entre autorités administratives indépendantes. Hier, l'*Information Commissioner's Office (ICO)*, l'autorité britannique de contrôle du traitement des données, et la *Competition and Markets Authority (CMA)*, autorité britannique de régulation de la concurrence, ont publié une déclaration de manière que leurs analyses convergent. Il ne me semble plus admissible que subsistent des incohérences dans la gestion d'un espace des données unique.

M. Philippe Latombe, rapporteur. La portabilité des données implique l'interopérabilité des systèmes et des plateformes.

M. Jean-Luc Sauron. En effet. Je souhaite bonne chance aux utilisateurs de Microsoft Azure pour exploiter leurs données dans un autre *cloud*.

M. Philippe Latombe, rapporteur. L'interopérabilité des systèmes s'avère donc indispensable, si l'on veut déposer des données chez un autre hébergeur.

M. Jean-Luc Sauron. Bien sûr, sinon l'utilisateur se retrouve prisonnier de son opérateur.

M. Philippe Latombe, rapporteur. J'aborderai le sujet avec les représentants de Microsoft jeudi.

M. Jean-Luc Sauron. Vous leur rappellerez les cris d'orfraie des opérateurs téléphoniques lorsque l'interopérabilité leur a été imposée. Tous ont juré qu'une telle exigence relevait d'une impossibilité technique, or ils sont finalement parvenus à s'y plier, en y mettant un peu de bonne volonté.

M. Philippe Latombe, rapporteur. Commercialement, ils l'ont ensuite présentée comme un avantage.

M. Jean-Luc Sauron. J'ai parfois l'impression que le secteur économique lui-même est en décalage avec la réalité. L'anticipation s'avère aussi nécessaire qu'une stratégie valable et les outils pour la mettre en œuvre. Nous l'avons déjà dit.

Audition, ouverte à la presse, de MM. Olivier Vallet, président-directeur général de Docaposte, membre du comité de direction de la branche numérique, et Gabriel de Brosses, directeur de la cybersécurité, du groupe La Poste
(25 mai 2021)

Présidence de M. Philippe Latombe, rapporteur.

M. Philippe Latombe, président et rapporteur. Le groupe La Poste a souhaité s'exprimer devant notre mission d'information. Nous nous réjouissons de pouvoir répondre favorablement à sa sollicitation.

Le groupe La Poste a développé ses actifs et infrastructures numériques afin de consolider sa position de tiers de confiance, conformément aux orientations de son plan stratégique La Poste 2030. Le troisième des sept axes prioritaires de ce plan préconise d'accélérer la transformation numérique, de développer les services de confiance numériques et de contribuer à l'inclusion numérique.

Je souhaiterais, pour commencer, évoquer trois sujets.

D'abord, comment concevez-vous la souveraineté numérique ? Cette question rituelle lors de nos auditions procède de la grande diversité des définitions données à cette notion. Comment votre approche de ce concept se traduit-elle concrètement, au plan opérationnel, dans vos activités ? Quelle appréciation portez-vous sur le dispositif de régulation du numérique prévu par le cadre juridique national et européen de la protection des données ?

Pourriez-vous ensuite nous présenter la stratégie de transformation numérique du groupe, telle que la définit le plan stratégique La Poste 2030 ? Le groupe La Poste participe par l'intermédiaire de sa filiale Docaposte à l'initiative GAIA-X. De quelle manière y contribuez-vous ? Le groupe La Poste a récemment acquis la société Open Value, spécialisée dans l'Intelligence artificielle. Quelles solutions développez-vous à l'aide de cette technologie ? Quel positionnement comptez-vous adopter dans le domaine des technologies numériques de pointe telles que l'Intelligence artificielle, justement, ou encore la *blockchain* ?

Comment la crise sanitaire a-t-elle par ailleurs rejailli sur la mise en œuvre de votre démarche de transformation numérique ? Comment, plus généralement, cette crise a-t-elle selon vous modifié le rapport des entreprises au numérique, leur protection contre les risques cyber ou encore la numérisation de leurs infrastructures ?

Enfin, j'aimerais que vous nous présentiez votre solution d'identité numérique et ce que vous en attendez en termes, notamment, de modèle économique.

M. Olivier Vallet, président-directeur général de Docaposte, membre du comité de direction de la branche numérique du groupe La Poste. Le groupe La Poste a subi une transformation considérable. Le courrier ne représente plus aujourd'hui que 20% de son chiffre d'affaires. Un premier cycle stratégique La Poste 2020 vient de se terminer. Notre président, M. Philippe Wahl, vient d'annoncer un nouveau plan stratégique : « La Poste 2030, engagée pour vous ».

Ce plan 2030 repose sur deux moteurs de croissance essentiels : l'e-commerce et la logistique, d'une part, et d'autre part, le pôle banque et assurance. CNP vient de rejoindre la Banque postale. M. Philippe Wahl a manifesté sa volonté d'accélérer nos investissements afin que nous puissions nous appuyer sur deux nouveaux moteurs de croissance. Le premier – les

services de proximité à domicile – reposera sur le maillage du territoire par les postiers. Le second, qui nous occupe aujourd'hui, correspond aux services de confiance numériques, domaine dans lequel La Poste souhaite s'imposer comme une référence.

Depuis plusieurs années, le groupe La Poste, à travers sa filiale Docaposte, qu'il détient sans partage, a investi dans les services numériques de confiance, en vue de les développer. Ces services correspondent à trois étapes ayant leur pendant dans le monde physique : d'abord, l'identification ou authentification, ensuite l'échange d'informations, ou encore les transactions et, enfin, leur archivage, c'est-à-dire le stockage des données correspondantes. Le groupe La Poste a investi dans une gamme de solutions qui lui permet désormais de couvrir l'ensemble de ces trois étapes.

Nous reviendrons sur la première, à savoir l'identité numérique, puisque, grâce aux investissements de notre groupe, nous sommes les premiers en France à disposer d'une identité numérique dite de niveau substantiel. Je préciserai ultérieurement le modèle économique selon lequel nous envisageons de la déployer afin qu'y adhèrent le maximum de Français. En matière de numérique, il faut qu'un grand nombre de personnes utilisent une solution pour qu'elle s'impose mais, avant d'en arriver là, il faut à cette solution des usages pratiques, ce qui découle en général de son utilisation par un grand nombre de personnes. En somme, il faut travailler sur les deux aspects du problème en même temps.

Concernant la deuxième étape, celle des transactions, notre groupe propose l'ensemble des services visés par le Règlement européen *Electronic identification authentication and trust services* (eIDAS), qu'il applique d'ailleurs à la lettre.

Enfin, pour ce qui est de la troisième étape, d'archivage, nous avons investi dans un coffre-fort numérique Digiposte, atout de notre groupe, puisqu'il compte à ce jour plus de six millions de clients.

Nous sommes conscients que la confiance constitue un préalable à la souveraineté. L'une ne va pas sans l'autre et notre groupe doit s'appuyer sur les deux. Si l'État se porte garant de la dimension souveraine de nos services, La Poste bénéficie quant à elle d'un capital de confiance auprès des entreprises, des citoyens et des administrations. Plus personne ne soupçonnerait un facteur d'ouvrir le courrier pour en prendre connaissance. Nous tentons de transposer cette confiance qui nous honore, du monde physique dans le monde numérique, de manière inclusive, sur tout le territoire, en proposant à nos clients des solutions d'une grande simplicité d'utilisation pour leur simplifier la vie. Notre qualité de service irréprochable doit correspondre au niveau d'exigence souvent élevé des usagers du numérique.

Nous avons conscience des doutes, ou de la résistance au numérique, je ne sais quel terme employer, d'une partie de la population qui manque de confiance dans les nouvelles technologies. Le groupe La Poste doit pouvoir y remédier en s'appuyant sur son ADN et sa capacité à atteindre tous les Français, quel que soit leur lieu de résidence, afin d'accompagner physiquement nos concitoyens les plus éloignés du numérique. J'ai la conviction que le numérique servira de trait d'union entre les Français et leur administration et que nous bénéficierons tous, grâce au numérique, de services d'une facilité d'utilisation croissante.

Docaposte, en tant que filiale de La Poste, aide notre groupe à se numériser pour proposer à ses clients une offre à la fois physique et numérique. Tournée vers l'extérieur, Docaposte investit considérablement dans nombre de technologies. Nous disposons de nos propres centres de données et d'informaticiens « maison ». Notre force de frappe nous permet de fournir des solutions à la pointe. Docaposte compte parmi sa clientèle les plus grandes entreprises françaises, ce qui démontre la compétence et le savoir-faire du groupe La Poste.

Je terminerai sur une note positive. Nous nous félicitons de toutes les initiatives mises en œuvre par l'État, telles que le plan cyber annoncé récemment, ou la nouvelle directive sur le *cloud* (ou informatique en nuage), qui va selon nous dans le bon sens. Bien entendu, nous y souscrivons. Nous venons de déposer un dossier en vue d'obtenir le label SecNumCloud.

Je nourris malgré tout une petite frustration. Les solutions du groupe La Poste ont toutes été développées à l'échelle de la nation, au prix, d'ailleurs, d'investissements conséquents, or nous nous heurtons à la difficulté de les déployer à la vitesse qu'il faudrait. Nos concitoyens devraient à mon sens disposer de ce que j'appelle un trousseau numérique, pour mener leur vie numérique en toute confiance. Ce trousseau inclurait une identité numérique, un coffre-fort numérique et une messagerie électronique.

Docaposte, détenue par La Poste, un groupe à l'actionnariat public, est à même de servir de bras armé à la transformation numérique de l'État au service des citoyens en vue de leur faciliter la vie au quotidien. Néanmoins, la complexité du déploiement de nos solutions, qui requiert en outre beaucoup de temps, génère en nous une légère frustration, d'autant que La Poste, en tant que marque de confiance, apparaît tout à fait en mesure, au côté de l'État, de dissiper les doutes et les inquiétudes qui subsistent encore chez certains de nos concitoyens vis-à-vis du numérique.

Le lancement de l'application TousAntiCovid l'a montré : le caractère souverain d'une solution numérique n'est pas un critère suffisant de succès. Peut-être TousAntiCovid n'a-t-elle pas assez inspiré confiance. La Poste pourrait apporter son capital de confiance dans la mise en œuvre d'autres solutions numériques, rassurant ainsi l'ensemble de nos concitoyens sur la possibilité de gérer leur vie numérique sans inquiétude.

Souveraineté et confiance vont de pair. Toutes les initiatives prises en ce moment, et notamment la récente directive sur le *cloud*, vont dans le bon sens pour créer des champions français et européens souverains du *cloud*, grâce auxquels nous pourrons utiliser, en toute sécurité, des technologies avancées. Nous nous en félicitons.

Il reste tout de même à s'assurer que des effectifs en nombre suffisant mettront en œuvre ces directives de manière à délivrer les labels indispensables. Nous entretenons des relations nourries avec l'agence nationale de la sécurité des systèmes d'information (ANSSI), qui fournit un travail extraordinaire au quotidien. Le nombre de dossiers qu'elle doit traiter risque tout de même de conduire à un goulot d'étranglement. Les certifications et labels reconnus par l'État devraient pouvoir s'obtenir le plus rapidement possible. La Poste répond en tout cas présente à toutes les initiatives que j'évoquais, aussi bien dans le domaine cyber que dans celui du *cloud*.

Docaposte compte parmi les membres fondateurs de GAIA-X et appartient à son conseil de direction. Nous avons beaucoup participé aux réflexions sur l'interopérabilité des solutions à proposer *via* GAIA-X ainsi qu'aux travaux sur le *cloud* et ses usages dans la finance ou la logistique. Nous sommes fortement engagés dans cette initiative qui présente, selon nous, un intérêt certain pour l'Europe.

La stratégie de transformation de La Poste s'articule en deux volets.

Tout d'abord, La Poste elle-même doit se numériser et se transformer conformément aux deux objectifs que j'ai mentionnés : offrir aux clients des parcours simples et fluides et améliorer la qualité de nos services au quotidien. Pour y parvenir, La Poste a décidé de créer, début 2021, une nouvelle branche Grand public et numérique. Nous avons fusionné notre réseau physique avec les technologies numériques pour offrir à notre clientèle des parcours

fluides, à la fois physiques et numériques. Un client se rendant dans un bureau de poste peut dorénavant y entamer des démarches numériques, passant d'un canal de communication à l'autre sans heurt tout au long de son parcours.

Ensuite, La Poste doit se tourner vers l'extérieur en se positionnant, principalement à travers sa filiale Docaposte, comme un acteur de référence des services de confiance numériques. Nous disposons d'une gamme complète de solutions, allant de l'identité numérique au vote électronique, secteur où nous occupons une position prééminente en France. Nos nombreux investissements et acquisitions, dont celle de Pronote, un logiciel beaucoup utilisé par l'Éducation nationale, nous permettent d'offrir des solutions en toute sécurité aux entreprises et aux administrations comme aux particuliers. La volonté de Docaposte de devenir un moteur de croissance du groupe nous amène à poursuivre nos investissements pour soutenir notre croissance externe, de même que nos acquisitions. Nous comptons renforcer la dimension numérique de La Poste pour que le groupe propose à ses clients des solutions numériques de bout en bout.

À propos des données, nous avons racheté ProbaYes et Softeam, société de services numérique forte de son savoir-faire en matière de données et, plus récemment, la société Openvalue. Nous disposons ainsi de l'un des plus grands pôles de *data scientists* (ou experts en analyse de données) de France, au nombre de 250 à 300 dans notre entreprise. Nous ambitionnons d'accélérer, grâce à eux, la transformation interne du groupe La Poste pour offrir à nos clients des services innovants basés sur l'analyse des données. Docaposte envisage également de prolonger son offre de services auprès de sa propre clientèle, qui compte quatre entreprises sur cinq du CAC40, ainsi que de nombreuses entreprises de taille intermédiaire (ETI) et de petites et moyennes entreprises (PME).

M. Gabriel de Brosses, directeur de la cybersécurité du groupe La Poste. La cybersécurité se développe dans notre groupe selon la même voie que nos services numériques.

La première question que soulève la souveraineté numérique porte sur la disponibilité de l'offre numérique. Les dispositifs qui l'encadrent définissent des standards grâce auxquels se développent des solutions de remplacement au stockage des données sur un support physique.

La Poste propose une offre complète de services numériques de confiance, incluant tous ceux que visent le règlement eIDAS. Le groupe maîtrise parfaitement les problématiques liées à l'hébergement de données. Il applique des référentiels d'un haut niveau d'exigence, comme celui de certification HDS (hébergeur de données de santé) ou encore celui qui s'applique aux établissements bancaires. La règlementation en vigueur définit des standards garantissant la protection des données.

Le pôle dédié aux données, d'une extrême importance au sein du groupe, s'est construit par agrégation. La sécurité des systèmes d'information passera de plus en plus par la maîtrise de la donnée et par la capacité d'appliquer des solutions d'Intelligence artificielle ou d'apprentissage automatique à nos échanges d'information.

Souhaitez-vous que nous abordions maintenant les effets de la crise sanitaire par rapport au numérique ?

M. Philippe Latombe, rapporteur. Le sujet a beaucoup mobilisé, ces derniers mois. Comment percevez-vous l'impact de la crise sanitaire, non pas sur le plan économique mais en termes de pratiques du numérique et d'inflexion des politiques du numérique ?

M. Gabriel de Brosses. Dès le début du mois de mars 2020, le groupe s'est préparé à un télétravail massif. Nos collaborateurs devaient accéder à des espaces de travail en ligne pour que La Poste assume son obligation de maintenir l'activité des métiers du groupe à distance. La Poste compte en France 240 000 employés. Nous disposions heureusement d'une infrastructure de systèmes d'information en mesure de supporter la charge correspondante : jusqu'à 50 000 personnes ont pu s'y connecter simultanément.

Nous nous sommes par ailleurs rendu compte de notre dépendance vis-à-vis des solutions de Microsoft comme Office 365. Grâce à la solidité de ce partenaire, qu'on ne définirait certes pas, *a priori*, comme souverain, les postières et postiers ont pu maintenir leur activité. Le taux de télétravail à La Poste demeure élevé depuis mars 2020 : seule une petite proportion de nos collaborateurs se rend actuellement dans nos locaux. La plupart des métiers que l'on pensait impossibles à réaliser à distance se sont finalement adaptés au télétravail. Certains métiers de la Banque postale l'ont illustré. Le département comptabilité de La Poste emploie 600 personnes qui, du jour au lendemain, contre toute attente, ont poursuivi leur activité depuis leur domicile.

Nous avons acquis, à la faveur de la crise sanitaire, la capacité de faire fonctionner la nouvelle branche grand public et numérique du groupe. Au début de cette crise, notre réseau historique a subi ce que j'appellerai une réduction de la voilure. Même en appliquant les gestes barrière et les mesures de confinement, ce réseau reste aujourd'hui entièrement ouvert. Le groupe combine, comme le veut son histoire, des activités nécessitant une présence physique, sans lesquelles il cesserait de fonctionner, et des activités réalisables à distance. En résumé, la crise sanitaire, si elle n'a pas empêché la poursuite de notre activité, a tout de même changé notre manière de travailler.

M. Olivier Vallet. Le premier confinement a fortement impacté les clients de Docaposte. Certaines entreprises n'ayant pas suffisamment dématérialisé ne serait-ce que leurs processus de recrutement ou de signature se sont retrouvées paralysées. Nous avons noté une forte accélération des usages du numérique à l'issue de la première période de confinement. La demande de services de signature électronique et de dématérialisation des démarches liées aux ressources humaines ou à la facturation a littéralement explosé, entre autres en raison des problèmes de trésorerie des entreprises. Ces services ont connu une croissance de 30% à 50% alors que d'autres, plus traditionnels, comme le traitement de chèques, ont reculé de 20% à 30%.

Les entreprises ont pris conscience de la nécessité d'accélérer leur transformation numérique. Docaposte a développé beaucoup de solutions destinées aux PME ou aux très petites entreprises (TPE) confrontées à l'enjeu crucial de la numérisation de leurs processus. Nous avons mis en place des offres gratuites pour les aider à l'issue du premier confinement. Citons parmi nos initiatives : une plateforme numérique de livraison de masques s'appuyant sur la capacité logistique du groupe La Poste, ou encore une application qui a permis de désengorger la ligne du SAMU (le Service médical d'aide urgente, joignable par le 15). Nommée « maladiecoronavirus.fr », et développée en partenariat avec une *start-up* et d'autres sociétés œuvrant dans le domaine de l'Intelligence artificielle, cette application permettait à l'utilisateur d'évaluer son état de santé afin de l'encourager, soit à composer le 15, soit à contacter son médecin traitant, soit encore à rester chez lui. Nous y avons dénombré plus de douze ou quinze millions de connexions. En somme, nous avons essayé de nous rendre utiles en cette période difficile.

En conclusion, depuis trois à cinq ans, le besoin de passer au numérique, en forte hausse chez les entreprises et les administrations, continue de se manifester au quotidien.

M. Gabriel de Brosses. L'État et l'ANSSI ont fortement soutenu l'emploi de solutions numériques.

Les phases de confinement nous ont donné l'occasion de constater, avec le plus grand intérêt, que la combinaison des solutions numériques dont nous disposions, comme la signature électronique ou encore la lettre recommandée électronique, permettait de répondre à un ensemble de besoins et de rendre des services requérant jusque-là une présence physique. L'association de notre solution d'identité numérique avec celle d'authentification du recommandé électronique, validée par l'ANSSI, a séduit une clientèle qui n'aurait pas pu, auparavant, adhérer à nos services à distance. Le confinement s'est en somme avéré un formidable accélérateur de la numérisation par la création de nouveaux usages.

M. Olivier Vallet. Le groupe La Poste a commencé d'investir dans l'identité numérique dès 2018. Il nous a fallu plus de dix-huit mois de développements technologiques, d'investissements et de parcours avec l'ANSSI pour obtenir le label de niveau de sécurité substantiel au 1er janvier 2020. Jusqu'au premier confinement, un client souhaitant obtenir une identité numérique, une fois entamé un parcours en ligne, avait le choix entre un contrôle de son identité réalisé de visu lors d'un rendez-vous avec son facteur ou en bureau de poste. Comme le confinement interdisait de procéder à l'étape de vérification physique de l'identité, nous avons mis en place un parcours entièrement numérique validé par l'ANSSI.

Aujourd'hui, trois possibilités s'offrent ainsi à toute personne désireuse de se doter d'une identité numérique : une entrevue avec le facteur, un passage au bureau de poste ou un parcours 100% numérique. Cette identité peut être utilisée au quotidien dans n'importe quelle démarche à réaliser en ligne. Nous lancerons un plan de communication et une campagne de promotion de notre solution d'identité numérique à partir du 7 juin. Le personnel de l'ensemble des bureaux de poste encouragera les personnes qui s'y rendent à se doter d'une identité numérique. Nous développons aussi des usages postaux de cette identité numérique, qui permettra entre autres de retirer des colis.

En parallèle, nous menons des discussions dans le domaine bancaire autour des processus de vérification de l'identité des clients (*Know your customer* ou KYC) et de l'entrée en relation avec la clientèle. Les banques sont très demandeuses de solutions d'identité numérique.

J'en profite pour répondre à votre question sur notre modèle économique. Nous avons toujours clairement affiché la gratuité de l'identité numérique pour les particuliers. En revanche, nous la rendrons payante pour les entreprises qui proposent des biens ou des services au grand public. Cette identité numérique les aidera à réduire les fraudes ou améliorer leur connaissance de leur clientèle. Nous travaillons en partenariat avec FranceConnect et FranceConnect+. Nous aimerions qu'un certain nombre de démarches administratives encouragent l'utilisation d'une identité numérique, avec un niveau de sécurité substantiel, de manière à limiter la fraude et développer des usages, de sorte qu'un plus grand nombre de Français y adhèrent.

Le déploiement de la carte nationale d'identité électronique (CNIe) est en cours. Nous avons tissé un partenariat avec l'Imprimerie nationale, de manière à proposer une solution complète à chaque Français. Tout citoyen pourra, lors de la réception de sa CNIe, récupérer par lettre recommandée (papier ou numérique) un code PIN lui permettant de se créer une identité numérique en posant son téléphone contre la carte à puce logée dans sa CNIe. Nous attendons l'autorisation de l'État pour délivrer les codes PIN nécessaires, faute de quoi nous ne serons pas habilités à récupérer les informations contenues dans la CNIe. L'obtention par chaque Français d'une identité numérique en même temps que sa CNIe nous apparaît comme

une formidable opportunité pour nos concitoyens d'évoluer pleinement dans le monde numérique.

M. Philippe Latombe, rapporteur. Beaucoup d'entreprises utilisent votre coffre-fort numérique pour y stocker des documents dématérialisés tels que des bulletins de salaire. Avez-vous senti chez les sociétés qui composent votre clientèle une prise de conscience des enjeux de la cybersécurité ? La crise les a-t-elle sensibilisées aux risques cyber ? Exigent-elles de votre part des garanties ?

M. Olivier Vallet. Les entreprises apprécient vraiment de pouvoir compter sur notre coffre-fort labellisé « La Poste » pour stocker leurs données en France, sans que nous les utilisions à des fins mercantiles. L'obligation de conserver au moins cinquante ans certains documents attire les entreprises vers un opérateur comme Digiposte. Elles sont en effet certaines que, d'ici cinquante ans, son capital restera public et français. Salariés et directions des ressources humaines (DRH) prêtent une attention croissante au lieu et à la pérennité du stockage des bulletins de salaire.

M. Gabriel de Brosses. Le nombre de cyberattaques a quintuplé à partir du premier confinement, de même que le *phishing* (ou hameçonnage), utilisé en préalable à des attaques plus élaborées. En 2020, les entreprises, administrations et hôpitaux se sont révélés particulièrement victimes de cyberattaques. Il apparaît désormais impossible d'ignorer les préoccupations liées à la cybersécurité.

Dans l'exercice de mon métier, je n'ai plus à en expliquer l'importance. D'entrée de jeu, face à mes interlocuteurs, surgit la question des moyens à mettre en œuvre pour assurer cette cybersécurité. La Poste assume de plus en plus un rôle de prestataire vendant des contrats d'assurance cybersécurité. Nos clients témoignent d'exigences croissantes. Les certifications dont bénéficie notre groupe favorisent le développement de son activité de ce point de vue.

Le niveau de sécurité de notre identité numérique a été considéré comme substantiel en décembre 2019, mais cette reconnaissance ne vaut que pour trois ans. Nous devons donc sans cesse nous améliorer. En somme, la cybersécurité s'apparente à la pratique de la bicyclette : il est impossible de s'arrêter d'avancer, sous peine de tomber.

M. Olivier Vallet. Il apparaît crucial pour les opérateurs de solutions numériques, dans leurs relations avec l'État, de s'appuyer sur les compétences et les investissements seuls à même de répondre aux problèmes de cybersécurité. Beaucoup d'espaces numériques de travail (ENT) ont subi de cyberattaques, dernièrement. Le logiciel PRONOTE, qui nous appartient désormais et qui a conquis 60% du marché des collèges et des lycées, n'a pas rencontré de problème de ce type, non pas du fait d'une meilleure conception par rapport aux solutions concurrentes, mais parce que nous nous sommes appuyés sur le savoir-faire de notre groupe pour le protéger de tout risque cyber. Malheureusement, la plupart des ENT, gérés par de petites entreprises ancrées dans les territoires, ne disposaient pas de l'expertise nécessaire pour parer les cyberattaques.

Seuls des acteurs dotés de suffisamment de compétences en la matière, grâce à des investissements conséquents, semblent aujourd'hui en mesure de répondre aux enjeux de cybersécurité.

M. Philippe Latombe, rapporteur. La Poste constitue aujourd'hui une référence en matière de numérique auprès du grand public. À quel point jugez-vous nos concitoyens mûrs sur ce sujet ? Se sentent-ils de plus en plus concernés par le numérique ? Quelle distance nous sépare encore, en France, d'une complète acculturation au numérique ?

M. Olivier Vallet. La question nous préoccupe sérieusement. En France se manifestent, à propos du numérique, des doutes et des inquiétudes réelles, quoique compréhensibles. Avant de déployer une solution, il faudrait s'assurer qu'elle puisse s'étendre à l'ensemble du territoire, sous peine de se lancer dans une numérisation à deux vitesses.

La Poste vient de signer un partenariat technologique avec l'Institut national de recherche en sciences et technologies du numérique (Inria), tout en réfléchissant au rôle que le groupe pourrait jouer dans l'acculturation au numérique. Comment expliquer à nos concitoyens que le numérique ne s'oppose pas au monde physique et qu'ils peuvent mener leur vie numérique en toute sécurité ?

Nous en revenons à la question qui nous occupe aujourd'hui, de la souveraineté. Il faut créer la confiance en passant par l'inclusion, la formation, l'écoute et, sûrement aussi, par un travail éducatif à mener le plus tôt possible dans nos établissements scolaires.

Nous-mêmes ne parvenons pas toujours à exposer de manière assez convaincante les bénéfices des solutions que nous proposons. Les acteurs du numérique usent souvent d'un langage très technique pas forcément intelligible pour tout le monde. Nous devons mettre en avant les usages du numérique et leurs avantages, de même que la complémentarité entre les univers numérique et physique. La présence du groupe La Poste sur tout le territoire doit lui permettre de jouer un rôle d'accompagnement des Français en levant leurs doutes.

Tout le monde finira par mener une vie numérique, que nous le voulions ou non. Si chacun, en France, disposait d'un trousseau numérique souverain de confiance, peut-être les craintes qu'inspire le numérique finiraient-elles par se dissiper et son usage par se généraliser.

M. Gabriel de Brosses. La confiance dans le numérique dépend d'une bonne compréhension du sujet. Nous avons constaté un considérable illectronisme (ou illettrisme numérique) parmi la population. Beaucoup de nos concitoyens ne sont pas familiers du sujet.

La plupart des utilisateurs du numérique optent aujourd'hui pour les solutions que proposent les principaux acteurs du marché. Par défaut, ils ouvrent une messagerie sur Gmail ou chez Microsoft. Il est tentant, pour qui connaît mal un domaine, de se tourner vers des entreprises reconnues. Les solutions françaises souffrent d'un déficit de notoriété.

Le choix d'un trousseau numérique valable implique pourtant de discerner les acteurs dignes de confiance, sous peine que se pose, *in fine*, un véritable problème de cybersécurité. Ce point renvoie à la question de la publicité de notre offre numérique souveraine. Les outils sont disponibles. Seulement, nous nous heurtons aux difficultés de leur commercialisation. Or, si nos concitoyens ne s'embarquent pas dans une vie numérique, munis du bon viatique, c'est-à-dire s'ils passent par un portail à la fiabilité sujette à caution, il sera impossible de générer un cercle vertueux de protection de données souveraines.

M. Philippe Latombe, rapporteur. Selon vous, à quelle échéance l'identité numérique deviendra-t-elle une réalité quotidienne pour les citoyens français ? Cette identité numérique, tel un serpent de mer, s'est heurtée à des difficultés lors de sa conception comme de sa mise en œuvre. L'acculturation des Français au numérique n'apparaît d'ailleurs pas aisée. Quand pensez-vous que le marché de l'identité numérique parviendra à maturité ?

M. Olivier Vallet. Le groupe La Poste est en mesure à la fois d'encourager les Français à passer au numérique et de développer les usages postaux des nouvelles technologies. Nous sommes en contact avec l'ensemble des banques, conscientes des bénéfices que peut apporter

l'identité numérique en matière de mise en conformité avec les règlements bancaires mais aussi pour faciliter l'entrée en relation avec les clients.

Il faudrait quand même clairement savoir quels services de dématérialisation de l'État nécessiteront le recours à une identité numérique substantielle. Un grand nombre de démarches dématérialisées via FranceConnect n'exigent pas aujourd'hui un tel niveau de sécurité. Nous discutons beaucoup avec certains ministères, mais nous ne savons pas encore très bien quels services administratifs pourraient fonctionner, auprès des citoyens, comme un levier d'enrôlement. Le déploiement de la CNIe nous offre une formidable opportunité, qu'il serait dommage de manquer. Chaque Français pourrait associer à un document d'identification matériel une identité numérique lui permettant de mener sa vie numérique en toute sécurité dans le respect de notre souveraineté nationale.

M. Philippe Latombe, rapporteur. De nombreux acteurs de l'identité numérique que nous avons auditionnés nous ont confirmé que la communication d'un code PIN aux Français recevant leur CNIe pour qu'ils créent en même temps leur identité numérique donnerait une impulsion certaine aux usages du numérique.

Souhaiteriez-vous évoquer un sujet que nous n'aurions pas encore abordé ou mettre en avant un point particulier ?

M. Olivier Vallet. J'insisterai simplement sur le fait que La Poste, acteur public, dispose de solutions numériques souveraines et de confiance au service des citoyens et de l'État. Nous souhaitons, dans le cadre de cette relation de confiance, contribuer à la numérisation indispensable de notre pays.

M. Gabriel de Brosses. L'investissement dans l'écosystème des *start-up* cyber françaises, bien qu'indispensable à notre souveraineté numérique, si nous voulons notamment, pour y parvenir, recourir à des solutions françaises ou européennes, demeure malheureusement limité. Trop souvent, en phase de croissance (ou *scale-up*), une fois validée la viabilité de leur modèle économique, les *start-up* migrent à l'étranger en quête de nouveaux investissements. Nous peinons à conserver en France des sociétés proposant des solutions de cybersécurité souveraines, ce qui oblige à s'interroger sur la pérennité des solutions envisagées pour sécuriser des systèmes d'information. Si nous optons aujourd'hui pour une solution souveraine, rien ne nous garantit que, d'ici trois ou quatre ans, le rachat, dans l'intervalle, des entreprises qui les proposaient, ne nous conduira pas à des discussions avec le Service de l'information stratégique et de la sécurité économiques (Sisse) du ministère de l'économie, des finances et de la relance.

M. Philippe Latombe, rapporteur. Au-delà du domaine de la cybersécurité, existe-t-il, au sein du groupe la Poste, des dispositifs ou des programmes favorisant l'éclosion de *start-up* ou leur croissance ?

M. Olivier Vallet. Notre programme French IoT donne l'opportunité à des *start-up* de se développer et de grandir, moins sur le plan financier, puisque ces sociétés parviennent assez facilement à lever des fonds, qu'en termes d'infrastructures, pour leur permettre de développer plus rapidement leurs offres. Surtout, nous les mettons en relation avec un écosystème d'industriels qui les assistent.

Tous les ans, nous définissons des thématiques en résonance avec la stratégie de La Poste. D'autres acteurs, de grandes entreprises, notamment, se joignent à nous pour faciliter le développement des candidats sélectionnés, parmi lesquels nous désignons un lauréat.

Auparavant, nous les emmenions à Las Vegas. Sans doute les accompagnerons-nous bientôt à VivaTech.

Depuis dix-huit mois, nous obligeons les *start-up* intéressées par notre programme French IoT à se présenter en tant que binômes composés d'un homme et d'une femme, de manière à encourager la féminisation des métiers du numérique.

M. Gabriel de Brosses. La plateforme de la banque postale, platform58, a incubé notamment YesWeHack, une société de *bug bounty* (ou recherche de vulnérabilités) qui fonctionne très bien. CNP assurances a investi entre autres dans la société Egerie. Nous pourrions aussi évoquer, toujours dans le domaine de la cybersécurité, les initiatives prises par notre actionnaire, la Caisse des dépôts et consignations, *via* Bpifrance (banque publique d'investissement).

Audition, ouverte à la presse, de Mme Corinne Caillaud, directrice des affaires extérieures, publiques et juridiques, membre du comité exécutif, et M. Jean-Renaud Roy, directeur des affaires institutionnelles, de Microsoft France
(27 mai 2021)

Présidence de M. Philippe Latombe, rapporteur.

M. Philippe Latombe, président et rapporteur. Je vous remercie pour votre participation aux travaux de notre mission d'information.

Microsoft est une multinationale informatique et microinformatique américaine, fondée en 1975 par Bill Gates et Paul Allen et présidée aujourd'hui par Satya Nadella. Son activité principale consiste à développer et vendre des systèmes d'exploitation, des logiciels et des produits matériels dérivés, ainsi que des solutions *cloud* (Azure), web (Bing, LinkedIn, Outlook) et des consoles de jeux vidéo.

Fondée en 1983 par sept collaborateurs, Microsoft France fut l'une des premières filiales de Microsoft à être créée dans le monde. 37 ans plus tard, Microsoft compte environ 1 800 collaborateurs en France, principalement localisés sur le campus d'Issy-les-Moulineaux.

Je souhaiterais vous poser trois questions.

La première concerne votre conception de la notion de souveraineté numérique en tant qu'acteur américain opérant en France. Cette question procède de la grande diversité des définitions qui peuvent exister de cette notion. Comment la définissez-vous et comment l'intégrez-vous dans les solutions que vous offrez à vos clients ?

Je souhaite ensuite vous interroger sur votre partenariat avec le Health Data Hub, qui a soulevé de nombreuses questions quant à votre capacité à sécuriser les données de ce dernier. Les auditions menées jusqu'à présent ont par ailleurs donné lieu à des positions différentes sur la soumission ou non d'entreprises américaines opérant en France au *Cloud Act* américain. Nous souhaiterions donc recueillir votre vision sur ces sujets.

Je souhaite enfin aborder avec vous le sujet de la formation. Quels sont les grands projets menés par Microsoft France dans le domaine de la recherche ? Comment Microsoft France participe-t-elle au développement en France d'un vivier de talents du numérique ?

Mme Corinne Caillaud, directrice des affaires extérieures, publiques et juridiques, membre du comité exécutif de Microsoft France. Je n'ai pas d'éléments à ajouter à la présentation faite de Microsoft France, si ce n'est à souligner notre engagement en France : nous animons un écosystème de 3 500 *start-up* et de 10 500 entreprises partenaires, distributeurs, intégrateurs. Cela représente environ 80 000 employés en France. Je laisserai la parole à M. Jean-Renaud Roy pour répondre à votre première question sur la notion de souveraineté numérique.

M. Jean-Renaud Roy, directeur des affaires institutionnelles de Microsoft France. Il existe la souveraineté numérique et la souveraineté numérique par les actes. Orange et Capgemini ont annoncé ce matin la création d'une nouvelle entreprise, Bleu, qui concourra pour obtenir la certification de *cloud* de confiance du gouvernement. Ce *cloud* de confiance sera basé sur les technologies hyperscale et *cloud* de Microsoft. Cela est nouveau et unique, pour Microsoft, de livrer ses technologies dans la confiance à deux partenaires de rangs mondiaux afin de répondre à des besoins très spécifiques en France.

La société créée par Orange et Capgemini ne réunira que des investisseurs et des capitaux français. Elle sera de droit français et ne fournira de services qu'en France. Microsoft licenciera sa technologie à travers un accord commercial. Ce cadre juridique est conforme aux annonces faites le 17 mai par le gouvernement et l'agence nationale de la sécurité des systèmes d'information (ANSSI). Ce cadre fonde l'immunité de cette société à l'exposition aux lois extraterritoriales, américaines mais pas seulement. De fait, en licenciant la technologie employée au sein de cette nouvelle entreprise créée très prochainement, Microsoft n'aura pas accès à l'infrastructure de ce *cloud* de confiance français. L'ensemble des technologies hyperscale seront les mêmes que celles que Microsoft distribue dans son *cloud* hyperscale à l'échelle mondiale, avec le même niveau de service, mais seront totalement détachées de notre propre infrastructure.

Revenant à la notion de souveraineté elle-même, je ne pense pas qu'une entreprise privée soit légitime pour définir la souveraineté – c'est le rôle du législateur et l'expression d'une volonté collective. En revanche, notre rôle, en tant qu'entreprise fournissant des solutions technologiques – aujourd'hui majoritairement centrées sur le *cloud* et les technologies intelligentes – est de mettre au service d'une puissance publique adossée à un État de droit une forme de savoir-faire qui permet de garantir des conditions de souveraineté, de résilience et de cybersécurité telles que cet État (ou cet ensemble d'États dans le cas de l'Union européenne) les aura définies. Il s'agit donc pour nous de nous adapter à un État qui édicte ses règles de protection des données et ses usages. Grâce à son réseau de plus de 10 000 partenaires en France (qui regroupe aussi bien des intégrateurs que des revendeurs), Microsoft permet à la souveraineté du droit de s'exercer, comme dans le cas de l'application du Règlement général sur la protection des données (RGPD).

Le premier aspect de la souveraineté pour un État, surtout dans le cyberespace, est de conserver sa capacité à contrôler et à appliquer les règles dans le temps et dans l'espace. Le numérique s'affranchit des frontières géographiques : même dans le cyberespace, les États ont besoin d'assurer leur souveraineté. Le RGPD par exemple est une réglementation qui permet d'assurer la protection des données personnelles des Européens au-delà des frontières européennes. La souveraineté s'exerce ainsi bien au-delà des frontières des États. L'application du droit dans le cyberespace me semble donc être le premier critère de souveraineté pour un État. Nous y participons en tant qu'acteur numérique du cyberespace. L'État n'a pas seul la capacité de gérer le cyberespace. Il doit le faire avec nous. Quand un État subit une cyberattaque, Microsoft est en première ligne. Microsoft est présent dans le tissu industriel et institutionnel et équipe beaucoup d'acteurs. Nous avons toujours souhaité nous engager aux côtés des États pour réguler et maintenir la sécurité dans le cyberespace, car la première souveraineté est de garantir la sécurité des personnes et de leurs biens, la résilience des États et des institutions démocratiques. Microsoft a soutenu l'Appel de Paris pour la sécurité dans le cyberespace en novembre 2020. Nous sommes l'une des premières entreprises à l'avoir fait et à avoir milité auprès de nombre d'écosystèmes numériques pour revendiquer l'importance de cet appel.

Par ailleurs, la notion de souveraineté peut varier d'un espace géographique à l'autre. L'Europe se questionne ainsi sur l'émergence d'une troisième voie qui lui serait propre en matière de protection des données personnelles. Avec le RGPD, l'Europe a édité le standard mondial de référence en matière de protection des données. Cela est une très bonne chose. Nous appliquons les règles du RGPD aux personnes et à nos personnels dans le monde entier. Cela montre notre engagement. Cela montre également que le RGPD constitue une opportunité pour nous de gagner la confiance de nos clients, partenaires et utilisateurs.

Compte tenu de la jurisprudence européenne récente, comme l'arrêt *Schrems* II qui a mis fin au *privacy shield*, nous avons annoncé, il y a quinze jours, mettre en œuvre une frontière européenne des données. Cela permettra à nos clients européens, conformément aux annonces faites par le commissaire européen, M. Thierry Breton, de traiter et de stocker leurs données en Europe, mais aussi d'en assurer le support à partir des territoires européens – cela est tout à fait nouveau – et donc, si ces clients le souhaitent, d'empêcher tout transfert de données en dehors du territoire européen. Je précise que ce projet ne traite pas de la question de l'extraterritorialité du droit, et notamment du droit américain en Europe. À ce sujet en revanche, nous avons aujourd'hui franchi un nouveau cap sous la forme du partenariat proposé par Orange et Capgemini, qui consiste en la création d'un *cloud* de confiance qui permettra l'immunité aux lois extraterritoriales, d'où qu'elles proviennent.

M. Philippe Latombe, rapporteur. Vous avez expliqué la nouvelle architecture juridique présidant à la création de Bleu : la société sera opérée par Orange et un de ses partenaires, qui seront majoritaires au capital. Microsoft sera, lui, fournisseur de licence.

M. Jean-Renaud Roy. Oui, nous concluons un accord commercial pour lequel nous fournirons la licence d'utilisation des technologies Microsoft.

M. Philippe Latombe, rapporteur. Cela signifie que cette solution permet de s'affranchir juridiquement de l'extraterritorialité du droit américain, car vous êtes fournisseur de licence.

M. Jean-Renaud Roy. Absolument.

M. Philippe Latombe, rapporteur. *A contrario*, cela montre que le Health Data Hub – qui fait écho à l'ensemble des débats tenus sur l'extraterritorialité américaine dans le cas de l'utilisation de votre *cloud* Microsoft Azure et de l'ensemble des *clouds* américains – est bien soumis à l'extraterritorialité américaine.

M. Jean-Renaud Roy. Nous n'avons jamais dit que nous ne l'étions pas. Nous sommes tout à fait soumis à l'extraterritorialité américaine.

M. Philippe Latombe, rapporteur. Je pose la question car il a été affirmé à plusieurs reprises, et notamment par la directrice du Health Data Hub, que nous disposions des moyens juridiques pour sécuriser l'ensemble du processus. Elle a affirmé qu'en stockant les données en Europe, en les opérant avec des clés sécurisées et en obtenant des garanties juridiques supplémentaires, nous nous affranchissions de tout risque d'extraterritorialité du droit américain. Je préfère donc que l'on précise les choses, d'autant que nous avons eu à ce sujet des opinions très divergentes : IBM nous a expliqué que puisque IBM France était une société par actions simplifiée française, elle n'était pas soumise au *Cloud Act* et à toute l'extraterritorialité du droit. La seule solution juridique valide que vous ayez trouvée aujourd'hui pour répondre au *Cloud Act* et à l'invalidation du *privacy shield* est donc d'opérer sous forme de licence ?

M. Jean-Renaud Roy. Non. Quand Mme Stéphanie Combes explique que la mise en œuvre de l'hébergement du Health Data Hub par Microsoft est garantie et permet de se soustraire aux lois extraterritoriales et au *Cloud Act*, c'est aussi car le champ d'application de ces lois extraterritoriales ne correspond pas aux activités du Health Data Hub aujourd'hui. Tout simplement. Les raisons au titre desquelles un juge américain peut lancer un mandat sous *Cloud Act* ne coïncident pas avec les activités du Health Data Hub.

Il faut savoir de quoi l'on parle, et pourquoi nous avons conclu cet accord avec Orange et Capgemini. Il s'agit, par cet accord, de répondre aux besoins de clients ayant des besoins très spécifiques en matière de résilience, de sécurité, de gestion de données sensibles. Les objectifs de GAIA-X sont la gestion des données sensibles des Européens.

Tout un espace du *cloud* est, formellement, au titre du droit, éventuellement exposé à une juridiction américaine – mais il n'en fera pas l'objet, car cela ne sert à rien, au titre du *Cloud Act*, d'aller rechercher une donnée de santé anonymisée, dont on ne sait rien faire et qu'on ne peut pas déchiffrer. Oui, sur le principe, nous sommes exposés à l'extraterritorialité, mais, dans la pratique, cela ne peut arriver.

L'application des lois extraterritoriales américaines ne peut pas nous viser pour plusieurs raisons. Tout d'abord, certains éléments nous font dire que la décision *Schrems* II ne s'appliquera pas au Health Data Hub. Ce point est très important. Ensuite, chaque loi extraterritoriale dispose d'un champ d'application propre : celui-ci permet au juge américain de se saisir d'un mandat en poursuivant un objectif. Rien ne concerne aujourd'hui le Health Data Hub dans les champs d'application des trois types de mandats existant et ouvrant la possibilité à la justice américaine de saisir des données par un exercice extraterritorial de ses fonctions *(Cloud Act, Foreign Intelligence Surveillance Act, Executive Order 12333)*. Cela est notre point de vue. De fait, Mme Stéphanie Combes a raison en affirmant que le Health Data Hub n'est pas concerné par le *Cloud Act*.

J'illustrerai mon propos par des exemples. Le *Cloud Act* nécessite que les données soient hébergées par Microsoft, qu'elles soient en notre possession, sous notre garde et notre contrôle. Les données du Health Data Hub ne sont pas en notre possession : elles sont sous notre garde, mais pas sous notre contrôle. De plus, elles sont chiffrées. En outre, pour être exposé au *Cloud Act*, il faut que le mandat spécifique concerne une personne visée par une enquête criminelle. Je ne vois pas comment un mandat – qui doit concerner une personne donnée, pour un crime donné – pourrait être édité au titre du *Cloud Act* afin d'accéder à des données anonymisées. Il faudrait, pour reconstituer ces données, disposer des bases de données originales et déchiffrées de la Caisse nationale de l'assurance maladie (CNAM) et du Health Data Hub. La reconstitution est donc très compliquée. Le Health Data Hub rassemble donc des données de santé qui n'entrent pas dans le champ d'une enquête criminelle du *Cloud Act*.

L'article 702 du *Foreign Intelligence Surveillance Act (FISA)* permet la surveillance ciblée d'une personne étrangère, à l'extérieur des États-Unis. Cela est important : cette définition a l'air très offensive et problématique en matière de souveraineté – je peux le comprendre. La cible du *FISA* est la surveillance d'un agent d'une puissance étrangère qui n'est pas un allié des États-Unis. La France est un allié des États-Unis et le Health Data Hub n'est pas un agent d'une puissance étrangère, tel que le définit le droit américain. L'article 702 du *FISA* cible le terrorisme (terrorisme international, activité clandestine de renseignement, prolifération d'armes). Le Health Data Hub ne sert à rien de tout cela. Il ne rentre donc pas dans le champ d'application de l'article 702 du *FISA*.

Le décret présidentiel *Executive Order 12333* permet d'exiger la transmission de données en dehors des États-Unis et peut conférer à une autorité américaine le pouvoir de mener des activités de renseignement. Je comprends que cela puisse soulever beaucoup de questions. Il faut tout de même reconnaître la transparence des États-Unis dans l'exercice de ces activités de renseignement : ces dispositions sont prévues dans leur droit. Un fondement légal est nécessaire pour qu'une entreprise, dans notre cas Microsoft ou même le Health Data Hub, soit sommée de fournir des renseignements. Ce décret présidentiel vise à l'acquisition de renseignements importants pour la détection d'activités terroristes internationales, de prolifération d'armes de destruction massive et d'espionnage menées par des puissances

étrangères de manière offensive contre les États-Unis. Franchement, les données contenues dans le Health Data Hub n'ont absolument rien à voir avec le champ d'application de ces trois lois extraterritoriales.

Enfin, nous pensons que la décision *Schrems* II ne s'applique pas au Health Data Hub. Le Conseil d'État a affirmé que la manière dont Microsoft a hébergé le Health Data Hub ne contrevenait absolument pas au RGPD même dans le cadre de la jurisprudence Schrems II. En fait, la décision *Schrems* II concerne le transfert de données d'une entreprise au sein de cette même entreprise, entre une filiale en Europe et une filiale aux États-Unis. Microsoft n'est que le pourvoyeur de la plateforme technologique d'hébergement du Health Data Hub. Le Health Data Hub a été construit par-dessus, comme une plateforme programmable totalement indépendante. Le Health Data Hub n'a pas d'entité juridique aux États-Unis, donc le Health Data Hub n'a pas à transférer de données vers les États-Unis. De fait, la décision *Schrems* II ne s'applique pas à notre cas et n'a pas de conséquence directe sur le fait que le Health Data Hub héberge ses données sur le *cloud* Microsoft en France.

M. Philippe Latombe, rapporteur. Je me permets une remarque un peu acide. Vous avez insisté sur le fait que chaque activité extraterritoriale américaine repose sur une base juridique. Rappelons-nous les écoutes massives opérées par la *National Security Agency (NSA)* et notamment la mise sur écoute de la chancelière allemande. L'Allemagne était pourtant une alliée des États-Unis. Cela génère des questions dans l'esprit de tout le monde. Ces questions ne sont peut-être pas réelles mais elles sont au moins légitimes.

M. Jean-Renaud Roy. Absolument.

M. Philippe Latombe, rapporteur. S'agissant de *Schrems* II, le Conseil d'État a également intégré à sa décision le fait que le gouvernement l'avait très rapidement informé que le Health Data Hub allait quitter le *cloud* Microsoft. C'est une des raisons pour lesquelles le Conseil d'État a rendu une décision dans ce sens-là. Le principe était bien la sortie du *cloud* Microsoft. Cela a été confirmé il y a quelques jours par le gouvernement – à l'inverse de ce qu'avait affirmé Mme Stéphanie Combes, en audition publique ici-même. Selon Mme Stéphanie Combes, le courrier fourni par le ministre de la santé au Conseil d'État et la prise de position de Cédric O devant les sénateurs n'allaient pas dans le sens de la sortie du *cloud* Microsoft – cela n'est pas vrai, et cela a été clarifié depuis.

Même si selon vous, *Schrems* II ne s'applique pas au Health Data Hub, un embarras persiste. Comment appliquer *Schrems* II pour respecter le droit européen et assurer la sécurité des données vis-à-vis du droit extraterritorial ? En quoi Bleu répond-il à cette question et les précédentes solutions n'y répondaient pas ?

M. Jean-Renaud Roy. Encore une fois, nous n'avons jamais affirmé ne pas être soumis aux lois extraterritoriales. Nous sommes une entreprise de droit américain, nous sommes soumis à la législation américaine. Je n'ai aucun problème avec cela et je suis totalement ouvert à ce sujet.

Nous mettons en œuvre des dispositions pour répondre aux exigences de la législation américaine et aux besoins de nos clients. Le *Cloud Act* a été émis suite à une contestation de la part de Microsoft d'une demande – qui ne nous semblait pas légitime – des autorités américaines d'accéder à des données situées dans un *data center* en Irlande. Nous sommes allées jusqu'à la Cour suprême pour cela. Nous savons donc aussi rejeter ce qui est illégal et défendre nos entreprises.

M. Philippe Latombe, rapporteur. Quand avez-vous commencé à travailler avec le Health Data Hub ? Votre collaboration n'a pas été scellée au terme d'un appel d'offres mais par un contrat. Avez-vous commencé à travailler avec le Health Data Hub préalablement à la signature de ce contrat, notamment pour la constitution de l'architecture de la plateforme ?

M. Jean-Renaud Roy. Non. Nous avons pris les premiers contacts avec le Health Data Hub au moment du rendu des travaux de la mission de préfiguration. Si ma mémoire est bonne, cela a eu lieu en octobre 2018.

Je sais d'où vient cette question. J'ai vu sur les réseaux sociaux que certaines personnes avaient consulté les registres de la Haute autorité pour la transparence de la vie publique (HATVP), où les personnes comme moi doivent répertorier leurs rencontres avec les représentants de l'État et des autorités publiques. Si l'on regarde bien le registre de la HATVP, il me semble que nous sommes la seule entreprise à avoir déclaré avoir rencontré le cabinet ministériel et le Health Data Hub après la mission de préfiguration. Je vous invite à le vérifier.

M. Philippe Latombe, rapporteur. Très bien. Il n'y a pas de critique de ma part à ce sujet. Je souhaitais simplement poser les faits.

Dans votre propos liminaire, vous avez affirmé que la souveraineté n'était pas l'apanage des sociétés privées – et *a fortiori* américaines – et qu'il appartenait plutôt à la puissance publique de la définir. La souveraineté est-elle un argument commercial en ce moment ? Votre site Internet propose un chapitre entier sur la souveraineté des données sur Azure et Azure Stack.

M. Jean-Renaud Roy. Nous définissons les offres souveraines en fonction des besoins exprimés par nos clients et du cadre réglementaire en vigueur, là où nous vendons le produit. L'Europe porte une attention toute particulière à sa souveraineté. Elle édicte des lois en matière de protection des données personnelles et de cybersécurité. Il est évident que la souveraineté fait partie des solutions qu'un acteur de notre taille est obligé d'appréhender, y compris d'un point de vue commercial, car nous répondons aux besoins de nos clients. Les besoins évoluent.

À l'époque, l'on ne parlait que du logiciel et l'on avait l'habitude de dire qu'il existait sept couches d'abstraction de souveraineté : le *hardware*, le *language machine*, le *software*, le système d'exploitation, le logiciel, etc. Il est normal que les pays qui ne maîtrisent pas l'ensemble de ces technologies portent une attention aigüe à la souveraineté. C'est le cas également des États-Unis, car le *hardware* et les puces électroniques sont construits en Asie.

Avec la crise sanitaire, les technologies *cloud* ont connu un très grand essor car elles ont permis la résilience des populations et de l'économie. Il est normal que l'attention aux questions de souveraineté porte aujourd'hui davantage sur ces technologies. Peut-être que demain, l'attention à la souveraineté portera sur l'informatique quantique.

M. Philippe Latombe, rapporteur. Le mot souveraineté, aujourd'hui utilisé dans beaucoup de sujets différents (souveraineté industrielle, souveraineté des médicaments, par exemple), n'est-il pas devenu essentiellement un argument marketing ? Y'a-t-il, de la part de vos clients, de vrais intérêts et besoins en matière de souveraineté, accompagnés de demandes précises à ce sujet ?

M. Jean-Renaud Roy. La création de Bleu est le résultat d'un dialogue avec nos clients, qui ont exprimé des besoins très spécifiques en matière de souveraineté, de sécurité et de résilience. Il existe un marché important pour le *cloud* souverain. Il ne s'agit pas seulement d'un argument marketing. Bleu met en place des solutions techniques. Certes, la labellisation

en *cloud* de confiance répond à certains impératifs juridiques, mais nous menons surtout un important travail d'ingénierie. Nous créons quelque chose de complètement nouveau, qui demande beaucoup d'investissements. Nous ne le ferions pas, s'il s'agissait seulement de développer un argument marketing. Nous le faisons car notre offre répond à un besoin.

Vous avez récemment reçu en audition les représentants du Club informatique des grandes entreprises françaises (Cigref). Ils ont exprimé leurs besoins en matière de souveraineté. Leur souveraineté ne se définit pas comme l'exclusion des technologies non européennes ou non françaises, mais comme la possibilité d'utiliser des technologies extérieures (notamment américaines) en toute compatibilité avec la protection des données, le droit européen, les valeurs européennes. C'est ce que nous sommes en train de faire.

M. Philippe Latombe, rapporteur. Le gouvernement a récemment communiqué sur deux thèmes et je voudrais recueillir votre opinion à cet égard. Des communications ont été faites suite au rapport présenté par M. Éric Bothorel sur les logiciels libres. Quelle est votre opinion à ce sujet ? L'Éducation nationale dit promouvoir les logiciels libres, mais en même temps travaille notamment avec vous. Jusqu'où peut-on aller en matière de logiciel libre ? Comment analysez-vous la trajectoire du gouvernement sur ce sujet ?

L'État a mis en place une stratégie *cloud* pour les administrations centrales. Qu'en est-il des collectivités territoriales, par exemple pour les *smart cities* ? Certaines de vos solutions pourraient-elles répondre aux besoins définis par l'État dans sa stratégie *cloud* en la matière ?

M. Jean-Renaud Roy. Si le *cloud* de Microsoft répond aujourd'hui aux besoins de l'État, c'est parce que le *cloud* est une plateforme agnostique sur laquelle il est possible de faire ce que l'on veut (utiliser de l'*open source*, des logiciels propriétaires, ou développer ses propres logiciels).

Nous sommes capables, si l'État le souhaite, de répondre à l'ensemble des besoins énoncés dans sa stratégie *cloud*. Mais l'État peut aussi développer ses propres solutions à partir d'un cloud public comme le nôtre. Le *cloud* public est important : il permet des effets d'échelle très importants et une élasticité à la demande, notamment en matière de puissance. Les choix sont ouverts. La France offre, grâce à son écosystème, le plus grand nombre d'offres et d'approches du *cloud*.

La marketplace de Microsoft accueille également les éditeurs de logiciel de tierces parties, et notamment des éditeurs français. Cela permet de projeter cette offre dans le *cloud* et à l'étranger. Nous accueillons donc tout un écosystème à l'intérieur de la marketplace de notre *cloud* Azure.

M. Philippe Latombe, rapporteur. Et le logiciel libre ?

M. Jean-Renaud Roy. Microsoft est aujourd'hui le premier contributeur mondial dans le logiciel libre. À l'échelle mondiale, près de la moitié des machines virtuelles installées dans notre *cloud* sont *open source*. Comme vous le savez, nous avons racheté GitHub, entreprise de développement de logiciels *open source*. Nous avons également rejoint la fondation Linux.

Microsoft a souvent été vu comme le grand détracteur de l'*open source* et du logiciel libre. Les dirigeants de Microsoft ont récemment reconnu que cette position constituait une erreur stratégique. Aujourd'hui, Microsoft considère que ses clients choisiront le mode d'utilisation qui leur conviendra le mieux, *open source* ou non – c'est le mode de distribution qui fait la différence.

M. Philippe Latombe, rapporteur. Je dresserai un parallèle avec la barre de recherche Google sur les téléphones portables. Il a fallu légiférer pour exiger que la barre de recherche Google ne soit pas systématiquement imposée aux consommateurs dans les téléphones. S'agissant du *hardware*, un certain nombre de PC sont systématiquement proposés avec Microsoft. Cela est-il le fait de partenariats mondiaux ou cela est-il décidé par région ? Une réglementation similaire à celle visant la barre de recherches Google vous poserait-elle problème ? Ces demandes de dissocier le *hardware* de l'exploitation sont portées par un certain nombre d'associations de consommateurs et d'usagers du numérique.

Mme Corinne Caillaud. Vous l'avez vous-même souligné : dans nos systèmes, les consommateurs ont le choix. Nous avons la volonté de proposer un choix pour l'installation du système d'exploitation. Les choix proposés se nouent sur la base de partenariats de développement. Il est clair que nous proposons et proposerons de façon constante ces choix. Il est possible aujourd'hui d'installer tout un choix de moteurs de recherches. Il s'agit de la même dynamique que l'*open source*. Nous souhaitons proposer une plateforme et la palette la plus large possible de propositions de solutions, afin de satisfaire les exigences des clients finaux.

M. Jean-Renaud Roy. Il est tout à fait possible de télécharger les distributions Linux avec Windows 10 et de les faire tourner de manière native. Cela progresse, et nous sommes les seuls à le faire. À travers nos ordinateurs, nous sommes donc aujourd'hui l'un des premiers vecteurs de diffusion de l'*open source* dans le monde.

M. Philippe Latombe, rapporteur. Merci de le préciser. Il s'agissait d'une question et non d'une critique.

Je souhaiterais maintenant aborder le sujet de la formation. Comment Microsoft se positionne-t-il en ce qui concerne la formation au numérique ? Je pense à la fois aux formations internes et externes.

Mme Corinne Caillaud. La formation et le développement des compétences numériques sont un des piliers majeurs et essentiels de Microsoft en France. Nous avons créé en 2018 les écoles IA, avec l'objectif de former 1 000 apprenants d'ici 2022. Nous disposons de 25 écoles IA et 16 sont en cours. Deux écoles *cloud* sont également en construction.

Nous sommes parti d'un double constat : il existe un vrai besoin en Intelligence artificielle et nous nous heurtons à l'absence de profils dits intermédiaires, notamment de techniciens. Cette formation est gratuite pour les demandeurs d'emploi et permet de devenir développeur en Intelligence artificielle.

Simplon est l'opérateur de cette formation depuis sa création. La pédagogie de Simplon est très active et axée sur les projets. Nous souhaitions une formation relativement courte et très orientée sur la demande, sur le marché de l'emploi. C'est une formation intensive de sept mois, suivis d'un an en alternance en entreprise. Ce partenariat inclut également Pôle Emploi, les régions et les entreprises. De nombreuses entreprises partenaires participent en intégrant ces écoles dans un cursus professionnel.

En 2019, la première formation était à 80% féminine. En 2020, elle incluait les intelligences atypiques avec une dizaine de profils Asperger.

Ces formations sont professionnalisantes : elles peuvent obtenir un titre de finalité professionnelle « développeur en Intelligence artificielle » avec un équivalent à bac+3.

Nous lançons cette année le programme des écoles *cloud* : nous accueillons deux promotions pilotes, toujours en partenariat avec Simplon, avec l'objectif de les former aux compétences de développeur technique et d'administrateur *cloud*.

M. Philippe Latombe, rapporteur. Ressentez-vous un changement dans l'intérêt des jeunes pour ce type de formation ? La féminisation des formations fonctionne-t-elle ?

Mme Corinne Caillaud. Nous évoluons dans la bonne direction. Mais il y a un énorme travail à faire en amont. Une fois que ces jeunes femmes ont postulé et intégré ces formations, le taux de réussite, de participation et d'engouement est extrêmement élevé. Mais il faut aller chercher ces jeunes femmes.

Les profils de techniciens manquent de femmes. Notre objectif est de sensibiliser les jeunes. Nous nous sommes ainsi appuyés sur l'association Unis-Cités pour lancer la mission « jeunes citoyens du numérique », qui a sensibilisé 19 000 jeunes aux compétences et aux formations numériques depuis 2018. Cet enjeu est critique pour les emplois du futur.

M. Jean-Renaud Roy. Nous avons été tant surpris par le succès de l'école IA que nous n'arrivons pas à répondre à la demande. L'État devrait aider les opérateurs comme Simplon à étendre ces formations.

Des besoins ont surgi, notamment en matière de transformation numérique des entreprises. L'objectif est de former une population capable de manier la data, d'entraîner à la data, de faire de l'Intelligence artificielle. Cela ouvre les perspectives pour les entreprises qui ne savent pas comment amorcer leur transformation numérique : des personnes très bien formées pourront répondre à leurs besoins. L'enjeu est de « matcher » ces personnes avec les entreprises, les plus matures comme les moins matures.

M. Philippe Latombe, rapporteur. La formation délivrée par Simplon est-elle agnostique ?

M. Jean-Renaud Roy. Tout à fait.

M. Philippe Latombe, rapporteur. D'autres formations non agnostiques connaissent-elles, elles aussi, une forte demande ? Des certifications pour les informaticiens existaient par le passé.

M. Jean-Renaud Roy. Elles existent toujours.

M. Philippe Latombe, rapporteur. Ces formations continuent-elles à attirer du public, ou y'a-t-il eu un déport des apprenants de ces formations vers les nouvelles formations délivrées par Simplon ?

M. Jean-Renaud Roy. Les deux cohabitent, car elles ne s'adressent pas au même public.

Il faut bien connaître le secteur pour se renseigner sur les formations Microsoft : elles visent des personnes ayant une appétence sérieuse sur ces sujets, qui savent déjà coder et veulent passer une certification pour se professionnaliser. Elles couvrent de très hauts degrés de technicité. Ces certifications sont liées à des technologies (pas seulement les technologies Microsoft).

Les écoles IA s'adressent à des personnes en recherche d'emploi, en reconversion professionnelle, qui ont des compétences en mathématiques et une appétence pour le code,

mais qui ne sont pas déjà formées à ces sujets. En revanche, les deux nouvelles écoles *cloud* recrutent à niveau bac.

M. Philippe Latombe, rapporteur. Souhaitez-vous aborder un sujet dont nous n'avons pas discuté jusqu'à présent ?

Mme Corinne Caillaud. À mes yeux, nous avons couvert l'essentiel des sujets que nous souhaitions vous présenter.

M. Philippe Latombe, rapporteur. Je vous poserai une dernière question. Quelle sera la place du numérique dans nos économies à moyen et long termes, et comment Microsoft se positionne-t-il ?

M. Jean-Renaud Roy. Le numérique n'est pas porté seulement par ceux qui le fabriquent et produisent des technologies. Nous allons par exemple développer une grande plateforme pour un constructeur automobile à partir du *cloud* de Microsoft. Ce constructeur utilisera cette plateforme pour rationaliser sa logistique, agencer ses relations avec ses fournisseurs, ses sous-traitants, ses concessionnaires. Il disposera donc d'une plateforme qui lui appartient et qu'il continuera de développer : il construira pour cela des compétences, notamment en matière de langages, de logiciels, de *frameworks*. Il continuera à proposer un service approfondi, agrémenté et mis à jour. Il va donc lui-même devenir une partie de l'offre du *cloud* : il deviendra un *cloud provider*.

Notre entreprise propose des moyens de production du numérique. À l'avenir, ces moyens de production du numérique pénétreront des industries qui ne sont pas numériques au départ, mais qui le deviendront, dans leurs modèles d'affaires et leurs manières d'opérer leur logistique, leurs circuits de vente, jusqu'à leur sécurité.

Audition, ouverte à la presse, de M. Arnaud Castaignet, directeur de la communication et des affaires publiques de Skeleton Technologies, ancien directeur des relations publiques du programme e-Residency du gouvernement estonien
(1er juin 2021)

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. M. Arnaud Castaignet est directeur de la communication et des affaires publiques de Skeleton Technologies, et ancien directeur des relations publiques du programme e-Residency du gouvernement estonien.

La création de la société Skeleton Technologies, spécialisée dans la fabrication de supercondensateurs, remonte à 2009. Si la technologie que cette entreprise a mise au point permet de stocker de l'énergie plus efficacement qu'une batterie classique, il convient de noter que les supercondensateurs se chargent et se déchargent aussi plus rapidement. Principalement utilisés à ce jour dans les batteries de voitures électriques, et devenus une référence dans l'industrie automobile, ces supercondensateurs marquent l'une des avancées technologiques majeures de ces vingt dernières années. L'entreprise Skeleton Technologies a connu une croissance exponentielle. Son chiffre d'affaires a triplé en 2019. Elle a enregistré plus de 100 millions d'euros de commandes.

M. Philippe Latombe, rapporteur. Je souhaiterais aborder trois sujets à titre liminaire.

Le premier n'est autre que votre conception de la notion de souveraineté numérique, question rituelle de nos auditions, procédant de la grande diversité de définitions données à ce concept. Comment l'appréhendez-vous ? Comment peut-elle se traduire concrètement en termes de politique publique ?

J'aimerais également qu'en tant qu'ancien directeur des relations publiques du programme e-Residency, vous nous parliez des politiques numériques menées en Estonie. Quelles raisons attribuez-vous à l'avance estonienne dans le domaine du numérique ? Comment jugez-vous l'action de l'Union européenne dans ce secteur ? Les vingt-sept États membres défendent parfois des positions différentes en la matière. L'Union européenne vous semble-t-elle capable de jouer un rôle de levier de souveraineté numérique pour les États somme toute assez divers qui la composent ?

J'aimerais enfin vous interroger sur vos fonctions actuelles au sein de la société Skeleton Technologies. Si les supercondensateurs sont pour l'heure surtout utilisés dans l'industrie automobile, il ne subsiste aucun doute qu'ils joueront à l'avenir un rôle stratégique majeur, à l'instar des semi-conducteurs. L'Europe vous semble-t-elle en mesure de prendre le virage technologique des supercondensateurs ? Les autres grandes puissances mondiales, dont les États-Unis et la Chine, ont-elles déjà pris de l'avance dans ce domaine ?

M. Arnaud Castaignet, directeur de la communication et des affaires publiques de Skeleton Technologies, ancien directeur des relations publiques du programme e-Residency du gouvernement estonien. J'occupe, dans l'entreprise estonienne Skeleton Technologies, le poste de directeur de la communication et des affaires publiques. Auparavant, j'ai travaillé pour le gouvernement estonien en lien avec le programme e-Residency. Avant cela, j'ai été chargé de communication numérique à l'Élysée sous la présidence de M. François

Hollande. J'ai donc évolué à la fois dans le secteur privé et dans le secteur public, en France comme en Estonie.

J'en ai tiré le constat qu'il n'existe pas, en matière de numérique, un seul modèle qui vaille. Chaque pays peut s'inspirer des autres, mais aussi s'avérer pour eux source d'inspiration. Ce que je dirai du modèle estonien du numérique n'implique pas que je l'estime supérieur au modèle français. De fait, il se heurte à des limites. La France comme l'Union européenne n'en gagneraient pas moins à s'en inspirer.

La question, fort intéressante, de la souveraineté numérique ne s'envisage pas de la même manière d'un pays à l'autre. La France reste sans doute le pays d'Europe à y avoir le plus réfléchi. Longtemps envisagée sous le seul angle du protectionnisme, cette question englobe désormais un champ beaucoup plus large. La meilleure définition, à mon sens, de la souveraineté numérique assimile cette notion à la capacité d'effectuer des choix en toute liberté. Je considère donc la souveraineté numérique synonyme d'autonomie stratégique, ce qui ne signifie pas qu'il faille à tout prix privilégier des solutions numériques françaises ou européennes. La coopération avec le reste du monde n'est pas à écarter *a priori*, à condition d'en décider librement et en toute connaissance de cause.

L'actualité de cette question s'explique par l'émergence de puissantes entreprises du numérique comme Google, Amazon, Facebook, Apple et Microsoft (les GAFAM). La notion de souveraineté numérique recoupe désormais de plus en plus celle de souveraineté industrielle, très liée à ces enjeux technologiques du futur, qui mêlent la science à l'innovation, tels que la 5G, la 6G (cinquième et sixième générations des standards pour la téléphonie mobile), l'ordinateur quantique ou les nouvelles solutions de stockage d'énergie. À très long terme, la question de la souveraineté numérique cédera toutefois la place aux débats sur l'autonomie stratégique, notion qui recoupe d'ailleurs celle d'indépendance industrielle.

Pourquoi l'Estonie constitue-t-elle un modèle intéressant en matière de numérique ? L'Américain Andrew Keen, dans son livre *How to fix the future*, identifie plusieurs modèles numériques étatiques différents de par le monde : le modèle chinois, le modèle russe, le modèle occidental, commun à la plupart des démocraties avancées, et enfin, le modèle estonien. Unique en son genre, ce modèle n'a été appliqué que dans un seul pays. Compte tenu des valeurs qui ont contribué à son émergence, il mériterait néanmoins de devenir plus influent à l'échelle européenne. Il repose en effet sur des principes apparentés à ceux de la France et de l'Europe, justifiant de s'y intéresser.

Le développement de la société numérique estonienne ne repose pas autant qu'on pourrait le penser sur des avancées technologiques. Le modèle numérique estonien mérite donc moins l'attention en raison de la technologie qui le soutient que du fait de la confiance sur laquelle il se fonde. Cette confiance, établie et à établir, entre l'administration et les citoyens, découle de la transparence, notamment de l'infrastructure, qu'il convient, il est vrai, d'attribuer à la technologie mise en œuvre. C'est cette transparence qui constitue la clé de compréhension du modèle numérique estonien.

Le développement continu du modèle numérique estonien a débuté voici une vingtaine d'années. Le lancement du premier programme numérique *Tiigrihüpe* ou *Tiger Leap* date de 1996. Ce programme avait pour objectif de raccorder toutes les écoles et les lycées du pays à Internet par l'achat d'ordinateurs et l'enseignement, aux élèves comme aux professeurs, du maniement des solutions numériques. À partir de là, chaque année, de nouveaux pans de l'administration se sont numérisés. L'Estonie a retrouvé son indépendance en 1991. Elle a dès lors dû construire *ex nihilo* toute son administration et n'a donc pas eu à numériser une structure déjà existante. Les services publics ont vu le jour sous une forme numérique au fur

et à mesure de leur naissance, ce qui explique que le modèle de l'infrastructure numérique estonienne ne soit pas forcément transposable tel quel partout dans le monde.

En 2000 a été créé un dispositif de déclaration et de paiement d'impôts en ligne. En 2001 a été mise en place une infrastructure, baptisée X-Road, essentielle à l'accès et à l'interopérabilité des données. L'année 2002 a coïncidé avec l'apparition de la carte d'identité numérique, reposant sur une technologie relativement simple, puisqu'une puce y autorise l'accès à un portail unique groupant l'ensemble des services publics. La même année a été proposée la signature numérique puis, en 2005, le vote en ligne. En 2010, ce sont les ordonnances médicales qui sont devenues disponibles en ligne. L'énumération pourrait encore se poursuivre.

La volonté de développer des services publics numériques fait l'objet d'un large consensus politique en Estonie. Pour cette raison, les plans d'action établis sur dix ans ne varient pas selon l'alternance des partis au pouvoir. Comme dans n'importe quel pays, le lancement d'un service public sous sa forme numérique ne signifie pas que l'ensemble de la population y adhère tout de suite. Seuls 5 % des électeurs ont voté en ligne lors de la première élection où cela leur était possible en 2007. En 2019, la proportion des citoyens à exprimer leur suffrage sous forme numérique était toutefois passée à 47 %.

Certains Estoniens continuent à effectuer leurs démarches comme avant l'ère numérique. Rien ne les oblige à recourir aux nouvelles technologies. Seulement, les démarches en ligne leur apparaissent plus faciles et pratiques, ce qui compte énormément à leurs yeux. Le lancement du dispositif de vote électronique n'avait pas pour objectif que 100 % des citoyens y recourent. Il visait uniquement à proposer aux électeurs une solution la plus facile possible d'utilisation.

Le modèle numérique estonien repose pour une part essentielle sur la notion de redevabilité mutuelle. Il s'agit là d'un élément clé de la confiance réciproque entre l'administration et les citoyens. Chaque interaction d'un citoyen estonien avec un service public implique l'usage d'une identité numérique unique, ce qui facilite la traque des abus. En contrepartie, tout usager de l'administration peut savoir qui a eu accès à ses données personnelles et à quel moment. La transparence s'exerce dans les deux sens. Constitue-t-elle un prérequis à la confiance ou en est-elle le fruit ? La question apparaît sujette à débat. En tout cas, l'enjeu des données personnelles ne porte pas, en Estonie, sur leur protection, entendue comme l'interdiction de les communiquer d'une administration à une autre, mais sur leur intégrité, à savoir l'usage qui leur est réservé.

En résumé, le modèle numérique estonien s'inscrit moins dans l'histoire des évolutions technologiques qu'il ne résulte de la construction d'une confiance réciproque entre l'administration et les administrés. L'infrastructure numérique mise en place n'a servi qu'à consolider cette confiance.

Pourquoi l'Estonie a-t-elle développé un modèle numérique innovant ? Pourquoi l'État a-t-il favorisé l'épanouissement d'une culture numérique et d'innovation à l'échelle du pays entier ? Le gouvernement estonien souhaitait avant tout créer puis fertiliser un écosystème favorable à l'émergence d'entreprises innovantes. L'Estonie est surtout connue pour son administration numérique et ses *start-up*, dont certaines se classent aujourd'hui parmi les plus importantes entreprises du pays. Le logiciel Skype a été en partie développé par un Estonien. Nous pourrions citer d'autres exemples de réussite plus récents, tels que Bolt, une entreprise de transport avec chauffeur sur le modèle d'Uber, TransferWise ou encore TomTom MyDrive. L'écosystème des *start-up* estoniennes a souvent manifesté la volonté de rendre à l'Estonie ce que le pays lui avait apporté. D'anciens employés ont ainsi créé leur propre entreprise, trouvant

des financements auprès de créateurs de sociétés ayant vendu la leur. L'écosystème estonien des *start-up* apparaît comme l'un des plus dynamiques d'Europe.

C'est d'ailleurs pour favoriser sa croissance que l'Estonie a lancé en 2014 le programme e-Residency. D'une grande simplicité, il offre une identité numérique estonienne à des ressortissants étrangers, à la fois dans une optique de *soft power* et, de manière plus pragmatique, pour favoriser la création d'entreprises en Estonie par des personnes qui, sans y vivre, ressentent le besoin et l'envie de bénéficier des services publics estoniens numérisés.

Les activités de Skeleton Technologies s'articulaient initialement autour du nanomatériau mis au point par ses créateurs, le graphène courbé (ou *curved graphene*). L'entreprise fabrique à partir de ce nanomatériau des supercondensateurs, parfois appelés ultracondensateurs. Ces dispositifs de stockage d'énergie s'apparentent assez aux batteries électriques, dont ils se distinguent toutefois par leur densité de puissance, souvent plus de soixante fois supérieure. Les supercondensateurs se heurtent toutefois à la limite de leur densité d'énergie, moindre que celle des batteries électriques. Les supercondensateurs sont donc souvent utilisés en complément de celles-ci, sans s'y substituer. Ils présentent l'avantage de ne pas comporter de lithium ni de cobalt ou autre métal rare toxique. Leur durée de vie dépasse en outre les quinze ans. Cette technologie, mise au point voici plusieurs décennies, n'a réussi à atteindre de performances notables que ces dernières années, notamment grâce aux avancées dans le champ des nanomatériaux.

La principale entreprise au monde à fabriquer des supercondensateurs se situe aux États-Unis et se nomme Maxwell Technologies. Tesla l'a rachetée voici un peu plus d'un an. Skeleton technologies, qui domine le marché européen des supercondensateurs, a donc pour principal concurrent Tesla. Au fur et à mesure des innovations qu'elle mettra au point, notre société produira des solutions aux propriétés de plus en plus proches de celles des batteries, notamment en lithium. Notre technologie est utilisée dans le secteur automobile et des transports au sens large (tramway, train ou bus) mais aussi dans le champ des énergies renouvelables, puisqu'elle offre une solution au problème posé par l'intermittence de ces énergies.

En termes de capital, notre entreprise se classe au deuxième rang, après Bolt, des sociétés ayant leur siège en Estonie. Nous avons en effet levé plus de 150 millions d'euros de fonds. L'intégralité de notre chaîne de production et de valeur se situe en Europe. Skeleton Technologies illustre le prochain défi qui se pose à l'Estonie : permettre, hors du domaine des logiciels, l'émergence de géants des nouvelles technologies à l'impact industriel suffisant pour créer des emplois à tous les niveaux de compétences. L'Estonie doit relever l'enjeu de créer des synergies entre ces sociétés en croissance et d'autres entreprises européennes plus traditionnelles.

La principale difficulté à laquelle se confronte l'Europe a trait à la réussite de son pari sur les technologies de demain, telles que les microprocesseurs, l'informatique quantique et l'Intelligence artificielle, mais surtout à sa capacité, par sa quête de souveraineté numérique et d'autonomie stratégique, d'initier des synergies entre les *start-up* et les secteurs qui constituent ses points forts, comme la santé, la mobilité, l'urbanisme et l'agriculture. De ces synergies émergeront les géants de l'innovation de demain, à même de soutenir la croissance de notre économie.

M. Philippe Latombe, rapporteur. Pourriez-vous préciser, à l'intention de nos auditeurs, en quoi consiste le programme e-Residency ? À quelle stratégie obéissait son lancement ?

M. Arnaud Castaignet Ce programme, unique au monde lorsqu'il a vu le jour, en 2014, propose à des non-résidents de disposer d'une identité numérique estonienne et de ses avantages. Il présente surtout l'intérêt, pour ceux qui y adhèrent, de pouvoir créer en quelques minutes une entreprise, dès lors gérable entièrement en ligne. L'État estonien y trouve comme intérêt de faire connaître l'Estonie et son modèle numérique auprès du plus grand nombre, tout en offrant des opportunités aux entreprises locales de services à d'autres sociétés.

Dans la pratique, tout entrepreneur, indépendamment de sa nationalité ou de son lieu de résidence, peut bénéficier des services numérisés de l'administration estonienne en devenant e-résident en Estonie. La société qu'il crée est européenne. Le programme a rencontré un certain succès, même s'il se heurte à des limites. On dénombre à ce jour plus de 70 000 e-résident estoniens, principalement originaires de pays n'appartenant pas à l'Union européenne comme l'Ukraine, la Turquie ou la Russie, mais aussi d'Allemagne ou de France. Dans ces derniers cas, ces e-résidents voyagent en général sans cesse, partout dans le monde, d'où la nécessité pour eux de pouvoir gérer leur société entièrement à distance.

Il convient de relativiser les avantages de nature fiscale que l'Estonie a retirés de ce programme. En réalité, les entrepreneurs e-résidents continuent de payer leurs impôts sur le revenu à leur pays de résidence fiscale. Quant à l'impôt sur les sociétés, il est acquitté sur le lieu de la création de valeur, c'est-à-dire, dans la plupart des cas, hors du territoire estonien. L'argument fiscal n'apparaît pas non plus comme le plus convaincant du point de vue des entrepreneurs. En revanche, diriger une entreprise européenne comporte des avantages de taille pour des non-Européens. Ce programme a permis à l'Estonie de soutenir l'émergence d'entreprises spécialisées dans les services aux e-résidents, tels que la comptabilité, la prospection de clients ou le secrétariat en ligne. Au final, c'est tout un écosystème d'entreprises qui a vu le jour grâce au programme e-Residency.

L'Estonie compte 1,3 million d'habitants. Les sociétés du pays peineraient à se développer uniquement dans les limites physiques du territoire, ce qui explique leur volonté de nouer des relations d'affaires avec des entreprises internationales.

Au fil du temps, le programme e-Residency a gagné en importance en tant qu'outil de *soft power* au service de la diplomatie estonienne. L'Estonie développe de plus en plus ses activités de conseil aux autres États désireux d'étendre et de consolider leur infrastructure numérique afin d'attirer les entrepreneurs internationaux.

M. Philippe Latombe, rapporteur. D'autres États ont-ils tenté de copier le modèle estonien ? Y sont-ils parvenus ? Certains pays y ont-ils apporté des modifications ou des innovations ? Les États qui se sont inspirés de l'Estonie partageaient-ils comme point commun leur petite taille ? Ont-ils dû, eux aussi, créer leur administration *ex nihilo* ? Existe-t-il un exemple d'administration préexistante qui aurait développé un programme similaire ?

M. Arnaud Castaignet. Pour l'instant, ce sont plutôt de petits États ou des États émergents qui ont copié le programme e-Residency, comme la Lituanie, cette année. L'Ukraine a annoncé son intention de l'imiter, ainsi que Dubaï. Pourquoi le programme estonien e-Residency reste-t-il indéniablement plus populaire que ces autres versions ? D'abord, parce qu'il n'aurait pas vu le jour sans l'existence préalable d'une administration entièrement numérique. L'autorisation, pour un entrepreneur étranger, de créer une entreprise en ligne ne présente pas d'intérêt sans la possibilité d'en assurer la gestion en ligne également.

Le lancement du programme e-Residency remonte toutefois à 2014 et la technologie qu'utilise l'administration estonienne date de 2002. Les pays qui lanceront des programmes semblables dans un avenir proche en profiteront sans doute pour corriger certains défauts. Ni

la Lituanie ni l'Ukraine, me semble-t-il, ne prévoient de passer par une carte d'identité numérique. L'identité numérique ne requiert pas forcément de support physique, comme l'illustre celle développée par FranceConnect. Seule une ambassade estonienne est habilitée à délivrer la carte d'identité indispensable aux e-résidents, en recueillant pour ce faire leurs empreintes digitales, or l'Estonie ne compte qu'une trentaine d'ambassades à travers le monde, dont une seule en Afrique. Il apparaît donc difficile aux habitants de ce continent de souscrire au programme e-Residency. Les pays qui adapteront ce programme, sans pour autant en modifier les principes, privilégieront, à mon avis, le recours à une identité numérique dématérialisée.

M. Philippe Latombe, rapporteur. Comment jugez-vous le niveau de numérisation de l'administration française ? Comment évaluez-vous l'écart entre l'Estonie et la France ?

M. Arnaud Castaignet. Tout dépend de l'angle sous lequel on aborde la question. L'administration française se révèle beaucoup plus avancée que l'Estonie en matière de données ouvertes. L'Estonie ne considère pas ce sujet comme une priorité, à la différence de la France, comme l'a montré la gestion de la crise sanitaire dans notre pays. Les données publiques y sont présentées en toute transparence, de manière à ce que des experts en analyse de données puissent les réutiliser. Certains dispositifs français gagneraient à s'étendre à l'échelle européenne. Je serais ravi que l'Estonie s'en inspire.

Notre pays paraît moins avancé en ce qui concerne l'interopérabilité des données, pourtant essentielle en Estonie, où toute donnée transmise à une administration doit pouvoir être exploitée par une autre. La France accuse un retard dans ce domaine.

Les interactions avec l'administration, plus faciles en Estonie, passent par un seul et même portail « eesti.ee » permettant de se connecter à l'ensemble des services publics à l'aide de deux codes PIN et d'une carte d'identité numérique. Les citoyens estoniens utilisent ce portail aussi bien pour voter ou vendre leur voiture que pour consulter leurs prescriptions médicales en ligne. Par curiosité, j'ai entré dans mon navigateur l'adresse « france.fr ». Elle renvoie à une page qui propose la recette du clafoutis et répertorie les meilleures routes touristiques de notre pays.

L'habitude est vite prise de n'utiliser qu'un seul système d'authentification pour toutes les démarches, qu'elles relèvent du fisc ou de la santé, ce qui rend le recours à la version numérique des services publics estoniens particulièrement pratique. L'une des clés de la réussite de l'Estonie en matière d'administration numérique vient de la prise de conscience que la numérisation obligerait les agents à modifier leur façon de travailler. Sans verser dans les discours convenus préconisant une gestion du service public selon les mêmes principes qu'une entreprise privée, par l'imposition d'une culture du résultat, notamment, il faut bien comprendre que la dématérialisation des démarches peut aussi faciliter les échanges. En Estonie, quand je pose une question à un agent du service public, je reçois généralement une réponse sous deux ou trois jours. En France, la réactivité des agents n'est pas forcément perçue comme une priorité lorsqu'on envisage la dématérialisation des démarches. Il reste à former les fonctionnaires français pour qu'ils adaptent leur mode de travail au numérique de manière à favoriser les interactions avec le public. En réalité, le recours au numérique ne signifie pas forcément le recul de l'humain dans l'administration. Au contraire, la numérisation doit garantir une plus grande agilité dans les interactions entre les citoyens et leur administration.

M. Philippe Latombe, rapporteur. Vous avez parlé de redevabilité mutuelle. À vous entendre, le numérique permet à l'administration de vérifier certaines informations en les mutualisant. En contrepartie, chaque citoyen peut savoir qui accède à ses données et à quel moment. Ces deux aspects de la transparence du traitement des données vont-ils

nécessairement de pair ? Une telle réciprocité vous semble-t-elle indispensable à une numérisation réussie ? Nous avons l'impression qu'il existe en France une mutualisation des informations entre les administrations sans pour autant que s'impose une culture de la transparence. L'ouverture des données dans notre pays ne concerne bien sûr que les données publiques et non personnelles, dont la protection reste un sujet de préoccupation essentiel.

M. Arnaud Castaignet. J'estime pour ma part nécessaire que la transparence s'applique dans les deux sens. Pourquoi construire une infrastructure numérique ? Pour accroître l'efficacité du service public, mais aussi pour développer la confiance des citoyens en leur administration. Les dirigeants politiques ne bénéficient pas d'une meilleure image en Estonie qu'en France ou dans d'autres pays d'Europe. Les gouvernements qui se succèdent en Estonie doivent eux aussi relever le défi de gagner la confiance des citoyens. En revanche, les institutions, elles, sont davantage perçues comme transparentes, ce que l'on doit selon moi à la notion de redevabilité mutuelle.

Il n'existe pas, en Estonie, de base de données centralisée. Chaque administration dispose de la sienne. Cependant, les données sont interopérables et n'importe quel service public peut accéder à celles que détiennent les autres. Nul ne dispose malgré tout d'une vision globale des données relatives à une personne en particulier. Si un citoyen estime illégitime une consultation de ses données, il dispose de voies de recours et peut même déposer une plainte. Cela s'est déjà produit à l'encontre d'agents publics ayant récupéré des données qui ne les concernaient pas.

Chaque citoyen estonien peut obtenir, en temps réel, *via* le portail de l'administration, une liste semblable à un relevé bancaire indiquant quel service public a consulté lesquelles de ses données à quel moment et pour quel motif. Un tel dispositif implique d'éduquer la population à l'enjeu des données personnelles et de leur protection, mais aussi de sensibiliser aux bénéfices que peut occasionner leur traitement, dans la mesure où celui-ci facilite aussi la vie.

Je ne pense pas que les Estoniens accorderaient autant de confiance à leur modèle numérique sans la possibilité de vérifier qui accède à leurs données. Il faudrait accorder la priorité en France également à cette exigence de transparence réciproque, condition *sine qua non* d'une plus grande confiance dans le traitement des données par l'administration.

M. Philippe Latombe, rapporteur. Cette redevabilité mutuelle a-t-elle fait l'objet d'un contrat dès le départ ou s'est-elle imposée par la suite ? Est-elle apparue comme une exigence dès la construction du système administratif dans sa version numérique ou parce que l'administration l'a estimée nécessaire pour rallier à ce dispositif les citoyens ?

M. Arnaud Castaignet. La transparence a été considérée comme une priorité politique dès que la stratégie numérique du gouvernement estonien a pris forme. Sa mise en pratique a coïncidé avec la création de l'infrastructure X-Road, permettant l'accès aux données. Cette transparence apparaît comme le fruit d'une volonté politique indépendante de toute technique, liée à l'histoire de l'Estonie, qui n'a recouvré son indépendance par rapport à l'Union des républiques socialistes soviétiques (URSS) qu'en 1991. Très vite, les dirigeants estoniens ont compris que la population exigerait de la transparence de la part des institutions nouvellement créées, mais aussi que les citoyens tiendraient à rester maîtres de leurs données, à l'abri de tout espionnage.

M. Philippe Latombe, rapporteur. L'arrêt Quadrature du net de la Cour de justice de l'Union européenne a fait grand-bruit en France. Il portait sur la conservation des métadonnées des fournisseurs d'accès à Internet. L'arrêt Prokuratuur, de même nature mais concernant

l'Estonie, a-t-il rencontré un écho, peut-être pas auprès du grand public mais au moins de la frange de la population qui s'intéresse au numérique et à la transparence de l'accès aux données ?

M. Arnaud Castaignet. Je dirais que non, encore que des experts seraient sans doute mieux armés que moi pour répondre à votre question. Il me semble que cet arrêt n'a pas suscité un fort retentissement en Estonie, et n'a pas remis en cause le modèle numérique estonien.

M. Philippe Latombe, rapporteur. En France, des associations se mobilisent pour la protection des données personnelles, assumant un rôle de vigie, voire de lanceur d'alerte. En est-il de même en Estonie ou le contrat de confiance établi entre l'administration et les citoyens en a-t-il supprimé le besoin ?

M. Arnaud Castaignet. Il existe en Estonie des associations de défense des libertés publiques. L'utilisation des données donne lieu à des débats permanents. Des commissions rassemblent des représentants du gouvernement et de l'administration, des citoyens et des entreprises, afin de veiller au respect de l'intégrité des données, perçue comme prioritaire.

La protection des données n'est pas envisagée de la même façon en Estonie qu'en France. En Estonie, cette protection n'implique pas d'interdire l'accès aux données personnelles, mais la possibilité de savoir qui souhaite les consulter, pour quelle raison et, à partir de là, de l'y autoriser ou non. L'infrastructure numérique estonienne offre la possibilité aux citoyens de crypter certaines de leurs données. Une femme ayant subi un avortement peut ainsi choisir de ne communiquer cette information qu'à son seul médecin traitant. La plupart des usagers des services publics numériques ne recourent toutefois pas au cryptage. Ils estiment en tout cas plus pratique d'effectuer leurs démarches en ligne.

Des documents imprimés revêtus d'une signature manuscrite possèdent la même valeur juridique que ceux validés par une signature numérique. Le choix est laissé en permanence aux usagers. Chacun reste maître de ses données et de l'utilisation qui leur est réservée.

M. Philippe Latombe, rapporteur. Après le lancement de l'identité numérique et de la numérisation complète de l'administration, l'Estonie s'est-elle tournée vers des technologies de type *blockchain* pour renforcer la transparence du système mis en place ?

Comment l'administration estonienne s'assure-t-elle de rester à la pointe en matière de services publics numériques ? Comment continue-t-elle à innover ? S'appuie-t-elle sur des ressources et des programmes de formation internes ? Se tourne-t-elle vers le secteur privé et, si oui, comment s'organise la passation de marchés publics ?

Comment l'Estonie prépare-t-elle l'avenir, à présent que la numérisation des services étatiques s'est achevée et que le programme e-Residency a été copié à l'étranger ? Vous avez mentionné le souhait des autorités estoniennes de voir émerger des géants des nouvelles technologies. Qui, en Estonie, décide des domaines où il conviendra d'investir ? Comment ces secteurs d'avenir reçoivent-ils une impulsion ?

M. Arnaud Castaignet. L'administration estonienne utilise la *blockchain* pour doter d'un niveau de sécurité supplémentaire l'intégrité des données des citoyens. Elle a pris cette décision à la suite de cyberattaques par déni de service qui, en 2007, ont empêché l'accès à plusieurs sites internet. Aucune donnée personnelle n'a cependant été récupérée par des tiers. L'État n'en a pas moins réfléchi à un moyen de renforcer la sécurité de ses services numériques, ce qui l'a incité à se tourner notamment vers la *Keyless Signature Infrastructure*

(KSI) *blockchain* pour protéger ses données critiques. Cette technologie a été développée grâce à un partenariat avec le secteur privé.

La quasi-totalité des infrastructures numériques estoniennes résulte d'un partenariat du secteur public avec des entreprises privées estoniennes. La commande publique a d'ailleurs favorisé le développement de nouvelles compétences dans le pays. Le secteur des nouvelles technologies se compte aujourd'hui parmi ceux qui emploient le plus de salariés en Estonie. Il représente 6 % du Produit intérieur brut (PIB).

En Estonie, la *blockchain* n'est que peu utilisée pour le développement de cryptomonnaies. Le lancement d'une cryptomonnaie d'État, l'Escoin, a été évoqué dans le programme e-Residency, mais aucune suite n'y a été donnée.

Le développement du modèle numérique estonien a véritablement commencé en ce qui concerne l'éducation, par le raccordement des écoles à Internet et la formation des enseignants à l'utilisation des technologies numériques, ce qui a favorisé une meilleure compréhension des enjeux du numérique et l'émergence d'une culture de l'innovation et de l'entrepreneuriat, dès le plus jeune âge. Il existe beaucoup de junior-entreprises dans les lycées, voire les collèges. Comme ces initiatives ont débuté voici plus de vingt ans, les premiers étudiants formés au numérique sont aujourd'hui adultes. Ainsi, une grande part de la population estonienne est davantage formée que dans d'autres pays aux outils numériques. Lors du lancement de l'identité numérique, l'État estonien a décidé de former à son utilisation 15 000 personnes, qui ont chacune formé à leur tour dix de leurs concitoyens. L'idée de former les Estoniens tout au long de leur vie joue de ce point de vue un rôle clé.

M. Philippe Latombe, rapporteur. Cela signifie-t-il qu'il n'existe pas en Estonie de fracture numérique telle qu'on la constate en France ?

M. Arnaud Castaignet. Pas plus que tout autre pays, l'Estonie n'échappe à une fracture numérique, surtout notable dans les zones rurales et en restructuration industrielle, dans l'est du pays. Peut-être y est-elle moins marquée qu'en France. Je ne voudrais malgré tout pas nier les problèmes de l'Estonie. La fracture numérique y est en passe de se résorber, mais pas avant au moins une génération encore. Les limites du numérique se révèlent, par exemple, au travers de la campagne de vaccination contre le Covid. Un seul et unique portail public numérique permet de s'enregistrer en vue d'obtenir un vaccin, mais une partie de la population, encore peu habituée à utiliser Internet, peine à s'y inscrire. Il en résulte des disparités entre les taux de vaccination d'une région à l'autre.

L'Estonie a peut-être mieux compris que la France l'utilité d'une formation tout au long de la vie. Beaucoup de facilités sont offertes aux agents du service public pour se former, à l'université ou en ligne, en parallèle à l'exercice de leurs fonctions. Des programmes étatiques favorisent l'émergence de *start-up* d'État. Il me semble qu'il existe des programmes semblables en France, mais l'Estonie témoigne d'une plus grande volonté d'acclimater une culture de l'innovation au sein de l'administration. Ces *start-up* d'État contribuent à la conception des services publics de demain, en réfléchissant notamment aux usages possibles de l'Intelligence artificielle. L'Estonie s'est ainsi très tôt penchée sur la question du statut juridique des robots.

Beaucoup de spécialistes estiment que l'infrastructure numérique de l'Estonie, peut-être un peu délaissée par le passé, gagnerait à être modernisée, entre autres pour qu'elle résiste mieux à un très grand nombre de connexions simultanées.

M. Philippe Latombe, rapporteur. Comment le gouvernement estonien désigne-t-il les secteurs d'avenir dans lesquels il investira ? La création de votre entreprise, de haute technologie industrielle, résulte-t-elle d'une volonté de l'État ? Celui-ci a-t-il donné une impulsion à votre secteur d'activité par la mise en place d'une politique publique ?

M. Arnaud Castaignet. Le gouvernement estonien n'a pas impulsé le développement des technologies que produit mon entreprise. L'État ne considère ce secteur comme une priorité que depuis peu, peut-être grâce à la réussite de Skeleton Technologies, justement. L'Estonie s'est d'abord focalisée sur les logiciels ou la programmation informatique, et n'a que récemment découvert, ou redécouvert, les vertus d'une politique industrielle.

Qui prend les décisions relatives au numérique en Estonie ? Il y existe, comme en France, un ministère des nouvelles technologies, qui s'occupe aussi de l'entrepreneuriat. Cependant, à la tête de l'administration en charge de la mise en œuvre et du développement de l'infrastructure numérique est placé un fonctionnaire, dont l'alternance politique ne remet pas en cause la nomination, pour une durée de dix ans. L'Estonie a été dirigée pendant un an et demi par une coalition du centre, de la droite et de l'extrême droite, ayant succédé à une coalition du centre, de la droite et de la gauche. Pendant tout ce temps, le même administrateur est resté en poste. Les stratégies, planifiées par l'administration sur cinq ou dix ans, font l'objet d'un débat à l'Assemblée nationale, mais elles trouveraient une traduction concrète même en l'absence de personnalité politique pour les soutenir. Elles passent en effet pour échapper aux enjeux des luttes entre partis et suscitent un consensus.

M. Philippe Latombe, rapporteur. Il est beaucoup question en France de notre plan de relance et de sa version européenne. Comment un tel plan se décline-t-il en Estonie, dès lors que l'État n'intervient pas pour imposer des directions à l'industrie ? L'État français dispose d'un pouvoir d'injonction tel que le plan de relance se contente de soutenir, au niveau financier, l'application de sa volonté. Qu'en est-il en Estonie, qui a bénéficié de fonds européens, au même titre que les autres pays de l'Union européenne ? Les entreprises estoniennes s'adressent-elles spontanément au guichet de l'État ? Celui-ci répond-il favorablement à toutes les sollicitations selon les mêmes critères ou privilégie-t-il certaines filières ? L'innovation vient-elle uniquement d'entreprises privées ? L'État estonien la soutient-il par des dispositifs comparables au crédit d'impôt recherche (CIR) français ? L'Estonie assure-t-elle des avantages fiscaux aux sociétés innovantes ? Si jamais un acteur étranger tentait de prendre le contrôle de Skeleton Technologies, le gouvernement estonien tenterait-il de protéger votre entreprise ?

M. Arnaud Castaignet. L'État estonien n'est pas intervenu dans la création de Skeleton Technologies en 2009. Toutefois, du fait du plan de relance et du pacte vert (ou *green deal*) européens, les *cleantech* et les technologies visant à réduire l'empreinte carbone figurent désormais parmi les priorités stratégiques de l'Estonie. La politique industrielle revient partout à la mode, au point qu'elle est maintenant perçue comme une nécessité. Les débats autour de la question en Europe et même en France l'attestent. Ce n'était pas le cas voici dix ans. Le gouvernement estonien base sa relance économique sur le respect de l'environnement et la décarbonation. Une entreprise comme Skeleton Technologies passe donc aujourd'hui pour plus importante, sur le plan stratégique, que par le passé. Comme en France, les priorités politiques en Estonie vont à présent au numérique et au verdissement de l'économie.

Il existe en Estonie des aides pour les *start-up*. Des institutions telles que KredEx ou Enterprise Estonia assurent un soutien financier aux *start-up* dans la toute première phase de leur développement. Un tel système apparaît particulièrement pertinent pour les entreprises de *hardware*. La *deep tech*, terme en vogue, désigne des technologies de rupture alliant la science et la recherche au monde des affaires. C'est sur ce champ que se livreront les futures batailles

économiques et industrielles à l'échelle mondiale. Son développement nécessite un soutien public important, car beaucoup de temps s'écoule en général entre la création d'une société et l'apparition sur le marché de la technologie qu'elle souhaite mettre au point. Il a fallu près de cinq ans à Skeleton Technologies avant de proposer à la vente ses produits. Nous générons désormais un chiffre d'affaires, ce qui n'est pas le cas de beaucoup d'entreprises spécialisées dans le stockage d'énergie.

Dans le même ordre d'idées, nous pourrions mentionner BioNTech, qui produit des vaccins à ARN messager. Cette société a eu besoin d'un soutien financier, principalement public, à ses débuts. Les investisseurs privés ne désirent pas forcément subventionner des technologies sans la certitude d'en tirer un profit à court terme, ce qui explique la nécessité d'un investissement européen direct dans l'économie, suivi d'un achat des innovations. Il faudrait transposer au niveau européen ce qui a été mis en place aux États-Unis avec un outil tel que HyperPASS.

En Estonie, les sommes réinvesties dans une *start-up* sont exemptées de l'impôt sur les sociétés. Cette mesure favorise l'investissement. L'Estonie est toutefois loin de s'apparenter à un paradis fiscal. Les entreprises créées en Estonie n'y conservent pas forcément leur siège. Bolt et notre société ont gardé le leur en Estonie, bien que notre usine soit implantée en Allemagne, mais il n'en va pas de même de TransferWise. Recruter des talents dans un aussi petit pays n'est pas aisé. Ce problème de personnel qualifié se pose d'ailleurs partout, y compris en France.

Le gouvernement estonien n'entrerait pas dans une logique défensive, au cas où un acteur étranger tenterait de s'approprier Skeleton Technologies, pour la simple raison que l'État n'y a pas investi, contrairement à l'Institut européen d'innovation et de technologie (*European institute of technology* ou *EIT*). Nous avons également bénéficié du soutien de la Banque européenne d'investissement. Au fur et à mesure de nos levées de fonds, nous avons toutefois plutôt fait appel à des investisseurs privés. L'Estonie est un trop petit pays pour que son gouvernement intervienne vis-à-vis d'un acteur étranger qui adopterait un comportement prédateur à l'égard de notre entreprise. Malheureusement, l'Estonie ne dispose pas de l'équivalent de Bpifrance, perçue là-bas comme un modèle à suivre pour le développement de nouvelles industries, et que la France gagnerait à promouvoir davantage. Il faudrait, au niveau de l'Union européenne, un équivalent de Bpifrance, plus important encore que le Conseil européen de l'innovation, capable d'investir dans des *start-up* en phase initiale de développement en vue d'acquérir, à terme, les fruits de l'innovation. Rien ne favoriserait mieux le développement de technologies de rupture comme l'ordinateur quantique ou la 6G qu'une telle sorte de fonds souverain. Il faudra que l'Europe se dote davantage d'outils pour piloter sa stratégie industrielle, ce qui suppose un état d'esprit favorable à la prise de risque, hélas difficile à cultiver lors de la création d'une agence européenne.

M. Philippe Latombe, rapporteur. Voyez-vous aujourd'hui des politiques publiques numériques, en Estonie ou ailleurs, qui mériteraient notre attention, en vue de leur éventuelle transposition en France ?

M. Arnaud Castaignet. Il me semblerait intéressant de se pencher sur l'exemple du Danemark. Ce pays est arrivé à peu près au même point que l'Estonie en matière de dématérialisation de l'administration or, contrairement à l'Estonie, il lui a fallu numériser des services publics déjà existants. L'Ukraine a lancé un système favorisant la transparence des commandes publiques, qui répond certes à des besoins spécifiques à l'Ukraine, mais figure parmi les plus innovants au monde. Il a d'ailleurs été récompensé lors du sommet « Partenariat pour un gouvernement ouvert » organisé en France en 2016. J'estimerais pertinent d'échanger

avec les Ukrainiens au sujet de la transparence des commandes publiques en vue de transposer leurs innovations.

M. Philippe Latombe, rapporteur. Aurions-nous oublié d'aborder un sujet qui vous tiendrait à cœur ? Voudriez-vous revenir sur un point méritant selon vous d'être mis en lumière ?

M. Arnaud Castaignet. Il me semble qu'en matière de souveraineté numérique, nous gagnerions à nous interroger sur les moyens de soutenir la croissance de nos entreprises européennes pour qu'elles se hissent au rang de géants des nouvelles technologies. Elles n'y parviendront qu'au prix d'une transformation de leur modèle d'affaires. Amazon a d'abord été une librairie en ligne avant de devenir un puissant acteur de l'industrie du *cloud*. Chaque grande société du numérique est amenée à effectuer une transition vers l'industrie. Il me semble donc impératif que les futurs géants européens du numérique se dotent d'une dimension industrielle.

La France et l'Europe devraient, en s'appuyant sur leurs atouts, définir des secteurs prioritaires d'où émergeraient les futurs géants de demain. J'ai mentionné tout à l'heure la santé, la ville, l'agriculture ou encore la mobilité, autant de domaines où se livreront de féroces batailles. Un débat public doit préluder à l'établissement de ces priorités avant qu'une réflexion porte sur les moyens d'investir, *via* des fonds publics souverains, dans ces secteurs porteurs d'avenir. Il conviendrait aussi de favoriser la coordination entre les universités et le secteur privé. Les pôles européens, et en particulier français, de recherche fondamentale se classent parmi les meilleurs au monde, mais il reste à transformer leurs avancées par des *start-up*. La croissance d'entreprises innovantes en France pourrait passer par la création d'un marché numérique européen unique, ce qui pose la question d'une langue commune. La diversité linguistique au sein de l'Union européenne n'y favorise pas l'émergence de sociétés d'envergure européenne. À défaut, les entreprises françaises auraient tout intérêt à se tourner vers la francophonie et en particulier les pays d'Afrique pour s'imposer sur les marchés de ce continent. Des stratégies de coopération devraient dans ce cas se mettre en place.

Enfin, il me paraît souhaitable que se développe une identité numérique à l'échelle européenne, fondée sur les valeurs de transparence et de redevabilité mutuelle propres à l'Estonie. La France pourrait y contribuer par son attachement à l'ouverture des données, dans un esprit d'échange de bonnes pratiques.

Audition, ouverte à la presse, de M. Stéfane Fermigier, co-président du conseil national du logiciel libre (CNLL)
(1er juin 2021)

Présidence de M. Philippe Latombe, rapporteur.

M. Philippe Latombe, président et rapporteur. En guise d'introduction, je présenterai succinctement le conseil national du logiciel libre (CNLL). Fondé en 2010, il regroupe les principales associations et grappes d'entreprises de la filière *open source* et représente, par leur intermédiaire, près de 300 sociétés spécialisées dans le logiciel libre et le numérique ouvert : intégrateurs, éditeurs ou encore sociétés de conseil. Le CNLL s'est donné pour mission de représenter et de défendre auprès des pouvoirs publics la filière professionnelle du logiciel libre et du numérique ouvert en France, mais aussi de promouvoir son offre de logiciels et de services, ses atouts spécifiques et ses besoins, notamment en termes d'emploi et de formation.

Je souhaiterais, à titre de préambule, vous poser trois questions.

D'abord, j'aimerais savoir ce que recouvre pour vous la notion de souveraineté numérique, objet d'une attention croissante des pouvoirs publics depuis la crise sanitaire. Lors de nos précédentes auditions, nous avons recueilli de multiples définitions de cette notion très vaste, que certains rapprochent d'une forme d'autonomie stratégique ou décisionnelle. Je voudrais comprendre, d'une part, comment vous entendez cet impératif et, d'autre part, de quelle façon le logiciel libre peut y contribuer.

Mon second point portera sur la filière du logiciel libre en tant que telle. Vous nous avez transmis un ensemble de documents très complets sur ses principales caractéristiques et tendances d'évolution. J'attends de vous que vous nous dressiez un état des lieux de cette filière en mentionnant ses forces et ses faiblesses et, surtout, vos attentes vis-à-vis des pouvoirs publics. Nous avons conscience que le logiciel libre fonctionne comme un levier de souveraineté dans une approche de « promotion des communs numériques », pour reprendre l'expression de M. Henri Verdier devant notre mission. Comment pouvons-nous, parlementaires et pouvoirs publics, participer à son développement dans nos travaux ?

Enfin, je souhaiterais, pour conclure mon propos liminaire, évoquer avec vous l'échelon européen. Je sais que vous siégez à l'association professionnelle européenne du logiciel libre (APELL). Pourriez-vous nous parler de son actualité, puis du rôle de l'Europe en matière de souveraineté numérique et de logiciel libre ? En un mot, les différentes initiatives mises en œuvre vous semblent-elles suffisamment ambitieuses ? Que peut-on en attendre au cours des mois et des années à venir ?

M. Stéfane Fermigier, co-président du conseil national du logiciel libre (CNLL). La constitution du CNLL résulte en effet de la volonté de représenter et de défendre la filière du logiciel libre, présente en France depuis 1998, voire 1996. Nous menons régulièrement des études et nous efforçons, autant que possible, d'intervenir dans le débat public, aussi bien face aux parlementaires que vis-à-vis du pouvoir exécutif.

Je m'exprimerai ici à la fois en tant que spécialiste du logiciel libre et que créateur de sociétés. J'investis aussi, depuis plus de vingt ans, dans des entreprises de la filière. Par souci de clarté, je précise que j'utilise indifféremment les termes *open source* et « logiciel libre ». Le cadre de notre échange ne me semble pas justifier d'entrer à ce propos dans des querelles sémantiques.

La dernière étude commandée par le CNLL a justement été publiée ce matin. Assez complète, elle se focalise sur la filière du logiciel libre, ses attentes et son positionnement par rapport, entre autres à la souveraineté numérique. D'autres de nos études portent sur la taille des marchés français et européen, ainsi que leur évolution depuis une vingtaine d'années. Nous disposons ainsi de toutes les informations que vous pourriez souhaiter sur notre filière.

Notre confédération réunit 300 sociétés. En y ajoutant celles qui ne sont pas affiliées à des grappes d'entreprises, nous dénombrons en France 500 petites et moyennes entreprises (PME) spécialisées dans le logiciel libre. Elles emploient 50 000 à 60 000 personnes. Des études que nous avons commandées estiment le marché français à 5 milliards d'euros. Plus la filière prend de l'ampleur, plus sa croissance ralentit. Malgré tout, elle connaît globalement une croissance annuelle de 8 % à 10 %. Les logiciels libres sont souvent associés à des modèles de services. Cependant, le modèle d'éditeur progresse. Actuellement, le *cloud* joue le rôle d'un rouleau compresseur dans l'informatique, or le logiciel libre y est également présent. Les acteurs du logiciel libre proposent en effet des offres *cloud*.

La position prééminente de la France en matière d'*open source* est reconnue depuis plus de dix ans, encore que notre pays se situe à peu près à égalité avec l'Allemagne au niveau européen, ce dont il y a tout lieu de se féliciter. Nous avons fondé, avec une association équivalente à la nôtre en Allemagne, une sorte de consortium européen.

Comment la France en est-elle venue à occuper ce rang favorable à notre filière, bien que certaines de nos attentes demeurent insatisfaites au regard de la politique actuellement menée dans ce secteur ? Les pouvoirs publics ont commencé à s'intéresser au logiciel libre voici un peu plus de vingt ans. Plusieurs missions et agences gouvernementales se sont emparées du sujet, dès le début de l'administration électronique, soit en 1998. Citons la mission de soutien technique pour le développement des technologies de l'information et de la communication au sein de l'administration (MTIC), l'agence pour le développement de l'administration électronique (ADAE), auparavant connue sous le nom d'agence pour les technologies de l'information et de la communication dans l'administration (ATICA) et devenue depuis une dizaine d'années Etalab.

Je tiens à saluer le travail des parlementaires en matière de logiciel libre. De nombreux élus à la représentation nationale l'ont soutenu en interpellant l'exécutif à ce propos. Certains ont même déposé des propositions de loi, comme le sénateur Pierre Laffitte à la fin des années 1990, en vue d'accorder la priorité absolue aux logiciels libres *via* l'obligation pour l'administration de ne plus recourir qu'à des solutions *open source* à l'issue d'une période transitoire de deux ans. Bien que cette proposition prête à sourire lorsqu'on la relit aujourd'hui, et même si son application restait à préciser, ses motivations n'ont rien perdu de leur pertinence, au vu du débat actuel sur la souveraineté numérique.

Signalons aussi les interventions de l'exécutif, telle la circulaire de 2012 du Premier ministre, M. Jean-Marc Ayrault, qui a donné un coup d'accélération à la filière du logiciel libre. Sorte de guide de bonnes pratiques, elle préconisait de recourir aux logiciels libres en raison de leur moindre coût et de leur plus grande souplesse d'utilisation, ou à défaut, de s'en servir comme d'un levier de négociation avec les éditeurs de logiciels propriétaires. La loi Lemaire votée en 2016 (loi pour une République numérique du 7 octobre 2016) demandait aux administrations d'encourager l'utilisation des logiciels libres pour préserver leur indépendance. Selon moi, cette dernière notion s'apparente assez au concept de souveraineté, qui ne s'est imposé que progressivement. Mentionnons enfin la circulaire du Premier ministre, M. Jean Castex, bien que la date récente de sa publication ne permette pas encore d'en évaluer les effets.

Le logiciel libre présente un avantage économique indéniable. Des centaines de chercheurs parmi les plus prestigieux l'ont mis en évidence dans leurs travaux. Le prix Nobel d'économie, M. Jean Tirole, s'est lui-même penché sur les communs numériques. Une étude de la Commission européenne restant à publier indique que les investissements dans le logiciel libre sont d'un excellent rapport pour la société considérée dans son ensemble. Chaque euro investi dans la filière du logiciel libre engendre un retour sur investissement au moins quatre fois supérieur.

Je ne me considère pas comme un spécialiste de la souveraineté numérique, dont je n'ai d'ailleurs pas conçu de définition personnelle. Je reprendrai donc à mon compte celle du secrétariat général de la défense et de la sécurité nationale (SGDSN) publiée dans la *Revue stratégique de cyberdéfense* de 2018. Le SGDSN assimile la souveraineté numérique à l'autonomie stratégique, notion applicable aussi bien à l'échelle d'un État ou de l'Union européenne que d'une grande entreprise ou même de l'ensemble de la société. Le SGDSN précise bien qu'il ne s'agit pas de « chercher à tout faire en interne », c'est-à-dire qu'il ne faut pas verser dans la caricature en visant une autonomie totale. De même, nous ne préconisons pas le recours exclusif à du logiciel libre, d'autant qu'il favorise les collaborations, y compris internationales. Le SGDSN ajoute qu'une telle autonomie ne peut s'acquérir et se conserver qu'à condition de disposer d'une filière performante européenne. Le développement économique contribue donc en grande part à la préservation de la souveraineté. Ni la loi ni des contrats n'y suffisent.

Le SGDSN estime qu'*« une stratégie industrielle basée sur l'*open source*, sous réserve qu'elle s'inscrive dans une démarche commerciale réfléchie »*, c'est-à-dire sans recourir au logiciel libre uniquement par principe, *« peut permettre aux industriels français ou européens de gagner des parts de marché et par là même de permettre à la France et à l'Union européenne de reconquérir de la souveraineté »*. Nous adhérons entièrement à ces propos.

Nous pourrions citer, dans le même ordre d'idées, la publication de la Commission européenne sur le logiciel libre d'octobre 2020. Elle établit le lien entre souveraineté numérique et logiciel libre. *« Le modèle du code source ouvert a une incidence sur l'autonomie numérique de l'Europe. Il donnera probablement à l'Europe une chance de créer et de maintenir sa propre approche numérique indépendante par rapport aux géants du numérique dans le* cloud *et lui permettra de garder le contrôle de ses processus, de ses informations et de sa technologie. »*

Il en ressort clairement que le logiciel libre présente de nombreux avantages en matière de souveraineté numérique. Reprenons, pour plus de simplicité, les arguments de la Commission européenne. Le logiciel libre garantit l'indépendance ou, du moins, réduit la dépendance des utilisateurs vis-à-vis de certaines entreprises ou pays. Sa flexibilité en fait un atout pour l'innovation en facilitant la création de nouveaux produits ou usages. Le logiciel libre est omniprésent dans le *cloud*. Par sa transparence, il favorise la confiance des citoyens. Nous préconisons de créer des services décentralisés et fédérés, basés sur la coopération et l'interopérabilité, en opposition à la centralisation vers laquelle tend le recours à un nombre réduit de grands fournisseurs de solutions propriétaires.

La Commission européenne a mis en place un *open source program office (OSPO)* stratégique, devenu en France la Mission logiciels libres, créée par la circulaire du Premier ministre, M. Jean Castex. Elle doit servir de fer de lance de la stratégie européenne. Si nous n'allons pas jusqu'à émettre des réserves à son égard, nous souhaiterions tout de même un plan d'action plus ambitieux.

La filière du logiciel libre en France se sent, quoi qu'il en soit, concernée par les enjeux que nous abordons aujourd'hui. L'enquête que nous avons réalisée auprès de 150 entreprises montre que 90 % au moins de leurs dirigeants estiment le sujet de la souveraineté crucial et voient dans le logiciel libre un atout pour l'atteindre. Toute la filière tient à participer à cet effort de reconquête de la souveraineté numérique en Europe.

Nombre d'inventions dans le domaine de l'informatique et en particulier du logiciel libre ont vu le jour en Europe. Le *world wide web,* la technologie peut-être la plus présente dans le monde actuel, a été créé en Suisse. Linux, le système d'exploitation devenu l'emblème du logiciel libre, a été mis au point en Finlande. L'architecture ARM est née au Royaume-Uni, à l'époque où ce pays appartenait encore à l'Union européenne. C'est également à une société britannique que l'on doit le *platform as a service*, l'une des trois formes du *cloud.* L'Europe dispose donc d'atouts. Peut-être n'avons-nous pas su les exploiter autant qu'il l'aurait fallu. Peut-être aussi devrions-nous revenir aux fondamentaux afin de tirer le meilleur parti possible de notre créativité en matière numérique.

L'Allemagne a créé un centre pour la souveraineté numérique de l'administration, le 26 avril 2021. Signalons que sa mission première consiste à promouvoir les logiciels libres. Un lien très fort s'est instauré au sein de cette institution allemande entre le logiciel libre et la souveraineté. Trois *Länder* suivent en outre des politiques d'achat public favorisant le logiciel libre. Peut-être conviendrait-il de s'inspirer de cette prise de position tout à fait remarquable. La loi française accuse un retard de ce point de vue.

La filière du logiciel libre s'intéresse bien évidemment au *cloud* depuis qu'il en est question, c'est-à-dire depuis près de dix ans. Compte tenu de nos valeurs et de notre attachement à la collaboration et à l'interopérabilité, nous avons conscience des risques que comporte un verrouillage excessif du *cloud* par certains prestataires de services. *A contrario*, nous avons, dès 2010, essayé de mettre en avant la notion de *cloud* ouvert, fondée sur la possibilité de passer facilement d'un opérateur à un autre, en imposant aux fournisseurs des normes d'interopérabilité.

Au début, nous avons eu le sentiment que nous n'étions pas écoutés, puis nos préoccupations sont revenues au cœur du débat, notamment par le biais de l'initiative GAIA-X, allemande à l'origine, puis franco-allemande et maintenant européenne. Chacun y projette toutefois sa propre vision du *cloud*, de sorte que nous ne comprenons pas très bien laquelle prédomine en fin de compte.

Au départ, les Allemands voulaient créer un Airbus du *cloud.* Airbus marque certes une réussite industrielle européenne majeure, mais faut-il transposer la même formule dans le domaine du *cloud* ? Nous n'estimons pas judicieux de centraliser à l'excès la fourniture de services autour du *cloud*. Le Club informatique des grandes entreprises françaises *(*Cigref), porteur du projet en France, nous a paru plutôt attaché à des notions de gouvernance, *via* l'imposition de règles et de certifications.

Comme je l'ai dit plus tôt, nous ne reconquerrons pas notre souveraineté à moyen ou long terme uniquement en instaurant des règles. Le Règlement général pour la protection des données (RGPD) constitue certes un outil extrêmement important, d'un point de vue démocratique, mais aussi face à certaines entreprises dont le modèle d'affaires repose sur la commercialisation de données. Ni ce RGPD ni ses variantes ne suffiront toutefois à garantir notre souveraineté numérique.

La nécessité s'impose d'une vision industrielle qui ne se concentre pas uniquement sur de gros acteurs comme Orange ou Atos, surtout s'ils s'appuient sur des technologies qu'ils ne

maîtrisent pas. D'après une récente annonce, ces acteurs s'allieront aux fournisseurs de *cloud* américains comme Google et Microsoft. Selon nous, une telle stratégie se limite à reculer pour mieux sauter. Elle ne nous assurera jamais la souveraineté à laquelle nous aspirons.

Nous attendons des autorités qu'elles fassent appliquer la loi, en particulier la loi pour une République numérique de 2016 et son article 16, selon lequel il faut *« préserver la maîtrise, la pérennité et l'indépendance* [des] *systèmes d'information »* en encourageant les administrations à utiliser le logiciel libre. De simples encouragements ne suffisent pas. Encore faut-il donner des directives, sinon chacun continue de procéder comme il l'entend.

Le recours au logiciel libre passera aussi par l'instauration d'une culture qui lui soit favorable, au travers de formations et d'un travail d'animation de réseaux au sein de l'administration. Chaque ministère nourrit ses propres besoins et donc abordera ce sujet à sa manière singulière. La question se pose aussi à l'échelon européen et à celui des collectivités territoriales.

Nous nous réjouissons de l'annonce, par le Premier ministre, voici quelques semaines, de la création d'une Mission logiciels libres. Nous la réclamions depuis la promulgation en 2016 de la loi Le Maire, dont nous n'avons pas constaté l'effet concret. Telle qu'elle se préfigure, la Mission logiciels libres, à laquelle n'œuvreront que trois personnes, ne suffira cependant pas à animer toute l'administration française. Les chantiers sur lesquels il faut intervenir, ne serait-ce qu'au sein même des services publics, s'annoncent immenses.

Nous estimons en outre indispensable une politique industrielle de développement économique. Une mission logiciels libres uniquement rattachée à la ministre de la transformation et de la fonction publique, Mme Amélie de Montchalin, ne sera pas en mesure d'agir sur le versant industriel de la filière. Il faut, à mon sens, que le ministère de l'économie et la direction générale des entreprises (DGE) s'emparent de la question. Les ministères de l'éducation, et de l'enseignement supérieur et de la recherche sont eux aussi concernés par l'innovation et la formation en lien avec le logiciel libre.

Nous appelons de nos vœux l'extension rapide du périmètre de la Mission logiciels libres, par exemple par la mise en place d'actions similaires dans les autres ministères concernés, et par l'implication de la DGE. La dépense publique doit elle aussi jouer son rôle.

En 2014, Mme Isabelle Attard, alors députée, avait interrogé les principaux ministères sur leur niveau de déploiement du logiciel libre au sein de leur administration. Les réponses des quelques ministres qui se sont exprimés à ce sujet n'apportaient que des éléments qualitatifs, mentionnant tel ou tel logiciel. Il manque une étude poussée impliquant, par exemple, l'inspection générale des finances, afin d'établir la part du logiciel libre dans les dépenses informatiques de chaque ministère. Cette part demeure pour l'heure marginale. En Allemagne, pourtant, une analyse de marché stratégique a été réalisée en 2019, afin de réduire la dépendance des services publics du pays vis-à-vis des fournisseurs de logiciels propriétaires.

Notre étude a mis en lumière le rôle déterminant de la commande publique en tant que levier de croissance de notre filière. À l'évidence, l'État est le mieux placé pour aider une filière mettant au point des produits et des services qui correspondent à ses besoins, à savoir des outils utiles à sa transformation numérique.

Mme Amélie de Montchalin nous a récemment adressé un courrier. Je la cite : *« en accompagnant les administrations pour qu'elles utilisent l'*open source *au mieux, je souhaite que la Mission logiciels libres soutienne les acteurs économiques français et européens de cet écosystème, notamment* via *une meilleure prise en compte dans la commande publique du*

critère de transparence des codes sources. » Il s'agit là d'un élément relativement nouveau. Cette Mission logiciels libres ne s'inscrirait donc pas simplement dans une démarche de partage des codes sources ou de diffusion des bonnes pratiques. Prenant en compte la nécessité d'un soutien aux entreprises du logiciel libre, elle supposerait une attitude proactive vis-à-vis des acteurs de notre filière pour qu'ils participent efficacement aux marchés publics.

Une question récurrente se pose à propos des marchés publics : comment contractualiser ? Les marchés de support passés ces dernières années suffiront-ils à pérenniser des PME ou des très petites entreprises (TPE), éditrices de logiciels libres, ou participant activement à la création de logiciels libres ? En général, les marchés de support sont passés avec des intégrateurs, à la taille proportionnelle à celle du marché concerné. Nous estimons impératif qu'une partie de la valeur générée par ces marchés de support revienne directement aux spécialistes, c'est-à-dire à ceux qui produisent et maintiennent les logiciels et apparaissent comme les mieux à même de répondre aux questions, et de résoudre les éventuels problèmes, des administrations qui les utilisent.

Le rapport présenté par M. Éric Bothorel relevait les difficultés posées par le code des marchés publics, compte tenu des spécificités du logiciel libre. Je ne dresserai pas aujourd'hui la liste de tous les problèmes de la filière. Il me paraît toutefois important que les PME, les TPE et les intégrateurs concernés se réunissent pour en discuter avec les directions des achats des différents ministères, de manière à obtenir un panorama complet des problèmes juridiques liés, soit au code des marchés publics, soit à son application actuelle. Il conviendra dès lors de mettre en place des solutions passant par la révision de ce code ou son contournement.

La question subsiste des moyens par lesquels inciter l'administration à privilégier les logiciels libres, de manière à garantir le développement de la filière. Les débats sur ce point durent depuis vingt ans. La proposition de loi du sénateur Pierre Laffitte, que j'évoquais tout à l'heure, en atteste. Une directive du ministère de la défense a, dès 2006, formalisé la notion de préférence. *« On doit s'efforcer, avant toute acquisition, ou tout développement, d'identifier les solutions alternatives en logiciels libres disponibles, de fonctionnalité équivalente ou voisine. À coût global et risque et efficacité opérationnelle comparables, le logiciel libre est privilégié. »* L'idée que, toutes choses étant égales par ailleurs, il vaut mieux opter pour du logiciel libre constitue à nos yeux une première étape, qui devrait pouvoir se généraliser, peut-être pas sous forme de loi mais au moins de directive. Si une telle mesure ne donnait pas les résultats escomptés, nous pourrions bien sûr recourir à des moyens plus contraignants.

M. Benoît Thieulin, dans un rapport du Conseil économique social environnemental de 2019, évoquait la possibilité d'imposer des quotas relatifs, soit aux logiciels libres, soit aux PME innovantes européennes ou, mieux encore, aux uns et aux autres. De tels quotas permettraient de contrecarrer l'influence des grands acteurs à tendance monopolistique, le plus souvent étrangers. Il a régulièrement été question d'un *small business act* européen. Véritable serpent de mer, le sujet revient sur le devant de la scène depuis des années.

Le développement de la filière du logiciel libre passera aussi par un changement de mentalité. Notre filière est souvent dénigrée, voire laissée de côté, dans les opérations de promotion des acteurs du numérique français. Le logiciel libre est quasiment absent de la communication autour de la French Tech, alors qu'il figure parmi les principales réussites de l'industrie informatique française. La filière française du logiciel libre, rapportée à la taille du marché français, reste sans doute celle qui s'en sort le mieux au monde. Nous pouvons en être fiers.

Certaines idées reçues assimilent le logiciel libre à un logiciel au rabais. Au contraire, il se situe au cœur de toutes les innovations du numérique. À la différence de ce que beaucoup pensent, 57 % des entreprises utilisent au moins un modèle éditeur et pas uniquement de service. Elles associent d'ailleurs souvent les deux. Sans doute un travail d'éducation reste-t-il par ailleurs à fournir, autant dans l'enseignement primaire ou secondaire que supérieur, de manière à inclure les concepts du logiciel libre dans les savoirs fondamentaux.

Deux opportunités se présentent selon moi à notre filière. La première viendra de la présidence française de l'Union européenne l'an prochain. Il est souvent question de collaboration européenne. La Commission européenne, l'Allemagne et d'autres pays encore ont lancé des initiatives fort intéressantes relatives au logiciel libre. Il me paraît essentiel de les coordonner et de les porter à un niveau supérieur en prenant en compte les aspects industriels trop peu présents dans les communications de la Commission. Une seconde opportunité surgirait si le Parlement s'emparait de la question en consacrant par exemple une mission à la souveraineté et au logiciel libre.

M. Philippe Latombe, président et rapporteur. Quel bilan dressez-vous de l'utilisation du logiciel libre au sein de l'administration ? Identifiez-vous des ministères ou des pans de l'administration où la culture du logiciel libre ne serait pas du tout implantée, et d'autres où elle serait au contraire bien enracinée ? Une idée répandue prête à l'administration un fonctionnement « en silos ». Estimez-vous nécessaires des transferts de bonnes pratiques d'une administration à l'autre ? Qu'en est-il dans les collectivités territoriales ?

M. Stéfane Fermigier Je ne dispose pas d'informations précises. Malgré tout, nous avons constaté des niveaux de maturité variables selon les administrations. Tout dépend des circonstances. Il suffit parfois d'un directeur des services informatiques (DSI) enthousiaste pour qu'une attitude proactive s'impose. Je soulignais tout à l'heure que seule une partie des questions aux ministres de Mme la députée Isabelle Attard, en 2014, avait reçu des réponses. Je ne m'en rappelle plus suffisamment pour en donner un compte rendu synthétique. Par ailleurs, beaucoup d'eau a depuis coulé sous les ponts.

Aujourd'hui, le constat s'impose que des ministères jusque-là fortement impliqués dans l'utilisation du logiciel libre semblent s'orienter vers d'autres solutions. Malgré la volonté de mettre en avant la notion de souveraineté, peut-être de manière trop abstraite, de plus en plus d'acteurs se tournent vers des fournisseurs de *cloud* américains. Les contraintes qui en découlent risquent de contrecarrer à terme l'expansion des éditeurs de logiciels libres, mais aussi de l'industrie européenne du *cloud*. Les annonces récentes du gouvernement tendront plutôt à renforcer l'offre américaine, puisqu'elles supposent l'utilisation d'une technologie américaine, certes conjointement exploitée par des sociétés françaises.

Imposer des certifications à ces fournisseurs, comme le label SecNumCloud, risque, si les critères de sélection retenus s'avèrent trop exigeants, de menacer la survie des PME et TPE dépendantes de la commande publique. Notre étude révèle que 80 % de nos sociétés comptent parmi leurs clients des émanations du secteur public, même si ce pourcentage ne correspond pas à la part de leur chiffre d'affaires due à la commande publique. La plupart des sociétés de notre filière souhaitent acquérir de plus en plus de clients relevant de l'administration. Il ne faudrait donc pas imposer à ces entreprises des barrières, par méconnaissance de notre écosystème ou de notre offre, ou en raison d'une croyance en la supériorité des technologies américaines.

La mission d'animation et le transfert de bonnes pratiques qui incombent désormais à la Mission logiciels libres se réalisaient auparavant de manière plus informelle. Il faut que les acteurs les plus engagés dans l'utilisation du logiciel libre, autrement dit les premiers de

cordée, par le partage de leur expérience, convainquent les responsables informatiques encore réticents de suivre leur exemple.

Notre étude portait en partie sur les collectivités territoriales. Nous avons tenté de mettre en évidence des disparités régionales. La place prépondérante de l'Île-de-France, liée au nombre de sociétés de notre filière qui y sont implantées, reflète somme toute la prépondérance économique de cette région dans la quasi-totalité des secteurs.

Toutes les régions ne semblent pas également sensibilisées à la question. Toutes ne soutiennent pas notre filière au même degré. À vrai dire, une seule région, la Nouvelle Aquitaine, très en avance, mène depuis vingt ans une politique active en faveur du logiciel libre, par le soutien de certaines initiatives. Depuis quelques mois, elle suit un plan de développement de la filière numérique prenant pleinement en compte le numérique ouvert ainsi que les aspects éthiques du numérique, dont nous-mêmes nous préoccupons beaucoup.

Dans notre rapport figure le témoignage de M. Nicolas Vivant, directeur de la stratégie et de la culture numérique de la ville d'Échirolles, ancien directeur des systèmes d'information (DSI) de la commune de Fontaine. Il compte à son actif un certain nombre de réussites. Ainsi, la municipalité dont il s'occupait a économisé 100 000 euros par an sur les licences propriétaires par le passage à Linux de 60 % des postes de travail. *« Plus rapide, plus stable, plus esthétique et plus sécurisé, ce système d'exploitation revient moins cher que l'équivalent propriétaire »*, a déclaré M. Nicolas Vivant. Des professionnels qui s'engagent à faire profiter de leurs services des agents du service public, voire de simples citoyens, aboutissent à des résultats spectaculaires.

M. Philippe Latombe, rapporteur. Dans quels délais attendez-vous des résultats concrets de la Mission logiciels libres annoncée par la circulaire du Premier ministre, M. Jean Castex ? À partir de quand conclurez-vous à son échec en l'absence de mesures visibles ? À quels indices jugerez-vous de son efficacité ?

M. Stéfane Fermigier S'il est possible d'évaluer cette mission dans le périmètre qui lui a été imparti, il n'est par ailleurs pas interdit de s'interroger sur la pertinence de ce périmètre particulièrement restreint. La question de sa réussite se pose par rapport aux moyens, malheureusement réduits, dont elle dispose.

Je la vois engagée vers un objectif à long terme, celui de transformer de l'intérieur les mentalités, de généraliser les bonnes pratiques, de réaliser des catalogues de code sources promus par l'État, et de participer à la création de catalogues de solutions *open source* susceptibles d'être utilisés par l'administration, en lien avec la Mission LABEL, qui a récemment publié un catalogue de solutions numériques.

Je ne sais laquelle de ces tâches prime sur telle ou telle autre, mais à l'évidence, ce qui relève de l'animation interne par le partage ou la republication de codes sources n'exercera aucun impact immédiat sur notre filière. À moyen terme, il me semble important de promouvoir, en interne, la culture du logiciel libre et de la collaboration. J'ignore quels indicateurs de réussite ont été définis pour cette mission. La réalisation de catalogues ou d'annuaires, ou la participation, aux discussions animées par cette mission, d'un nombre conséquent de personnes pourront sans doute permettre d'en évaluer le succès. En l'absence d'outils adéquats, il semblerait hasardeux d'établir une corrélation directe entre l'activité de cette mission et, par exemple, le pourcentage de marchés publics impliquant du logiciel libre.

Je préconise, pour cette raison, la création d'un outil de comptabilisation des sommes versées, dans la commande publique, aux géants du numérique plutôt qu'aux acteurs européens du logiciel libre.

M. Philippe Latombe, rapporteur. La semaine dernière, les responsables de Microsoft, auditionnés par notre mission, ont présenté leur entreprise comme l'une des plus engagées au monde en faveur du logiciel libre. Qu'est-ce que de tels propos vous inspirent ?

M. Stéfane Fermigier. Même s'ils prêtent à sourire, vous soulevez là une question tout à fait sérieuse. Ceux qui se rappellent les grands débats avec les représentants de Microsoft à la fin des années 1990 et au début des années 2000 peuvent se réjouir d'un tel revirement.

Microsoft a changé de position en devenant indubitablement un contributeur notable à *l'open source* et un grand utilisateur de logiciels libres. Microsoft a intégré à sa stratégie de nombreux aspects du développement collaboratif propre au logiciel libre. La société finance même des manifestations de promotion du logiciel libre.

Google aussi se compte parmi les grands producteurs de logiciels libres. Un certain nombre de technologies utilisées dans le *cloud* dérivent d'innovations ayant vu le jour au sein de Google.

Néanmoins, nous ne saurions considérer Microsoft comme une société méritant une place de choix dans une politique de *cloud* souverain. Google ou Microsoft, quoique les plus engagés en faveur du logiciel libre parmi les géants américains du numérique, ont trouvé le moyen de déplacer le contrôle hors du code source. Dans le *cloud*, il est tout à fait possible de rendre les utilisateurs prisonniers d'un écosystème, tant au niveau des infrastructures que des plateformes, tout en diffusant par ailleurs du code source.

Notre filière ne s'oppose plus de manière frontale à Microsoft. Nous sommes nombreux à accepter les contributions de cette société au logiciel libre. Toutefois, les *clouds* de Google, de Microsoft ou d'Amazon nous semblent poser de nombreux problèmes, autant à notre propre écosystème que du point de vue de la souveraineté numérique européenne.

M. Philippe Latombe, rapporteur. Si l'on considère les smartphones comme des sortes d'ordinateurs, où en est aujourd'hui la création d'un système d'exploitation libre ? Nous avons constaté les difficultés de sociétés chinoises telles que Huawei par rapport à Android. Nous connaissons les critiques adressées à iOS, le système d'exploitation d'Apple, empêchant par exemple l'utilisation d'antennes MFC (*magnetic flux channel*). Des projets de systèmes d'exploitation libres sont-ils en passe d'aboutir ?

M. Stéfane Fermigier. Le logiciel libre est omniprésent dans les smartphones. L'iOS est basé en grande partie sur de l'*open source.* Le cas d'Android apparaît plus ambigu. Une partie d'Android, l'*Android open source project* (AOSP), est libre. Toutefois, différents mécanismes de certification des matériels, mais aussi la nécessité de pilotes informatiques propriétaires et l'existence d'une version d'Android estampillée Google créent des dynamiques qui s'inscrivent dans le prolongement de la question que vous posiez à propos de Microsoft.

Une société de la taille de Google peut très bien produire de *l'open source* tout en vendant des systèmes propriétaires en complément. Il en résulte une mainmise sur les services qui complètent le logiciel libre de départ.

Plusieurs initiatives, ces dernières années, ont visé la création d'un Android allégé des applications propriétaires de Google, ce qui suppose de modifier le code source d'Android dans l'optique d'éviter toute dépendance vis-à-vis de services proposés par Google, tels que l'authentification, la messagerie électronique Gmail, et tout ce qui relève de l'agenda et des photos. L'utilisateur d'un smartphone s'attend à ce que ces services en fassent partie, alors que son appareil n'est en réalité qu'un terminal grâce auquel il se connecte à des services hébergés dans le *cloud*.

La société e-corp vend, depuis deux ou trois ans, un système d'exploitation indépendant de Google tout en intervenant sur le marché du reconditionnement des smartphones usagés. Son modèle économique se base en partie sur la revente de smartphones d'occasion utilisant son système d'exploitation libéré des applications Google. Nous espérons qu'elle pérennisera ses activités et que son approche générera un chiffre d'affaires suffisant.

Une proportion de la population actuelle, de plus en plus réticente à voir ses données personnelles aspirées par l'un ou l'autre des géants du numérique, en revient aux téléphones mobiles à l'ancienne ou *feature phones* pour échapper aux difficultés liées à la protection de leurs données. Une telle démarche reste néanmoins assez rare, tant la plupart des utilisateurs peinent à se passer des services auxquels ils se sont habitués.

D'autres personnes se tournent vers des solutions alternatives. Pour que celles-ci s'imposent, il faut toutefois qu'un plus grand nombre de citoyens les utilisent. Même si leur notoriété peut s'imposer par le bouche-à-oreille, ces solutions gagneraient à devenir plus connues.

Aujourd'hui, par défaut, les utilisateurs optent pour les géants du numérique, comme ils le faisaient déjà, vingt ans plus tôt, au moment de choisir un navigateur Internet. Microsoft a été condamnée à des amendes significatives par la Commission européenne à cause d'Explorer. À présent, c'est Chrome, le navigateur de Google, qui s'est imposé presque partout. Le contrôle très strict exercé par Apple sur sa plateforme propriétaire d'achat d'applications ne permet pas à ses concurrents d'y proposer les leurs. Il en résulte un nouveau verrouillage du marché qui risque d'exclure, si tel n'est pas déjà le cas, les acteurs indépendants.

Nous espérons que des approches comme celle de YesYes rééquilibreront le marché en proposant une offre alternative au duopole iOS et Android.

M. Philippe Latombe, rapporteur. Quelle place occupera le logiciel libre dans les nouvelles technologies en plein essor comme l'Intelligence artificielle ou l'informatique quantique ? Ces innovations comportent-elles un risque du recul de l'*open source* ?

M. Stéfane Fermigier. Je ne le pense pas, bien au contraire. La plus grande part de l'Intelligence artificielle relève actuellement de l'apprentissage automatisé, où le logiciel libre est très présent. Je connais moins le domaine de l'informatique quantique, où les investissements portent de toute façon principalement sur de la recherche quasi fondamentale et moins sur les logiciels. L'*open source* n'y joue donc pas un grand rôle. Il existe certes des simulateurs de machine quantique *open source*, mais les enjeux du quantique touchent surtout au matériel.

Scikit-learn, l'une des vidéothèques les plus utilisées au monde en apprentissage automatisé, résulte d'un beau projet de l'Institut national de recherche en sciences et technologies du numérique (Inria). Ce projet comporte une dimension industrielle également,

car l'Inria a eu l'intelligence de créer au sein de sa fondation un consortium de grandes entreprises et de *start-up* utilisant sa vidéothèque à des fins d'apprentissage automatisé.

Google dispose de son propre outil d'apprentissage automatisé et Facebook également. Le logiciel libre n'en reste pas moins omniprésent dans l'Intelligence artificielle, où la plupart des logiciels propriétaires restent basés sur de l'*open source*.

La question se pose ensuite des modèles. L'apprentissage automatisé s'opère à deux niveaux. Le premier, celui du moteur d'exécution, repose sur du code machine traditionnel, qui requiert des connaissances poussées en mathématiques, en statistiques et en modélisation. Le code informatique correspondant peut être libre ou non.

Au second niveau de l'apprentissage automatisé, le moteur d'exécution utilise des modèles, à savoir des données à partir desquelles se définiront des réponses à des questions. Il en existe bien peu de libres, ce qui se conçoit sans peine. Une entreprise utilisera un moteur pour traiter ses propres données, mais, *a priori*, ne partagera pas celles-ci, à moins qu'elle n'en décide ainsi. Des dynamiques collaboratives voient le jour dans des industries entières, à partir du moment où plusieurs sociétés décident de partager leurs données pour créer un modèle utile à tous les acteurs du secteur. Bien sûr, rien n'empêche non plus de commercialiser des modèles. Je décris là des phénomènes déjà constatables.

M. Philippe Latombe, rapporteur. J'aimerais évoquer l'article paru hier dans *Les Échos*, sous le titre « Souveraineté numérique : le cri d'alarme du logiciel libre français ». Que manque-t-il, selon vous, pour que ce cri d'alarme soit entendu et qu'une prise de conscience en résulte ?

M. Stéfane Fermigier. Le titre de cet article, dont je reconnais qu'il est bien trouvé, a été choisi par l'auteur de l'article ou sa rédaction, qui en portent la responsabilité.

Le CNLL n'intervient pas dans le débat public uniquement pour dire que tout va mal. Notre situation comporte de bons côtés. Nous occupons une position dominante en termes de taille de marché, et de capacité technologique et humaine à mettre en œuvre nos innovations, en France, en Allemagne et, progressivement, en Europe. Malgré nos atouts, nous avons parfois l'impression d'être ignorés par la plupart des décideurs politiques. Je reconnais que le ministère de la transformation et de la fonction publique nous a écoutés plutôt attentivement ces derniers mois, notamment dans la mission de M. Éric Bothorel et ses suites, dont la circulaire du Premier ministre, M. Jean Castex.

Néanmoins, des déclarations d'intention ne suffisent pas. Notre filière est manifestement oubliée. Nous notons un tropisme vers les solutions les plus alléchantes, et pas seulement de la part de l'exécutif actuel, alors que tout ce qui brille n'est pas en or. Les présidents de la République et les Premiers ministres aiment se laisser prendre en photo auprès des grands du numérique comme Bill Gates, même si d'autres chefs d'entreprises l'ont éclipsé, depuis, dans les médias.

Dans le même temps, nous laissons Google venir en aide aux entreprises françaises. Des sociétés, tirant leur puissance de leurs moyens financiers conséquents, se livrent à un lobbying intensif. Il suffit de consulter les registres du lobbying à Bruxelles pour s'en rendre compte. La filière de l'*open source* est habituée à se débrouiller avec des moyens réduits et néanmoins beaucoup d'enthousiasme, dans le respect de valeurs et dans un esprit de collaboration. Nous peinons à faire entendre notre voix.

Il ne m'est pas agréable d'en parler, pourtant il le faudra bien : certains serviteurs de l'État quittent leur poste dans la fonction publique pour un autre dans des entreprises dominant le marché du numérique. Nous sommes en droit de nous interroger sur d'éventuelles distorsions de leur perception du secteur, voire sur l'indépendance de leurs décisions.

Sans aller jusqu'à dénoncer une corruption pure et simple, notre avocat M. Jean-Baptiste Soufron parle à ce propos de corruption des esprits. L'idée semble s'imposer d'une supériorité si manifeste des technologies du *cloud* en provenance des États-Unis sur celles inventées en Europe, que cela ne vaudrait pas la peine d'évoquer la filière européenne. L'exemple de la French Tech que j'ai évoqué tout à l'heure illustre bien ce travers.

Les contraintes et les difficultés que nous rencontrons, notamment d'ordre administratif en lien avec la passation de marchés publics, ne sont pas forcément perçues comme un véritable problème, alors que les contraintes liées au RGPD et à l'arrêt *Schrems* II ont incité les pouvoirs publics à concevoir une solution pour que l'administration française utilise la technologie du *cloud* américaine, en l'occurrence sur des serveurs hébergés en France. Nous observons un traitement selon deux poids, deux mesures. Nous souhaiterions être plus entendus. La Mission logiciels libres et la circulaire du Premier ministre, M. Jean Castex, montrent que nous l'avons été. Seulement, son périmètre nous paraît trop restreint au vu de nos attentes et de nos difficultés.

M. Philippe Latombe, rapporteur. En effet, votre discours n'est pas uniquement négatif et il ne faudrait pas le percevoir ainsi.

M. Stéfane Fermigier. Nous demandons à être valorisés. Peut-être souffrons-nous d'un manque d'amour des décideurs et des pouvoirs publics.

M. Philippe Latombe, rapporteur. Souhaiteriez-vous aborder un sujet que nous aurions laissé de côté ou revenir sur un point qui vous tient à cœur ?

M. Stéfane Fermigier. Il ne me semble rien avoir omis d'important.

Je voudrais juste rappeler que l'*open source* se fonde sur des valeurs démocratiques de coopération, de transparence et d'ouverture. La Commission européenne les présente comme compatibles et même en synergie avec celles de l'Union européenne, de sécurité, et de respect des données personnelles. Je pense qu'en travaillant sur ces valeurs à des niveaux politiques mais aussi plus opérationnels, touchant à l'animation de l'administration, aux marchés publics et à la formation, notamment, nous arriverons à jouer de nos atouts dans la reconquête de notre souveraineté numérique.

Audition de M. Patrick Pailloux, directeur technique de la direction générale de la sécurité extérieure (DGSE) (ministère des armées) *(2 juin 2021)*

Présidence de M. Philippe Latombe, rapporteur.

(Les propos tenus au cours de l'audition à huis clos n'ont pas fait l'objet d'un compte rendu.)

Audition, ouverte à la presse, de M. Marc Hansen, ministre délégué à la digitalisation du gouvernement du Grand-Duché du Luxembourg
(3 juin 2021)

Présidence de M. Philippe Latombe, rapporteur.

M. Philippe Latombe, président et rapporteur. Nous auditionnons ce matin M. Marc Hansen, ministre du gouvernement du Grand-Duché du Luxembourg chargé de la fonction publique, des relations avec le parlement et ministre délégué à la digitalisation et à la réforme administrative.

Nos échanges porteront sur les problématiques liées au numérique, sous l'angle de la souveraineté numérique, thématique récurrente dans l'actualité européenne, mais aussi sous celui des politiques du numérique au Luxembourg. Nous accueillons avec joie toutes les occasions de mieux connaître la façon dont les autres pays mènent des politiques dans ce domaine, afin de nous inspirer de leurs bonnes pratiques. Il me semblerait également intéressant, au vu de votre expérience, d'aborder les enjeux d'éducation et de formation au numérique.

J'aimerais vous poser trois questions à titre liminaire.

La première, devenue rituelle lors de nos auditions, porte sur votre conception de la souveraineté numérique. Comment appréhendez-vous ce concept ? Comment, selon vous, est-il possible de le traduire concrètement en termes de politique publique ?

J'aimerais ensuite que vous nous parliez des politiques du numérique au Luxembourg. Comment s'y organise leur gouvernance ? Sur quelles réformes portent-elles actuellement ? Les enjeux de la formation aux savoir-faire numériques nous interpellent. Il s'avère primordial d'y répondre pour que les citoyens puissent comprendre le fonctionnement du numérique et s'en servir comme d'un atout dans leur vie personnelle autant que professionnelle.

Peut-être pourrez-vous nous expliquer comment, au Luxembourg, de même qu'en France, le numérique a pu constituer un vecteur de résilience, grâce auquel les élèves ont poursuivi leur scolarité pendant la crise sanitaire liée à la Covid.

Enfin, je souhaiterais que nous échangions sur l'actualité de l'Union européenne en matière de numérique. Quel regard portez-vous sur les nombreux projets soutenus par la commission, tel le *Data Governance Act (DGA)* relatif à la circulation des données ? Comment l'Union européenne pourrait-elle servir de levier de souveraineté numérique aux différents États qui la composent ?

M. Marc Hansen, ministre délégué à la digitalisation du gouvernement du Grand-Duché du Luxembourg. Je ne vous cacherai pas que j'ai quitté la conférence des présidents du parlement luxembourgeois pour être présent à cette audition. Je vous salue d'ailleurs de la part des députés luxembourgeois. Je considère comme un honneur d'échanger avec vous à propos de la souveraineté numérique, compte tenu de l'importance que revêt ce sujet.

Je répondrai d'abord à votre question relative à la gouvernance des politiques du numérique en retraçant l'historique de notre ministère. Avant les élections de 2018, il n'existait pas de ministère de la digitalisation au Luxembourg, même si divers services et

administrations s'occupaient du sujet dans l'appareil d'État. C'est notre Premier ministre, M. Xavier Bettel, qui, dès son arrivée au pouvoir, a instauré le ministère dont j'ai la charge.

En réalité, deux ministres se trouvent à la tête de mon ministère, dont le Premier ministre, qui est donc de ce fait en même temps ministre de la digitalisation. Je suis quant à moi également en charge de la fonction publique. Une telle organisation montre notre attachement à la digitalisation, à laquelle nous souhaitons œuvrer de manière intensive. Jusqu'à l'instauration du ministère de la digitalisation, les administrations qui s'occupaient de l'informatique se heurtaient à des problèmes de coordination empêchant la digitalisation de progresser de manière conséquente.

L'implication, hautement symbolique, du Premier ministre dans la digitalisation envoie un signal fort à l'intérieur du pays comme à l'étranger. De même, le rôle dévolu au ministre de la fonction publique dans la digitalisation montre à quel point l'administration prend le sujet au sérieux. Les agents de l'État sont appelés à progresser dans cette voie afin de mieux communiquer avec les citoyens et les entreprises à propos du numérique.

Nous abritons sous notre tutelle un grand centre des technologies de l'information de l'État. Cette administration à part entière nous sert de bras armé technologique. Employant notamment des développeurs et des chefs de projets, ce centre s'occupe de mettre au point des solutions en réponse aux besoins spécifiques de l'administration, dont celle par exemple des contributions directes.

Le ministère de l'éducation nationale dispose de sa propre structure équivalente, de même que les services relatifs à la santé et à la sécurité sociale. Au niveau local, les échevins s'appuient sur un syndicat intercommunal de gestion informatique.

Nous abritons également sous notre tutelle un comité interministériel pour la digitalisation, réunissant les hauts fonctionnaires de l'ensemble des ministères intéressés par la question. Ce comité, en lien avec notre bras armé technologique, discute des projets des divers ministères, de manière qu'ils se concrétisent, mais aussi dans un esprit de partage des réalisations. De notre autorité dépend aussi un Haut comité à la transformation numérique. Instauré avant la crise liée à la Covid, il a pour mission de développer les échanges avec la société civile et les opérateurs du secteur privé afin que le numérique progresse au Luxembourg. Ses avancées ont beaucoup ralenti durant ces derniers mois, où la pandémie, de manière assez compréhensible, nous a contraints à donner la priorité à d'autres préoccupations.

Lors des cinq à six réunions annuelles du comité interministériel, les hauts fonctionnaires exposent leurs avancées respectives, puis échangent sur les difficultés qu'ils rencontrent avant de réfléchir ensemble à des moyens de les résoudre.

Nous avons mis en place un cadre national de l'interopérabilité, à la gouvernance spécifique. Ses prérogatives couvrent les trois pouvoirs de l'État. Il favorise la concertation et la sensibilisation, les échanges de bonnes pratiques, et l'instauration de synergies.

La souveraineté numérique me semble liée à différents facteurs, dont la bonne gestion d'Internet, des nouvelles technologies de l'information et de la communication, mais aussi des solutions numériques, sans oublier la protection du consommateur. La souveraineté numérique correspond à la capacité de décider et d'agir de manière autonome et en confiance, en tant qu'État, mais aussi au niveau de l'Union européenne, sur les aspects essentiels du numérique afin d'assurer le développement structurel, à long terme, de l'économie comme de la société.

Sur le plan européen, la notion de souveraineté numérique est apparue comme un moyen de promouvoir le *leadership* européen, mais aussi l'autonomie stratégique dans le domaine du numérique. Depuis quelques années, le numérique et toute innovation qui s'y rapporte sont perçus comme un secteur d'intérêt stratégique, également primordial pour l'Union européenne. Il va de soi que les objectifs définis aux niveaux national et européen pour atteindre cette souveraineté numérique doivent se combiner et s'harmoniser, puisque c'est seulement dans l'Union européenne que nous parviendrons à garantir cette souveraineté, eu égard à l'avance prise par beaucoup d'autres pays extra-européens en matière de numérisation.

Depuis les années 2000, le Luxembourg a beaucoup investi dans les Technologies de l'information et de la communication (TIC) et a promu le développement des infrastructures correspondantes. Le secteur du numérique a pris son essor au Luxembourg grâce à des investissements substantiels dans le réseau à haut débit et la construction de centres de données. Pays de petite taille, le Luxembourg peut se targuer d'une très haute densité de centres de données sur son territoire. De fait, cette densité s'y révèle la plus élevée au monde, puisque nos centres de données hautement qualifiés couvrent une superficie de près de 47 000 mètres carrés.

Reconnaissant l'importance du développement des nouvelles technologies, nous avons défini en 2019 une stratégie en matière d'Intelligence artificielle. Nous ambitionnons, à travers elle, de contribuer au développement des sociétés numériques. Récemment, un *hub* régional de GAIA-X a été lancé au Luxembourg. Cette initiative joue un rôle majeur dans le rassemblement et le développement des exigences communes pour une infrastructure de données européennes à la fois fédérée, sécurisée et souveraine.

Notre ministère de la digitalisation a vu le jour en 2018, soit avant la crise liée à la Covid. Très honnêtement, je dois vous avouer que bien des évolutions exceptionnelles sont survenues dans l'administration en raison de la pandémie. Du point de vue de la digitalisation, la crise sanitaire a contraint les services publics à réaliser un bond en avant spectaculaire. Sans doute en est-il allé de même en France. Si j'ose dire, nous n'aurions pas imaginé tout ce qui s'est mis en place au cours des douze derniers mois. Nous pourrions d'ailleurs revenir plus en détail sur les démarches qui ont basculé en ligne, ou encore sur la généralisation du télétravail.

Vous évoquiez tout à l'heure l'éducation. La crise a obligé les élèves et leurs enseignants à passer au *homeschooling*, selon le nom que nous donnons au Luxembourg à l'école à la maison. Heureusement, nos infrastructures étaient globalement prêtes à affronter cette transformation des pratiques, ce qui a facilité la transition de l'enseignement traditionnel vers la classe à distance au cours des douze à quatorze derniers mois.

M. Philippe Latombe, rapporteur. L'accélération subite de la numérisation, liée à la crise sanitaire, a-t-elle fourni l'occasion de modifier la gestion de l'administration ou ses relations avec les usagers ? A-t-elle changé l'organisation interne des ministères eux-mêmes, ou les transformations n'ont-elles porté que sur les infrastructures ?

M. Marc Hansen. Un réel changement s'est opéré dans l'état d'esprit des fonctionnaires et des employés du secteur public. Je ne doute pas qu'en France également, avant la crise, les moindres projets obéissaient systématiquement à une conception minutieuse où aucune étape n'était laissée au hasard, pas plus celle des études préalables que de la mise en œuvre. Il manquait à l'administration étatique un état d'esprit propre aux *start-up*.

Lors de sa création, notre ministère se présentait comme une sorte de *start-up* ministérielle ne comptant que deux collaborateurs : le Premier ministre et moi-même. Nous

avons réuni des équipes autour de la digitalisation, mais, jusqu'à la crise sanitaire, il fallait sans cesse les inciter à aller de l'avant.

La Covid, au Luxembourg comme en France d'ailleurs, a obligé le gouvernement à prendre des décisions qu'il a aussitôt fallu traduire concrètement par des démarches jusque-là inédites en ligne, que ce soit pour demander des congés ou un passage à temps partiel pour raisons familiales, ou encore pour s'inscrire à des tests de dépistage du coronavirus. Le temps manquait pour étudier une version-bêta. Les nouvelles mesures ont dû se mettre en place d'un jour à l'autre. Les erreurs dues à la précipitation ont été rectifiées sitôt décelées. Sans doute une telle évolution n'aurait-elle pas pu se concevoir dans le secteur public avant la pandémie. À tout le moins, il lui aurait fallu plus de temps pour aboutir, du fait des réticences des équipes. La crise liée à la Covid a contraint l'administration à mettre en ligne des formulaires du jour au lendemain. Pour peu que nous conservions une part de cet état d'esprit d'innovation, sans pour autant rester dans une logique d'urgence, c'est-à-dire en revenant à une plus grande rigueur, nous parviendrons à n'en garder que les bénéfices, et ainsi, notre progression continuera.

Je vais vous citer quelques chiffres significatifs. Nous disposons au Luxembourg d'une grande plateforme « guichet.lu », tenant lieu de guichet unique aux citoyens et aux entreprises souhaitant contacter les services publics par voie numérique. Cette plateforme héberge un espace personnalisé « myguichet.lu », où chacun peut déposer aussi bien une demande de plaque d'immatriculation que de permis de pêche, par exemple.

En 2019, 500 000 démarches au Luxembourg avaient été effectuées *via* cette plateforme. De janvier à novembre 2020, ce nombre est passé à 1,8 million. Un grand nombre de ces démarches étaient dictées par la situation sanitaire : des entreprises ont ainsi sollicité des aides ou un moyen de tester leurs employés au coronavirus. Au mois de février 2020, nous n'avions pas dénombré plus de 4 000 minutes de vidéoconférence entre agents de l'État. Le confinement a multiplié ce chiffre par 34. Les agents du service public ont été rapidement équipés pour le travail à domicile. En somme, la digitalisation a subi une formidable accélération, avec tous les avantages et les inconvénients qu'une transformation aussi subite peut comporter. Il reste encore des points à améliorer, mais je suppose qu'il en va de même en France.

Dans le domaine de l'éducation, certaines semaines, la totalité des élèves et des professeurs luxembourgeois ont été en *homeschooling*. Du jour au lendemain, 12 000 enseignants et 160 000 élèves ont ainsi dû poursuivre leurs cours en ligne *via* Zoom ou Teams. D'autres semaines, une moitié des effectifs se rendait à l'école avant de céder la place à l'autre, à partir du lundi suivant. C'est un basculement spectaculaire qui a eu lieu, du réel au virtuel.

M. Philippe Latombe, rapporteur. Comment les citoyens perçoivent-ils la numérisation ? Comment réussissez-vous, non seulement à les convaincre de se connecter à votre plateforme tenant lieu de guichet unique, mais à leur donner confiance en ce dispositif, notamment pour ce qui a trait à la collecte et au traitement des données ? Ce problème de confiance en l'utilisation, par l'administration, des données personnelles, se pose avec beaucoup d'acuité en France. L'administration luxembourgeoise a-t-elle conclu un contrat avec les citoyens, comme en Estonie, permettant à ceux-ci de savoir quel service accède à leurs données et pour quelle raison ? Ou ces informations ne leur sont-elles pas plus divulguées qu'aux citoyens français ?

M. Marc Hansen. Avant la crise déjà, la population luxembourgeoise accordait une grande confiance aux outils numériques de l'administration. Un sondage d'opinion commandé

à un prestataire, TNS Ilres, avait révélé un taux d'adhésion de la population à « myguichet.lu » de 80 à 90 %. Conformément à la loi, cette plateforme permet à ses usagers de savoir à tout moment quelles administrations ont eu accès, au cours des six derniers mois, à la partie qui les concerne du Registre national des personnes physiques répertoriant les données des Luxembourgeois. Si un service public a consulté les données d'un citoyen, sans que celui-ci comprenne pour quelle raison, cette personne peut interpeller le service en question, auquel il revient de s'expliquer. Il arrive par exemple à un père ou à une mère de ne pas comprendre pourquoi une administration a consulté ses données à la suite d'une demande de bourse déposée par son conjoint, pour leur enfant étudiant. Nous attachons une importance extrême à la transparence et au respect des données personnelles.

Il ne faut pas oublier, dans les discussions autour du numérique, d'évoquer l'inclusion digitale, qui constitue d'ailleurs l'un des piliers de la stratégie de notre ministère. Le Luxembourg a la chance de bénéficier de bonnes connexions au réseau. La plupart des citoyens ont acquis, par leur éducation, des compétences numériques. Toutefois, il ne faudrait pas laisser de côté la frange de la population moins impliquée dans ce domaine. Nous organisons des formations et des cours, avec des associations, pour les personnes âgées, encore que les connaissances en matière de numérique ne dépendent pas seulement de l'âge. La question de l'inclusion digitale mérite que nous la prenions très au sérieux.

M. Philippe Latombe, rapporteur. Revenons au traitement des données personnelles, mais sous l'angle technologique, cette fois. Vous avez évoqué le projet de *hub* luxembourgeois de GAIA-X. Comment appréhendez-vous les technologies liées au *cloud* dans vos politiques ? Comment vous assurez-vous de ne pas trop dépendre de Google, Apple, Facebook, Amazon ou Microsoft (les GAFAM) ? À moins qu'une telle perspective ne vous inquiète pas outre mesure ?

Ma question peut sembler abrupte, mais elle taraude beaucoup les Français en ce moment, depuis, entre autres, la polémique liée à l'hébergement de notre Health data hub.

M. Marc Hansen. J'ai déjà en partie répondu à votre question en évoquant les nombreuses bases de données implantées au Luxembourg. Nos services technologiques étatiques exploitent leurs propres centres de données. Or ceux-ci génèrent une grande confiance. La première ambassade numérique de l'Estonie est implantée au Luxembourg. Le fait qu'un grand nombre de données de nos concitoyens transite déjà par des centres implantés sur notre territoire favorise la confiance des particuliers comme des entreprises.

M. Philippe Latombe, rapporteur. Compte tenu du nombre de centres de données présents au Luxembourg, votre pays doit disposer aussi de tout un tissu d'entreprises du numérique. Comment développez-vous leur activité ? L'administration luxembourgeoise multiplie-t-elle les appels d'offres en ciblant de préférence les sociétés locales ? Menez-vous une politique spécifique de création et d'accompagnement de *start-up*, de manière à préparer l'avenir ?

M. Marc Hansen. Je ne fournirai à vos questions qu'une réponse limitée, car c'est le ministère de l'économie qui s'occupe de la plupart des dispositifs auxquels vous songez.

Nous avons lancé, voici quelques mois, un nouvel outil baptisé « GovTechLab ». Des projets semblables ont commencé à voir le jour dans plusieurs autres pays dans le monde. Notre centre informatique fournit en principe une solution aux besoins numériques de l'administration. Nous ne voulons toutefois pas y réinventer des technologies existantes. Nous n'hésiterons donc pas à nous tourner vers le secteur privé, grâce à une nouvelle organisation des marchés publics, au cas où celui-ci disposerait de solutions adaptées à nos demandes.

En somme, notre centre informatique ne développera plus systématiquement les projets nécessaires aux services publics. Concrètement, nous lançons des défis aux acteurs privés pour résoudre certains problèmes que rencontre l'État. Des jurys, composés entre autres d'agents de nos services, départagent les candidatures. Un premier projet pilote est en cours de finalisation. Dès que la situation sanitaire le permettra, nous organiserons des séminaires avec ces entités privées dans un espace intégré à notre centre informatique pour qu'elles œuvrent en réseau avec l'administration.

J'estime important de soutenir et de promouvoir le secteur numérique, et d'encourager les entreprises à investir dans la recherche et le développement, et dans l'innovation. Le ministère de l'économie encadre le secteur numérique par le biais de missions, d'actions de soutien aux *start-up*, et de nombreux programmes, notamment destinés à l'artisanat.

M. Philippe Latombe, rapporteur. Vous avez cité l'Estonie, qui héberge au Luxembourg son ambassade numérique. Coopérez-vous avec certains pays européens plutôt qu'avec d'autres ? Estimez-vous plus facile de nouer des échanges ou des partenariats avec des petits pays, ou travaillez-vous aussi bien avec vos homologues français ou allemands ?

M. Marc Hansen. Le Luxembourg reste bien sûr très ouvert aux pays voisins, dont la France. Nous échangeons quotidiennement avec l'ensemble des pays européens. Notre Premier ministre se trouvait à Paris, voici deux jours, pour échanger notamment avec les responsables des politiques du numérique en France.

Des échanges quotidiens ont également lieu entre notre pays et les régions frontalières voisines. Je ne me lasse pas de répéter que, dans le domaine du numérique, il est bon de nouer des échanges fructueux avec de nombreux acteurs. Au lieu d'adopter une attitude de défense de la souveraineté numérique, il vaut parfois mieux la promouvoir, par l'échange de bonnes pratiques et le soutien aux acteurs susceptibles d'y participer. Échanger avec d'autres pays s'avère en effet plus utile que de s'en tenir à un schéma purement national.

M. Philippe Latombe, rapporteur. Les programmes européens annoncés, les initiatives déjà lancées telles que GAIA-X ou encore les projets de *Digital Services Act (DSA)*, de *Digital Markets Act (DMA)* et de *DGA* vous semblent-ils œuvrer dans la bonne direction ? Apporteront-ils « un coup de pouce » dans la numérisation et la transformation de votre administration ?

M. Marc Hansen. Ces projets nous aideront sûrement. Nous devons, selon moi, coopérer pour avancer. Or, les initiatives que vous citez soutiendront à n'en pas douter les progrès des différents États membres de l'Union européenne.

M. Philippe Latombe, rapporteur. Les divers pays de l'Union européenne vous semblent-ils tous parvenus au même degré de maturité sur ces sujets, ou certains vous paraissent-ils plus à la pointe, comme le Luxembourg, alors que d'autres s'intéresseraient plus à d'autres champs d'action ? Pressentez-vous des difficultés à rallier certains gouvernements aux projets de *DSA*, de *DMA* et de *DGA*, qui ne se concrétiseront pourtant pas sans l'unanimité des membres de l'Union européenne ?

M. Marc Hansen. Je préfère m'en tenir à une certaine humilité quand je vous entends citer le Luxembourg parmi les pays à la pointe. Dans n'importe quel domaine, on trouve des pays plus avancés que d'autres. Malgré tout, si nous faisons l'effort d'avancer ensemble, par l'échange de bonnes pratiques, finalement, tout le monde y gagnera. Le Luxembourg tente de coopérer avec les autres pays de l'Union européenne. S'il est vu comme « à la pointe » du

numérique, alors autant se réjouir de sa capacité à contribuer aux progrès des autres dans ce domaine.

M. Philippe Latombe, rapporteur. Je souhaiterais ouvrir une parenthèse à propos de l'arrêt *Schrems* II et de l'extraterritorialité du droit américain. Votre ministère s'en préoccupe-t-il beaucoup ? Quel type de solution appelez-vous de vos vœux pour régler les problèmes posés par le *Clarifying lawful overseas use of data Act* (*Cloud Act*) ? Souhaitez-vous que des négociations transatlantiques aboutissent rapidement ? Peut-être aurais-je plutôt dû adresser ma question au ministère de l'Économie. Certaines entreprises luxembourgeoises se heurtent-elles aux mêmes difficultés que les sociétés françaises en matière de transfert de données de l'Union européenne vers les États-Unis ?

M. Marc Hansen. En effet, il serait plus pertinent que vous abordiez ces points avec notre ministre de l'économie ou celui des affaires étrangères.

M. Philippe Latombe, rapporteur. Comment envisagez-vous, à moyen terme, la numérisation de votre administration et le rôle que pourraient y jouer de nouvelles technologies en pleine émergence comme l'Intelligence artificielle, ou du moins, l'apprentissage automatique, l'informatique quantique, s'ils voient le jour à cet horizon temporel, ou encore la *blockchain* ?

M. Marc Hansen. En tant que ministre de la Fonction publique, j'ai sous ma tutelle un Institut national de l'administration publique, en charge de la formation initiale et continue des agents du service public. Nous sommes en train de transformer cet institut en « *digital academy* » pour faire connaître aux agents de l'État les dernières avancées en matière de numérique. Il me paraît de la plus haute importance qu'un agent public confronté à un citoyen ou une entreprise au fait de ces thématiques soit capable d'en traiter en toute connaissance de cause. Nous travaillons à la mise en place de modules et de cours à destination des fonctionnaires. Nous nous félicitons de nos avancées dans ce domaine, qui revêt une importance cruciale.

En 2019, notre gouvernement a adopté une stratégie relative à l'Intelligence artificielle, soutenant le développement de l'Intelligence artificielle centrée sur l'humain. En 2020, une consultation publique à ce sujet nous a permis de comprendre comment les citoyens appréhendaient l'Intelligence artificielle, et d'identifier leurs besoins, leurs craintes et leurs attentes. Nous avons lancé en interne un projet étatique baptisé « *AI4GOV* » et créé un comité interministériel pour nous occuper de ce sujet. Il s'agit d'encourager les ministères et les administrations à en faire usage par le soutien de projets concrets. Le cadastre a par exemple soumis un projet de ce type, relatif à la topographie des terrains. Le comité interministériel assure un accompagnement technique, juridique et éthique.

Nous avons lancé un projet de *blockchain* du secteur public permettant au gouvernement d'expérimenter et de développer de nouvelles applications réservées à l'administration, tout en prévoyant des interactions avec le secteur privé. L'une de ces applications concerne les bourses d'études et vise à faciliter les échanges des étudiants avec les banques, dans les cas où ils souhaiteraient contracter un prêt pour financer leur formation.

Nous échangeons avec les communes à propos d'un projet de *blockchain* portant sur les permis de construire.

M. Philippe Latombe, rapporteur. Comment arrivez-vous à définir une doctrine valable pour le gouvernement et l'administration, puis à l'appliquer sur le plan local, à l'échelon des communes, par exemple, ou en tout cas, au niveau le plus proche des citoyens ?

Je songe notamment aux projets de villes intelligentes. Établissez-vous des recommandations à l'intention des municipalités pour qu'elles déclinent à leur échelle votre stratégie étatique ?

M. Marc Hansen. Les communes du Luxembourg attachent une grande importance à leur autonomie. J'émettrai donc quelques réserves à l'égard de notre capacité à leur communiquer une doctrine. S'il n'existe pas de doctrine en tant que telle, les différents acteurs échangent cependant beaucoup. Comme je le mentionnais tout à l'heure, un syndicat intercommunal de gestion informatique mène des discussions fructueuses avec les opérateurs techniques. Des coopérations se mettent en place.

Concernant l'administration proprement dite, les deux ministres chargés de la digitalisation au sein du Conseil des ministres prennent les décisions qui s'imposent. Transposer ces décisions aux différents échelons des services publics s'avère dès lors assez aisé. Notre nouvelle gouvernance a simplifié les processus.

M. Philippe Latombe, rapporteur. Souhaiteriez-vous revenir sur un sujet, en lien avec la souveraineté numérique, qu'il vous paraîtrait nécessaire de mettre en avant ?

M. Marc Hansen. Une vingtaine de sujets me viennent à l'esprit, mais ils dépasseraient le cadre de cette audition.

Entre experts ou, du moins, entre ceux qui s'y connaissent en matière de nouvelles technologies, il arrive de céder à la tentation de « faire de l'art pour l'art », selon l'expression française consacrée, c'est-à-dire de recourir à la numérisation en vue de la simple satisfaction que procure le basculement vers le numérique. Nous ne devons pas perdre de vue dans l'intérêt de qui nous agissons, et nous demander si notre travail apportera une plus-value aux autres en tant qu'êtres humains, dans leur travail ou leur vie quotidienne. Une administration qui utiliserait le numérique uniquement par attrait pour les nouvelles technologies risquerait de perdre la confiance des citoyens et des entreprises. Il faut toujours songer à l'individu et à ce que la digitalisation lui apporte. Les citoyens nourrissent des craintes et des doutes qu'il convient de prendre au sérieux afin de les dissiper plutôt que de les balayer. Il importe de convaincre les usagers de l'administration que, loin de les priver de certains services, nous leur en offrons de supplémentaires.

M. Philippe Latombe, rapporteur. Cela signifie-t-il que la crise liée à la Covid aura marqué un avant et un après dans la recherche de solutions numériques au bénéfice des citoyens ? Est-ce là l'un des enseignements qu'il convient d'en tirer ?

M. Marc Hansen. Cette crise a mis en évidence les nombreux besoins des citoyens, liés aux problèmes posés par la pandémie. La digitalisation et la rapidité des évolutions qu'elle entraîne ont prouvé leur capacité à leur venir en aide. Il me semble que cette idée restera dans les esprits. Si nous continuons dans cette voie de la digitalisation, à l'issue de la campagne de vaccination, le pass sanitaire, en tant qu'outil informatique standardisé au niveau européen, pourra, dans le même esprit, faciliter les déplacements d'un pays à l'autre au sein de l'Union européenne en donnant une plus grande liberté de mouvement à ses utilisateurs.

M.Philippe Latombe, rapporteur. Je vous poserai une dernière question sur l'éducation. La crise liée à la Covid va-t-elle, à votre avis, changer la pratique de l'enseignement ? Faut-il revenir à du présentiel ? L'école à la maison ne constitue-t-elle en fin de compte qu'une béquille ou un pis-aller ? Ou s'achemine-t-on, au contraire, vers un modèle hybride dans les années à venir ?

M. Marc Hansen. Je crois l'enseignement présentiel indispensable à la plupart des enfants. Il m'apparaît d'autant plus essentiel qu'il permet d'acquérir les compétences sociales que s'évertue à inculquer le système scolaire. C'est d'ailleurs pour cette raison qu'au Luxembourg, nous avons maintenu les écoles ouvertes aussi longtemps que possible. À certains moments où le risque de contamination au coronavirus devenait trop élevé, les outils numériques nous ont aidés. Néanmoins, il faut en revenir à l'enseignement présentiel. Il s'avère très difficile d'assurer la classe à de tout jeunes enfants de trois ou quatre ans par écran interposé.

Dans beaucoup de lycées, nous allons introduire des cours de sciences spécifiques dans l'idée d'inculquer aux élèves des compétences en électronique et en informatique.

Nous nous apercevons par ailleurs que les outils numériques peuvent déboucher sur une forme d'enseignement hybride. Jusqu'à la veille de la pandémie, un élève immobilisé chez lui pour des raisons médicales ne pouvait pas assister à ses cours. Désormais, l'école à la maison lui permet de ne pas perdre tout contact avec sa classe et ses professeurs. Des situations se présenteront, à n'en pas douter, où le recours à l'école à la maison présentera un intérêt certain.

Avant la pandémie, au Luxembourg, du moins, les visioconférences restaient peu utilisées, aussi bien dans l'enseignement qu'au travail ou dans le monde de la politique. Vous et moi communiquons aujourd'hui *via* ce système. Sans la pandémie, je me serais probablement rendu à Paris, où nous aurions entamé un échange plus jovial en abordant, au fil de la conversation, d'autres sujets. Dans certains contextes, les outils numériques montrent leur utilité.

Il faut repenser le monde du travail également, en se penchant sur le télétravail. Si, voici quatorze mois, j'avais parlé d'une réunion Zoom, les personnes de mon entourage auraient cherché le nom de ce dispositif numérique dans le moteur de recherche de Google. Aujourd'hui, la plupart d'entre nous utilisent ces solutions digitales et d'autres encore. Il nous reste à acclimater ces nouveaux outils à nos anciennes façons de travailler. Des leçons devront en être tirées, même si nous gagnerons sans doute à renoncer à certaines pratiques au fil du temps.

M. Philippe Latombe, rapporteur. Votre ministère a été créé en 2018 sous la tutelle de deux ministres, dont le Premier ministre. Une telle organisation va-t-elle perdurer ? D'autres pays européens s'en inspireront ou la prendront-ils pour modèle ?

M. Marc Hansen. Depuis la pandémie, beaucoup de pays nous contactent, en vue d'échanger avec le Premier ministre ou moi-même. Nous participons à des conférences. Un intérêt certain se manifeste envers notre ministère de la digitalisation. Par son existence même, il compte donc beaucoup, y compris au-delà de nos frontières. Certains pays s'interrogent sur la manière d'adapter notre gouvernance. Au Luxembourg, la digitalisation ne s'opère pas seulement dans le ministère qui lui est consacré. Chaque ministère nourrit ses propres projets dans ce domaine. L'importance donnée à la digitalisation au sein de notre administration aide celle-ci, de l'intérieur, à prendre des décisions qui favorisent le recours aux nouvelles technologies. Des responsables politiques d'autres pays nous interrogent sur notre expérience. Sans doute certains comptent-ils suivre le même chemin que nous.

Audition de M. Nicolas Lerner, administrateur civil hors classe, directeur des services actifs de la police nationale, directeur général de la sécurité intérieure (DGSI) (ministère de l'intérieur)
(4 juin 2021)

Présidence de M. Philippe Latombe, rapporteur.

(Les propos tenus au cours de l'audition à huis clos n'ont pas fait l'objet d'un compte rendu.)

Audition ouverte à la presse de M. Margiris Abukevicius, vice-ministre de la défense nationale de la République de Lituanie. *(8 juin 9021)*

Présidence de M. Philippe Latombe, rapporteur.

M. Philippe Latombe, président et rapporteur. Nous avons l'honneur d'auditionner ce matin M. Margiris Abukevicius, vice-ministre de la défense nationale de la République de Lituanie.

Depuis près d'un an, notre mission d'information poursuit ses travaux sur les principaux enjeux de la souveraineté numérique. Parmi les thèmes que nous avons successivement abordés figure évidemment la cybersécurité, qu'il s'agisse de la nature et du niveau de la menace ainsi que de la réponse à y apporter.

M. le ministre, votre carrière et vos responsabilités ministérielles témoignent de votre exceptionnelle expertise dans ce domaine. C'est la raison pour laquelle nous attachons un grand prix à pouvoir vous entendre et échanger avec vous aujourd'hui.

En guise de propos liminaire, j'aborderai trois sujets.

D'abord, pourriez-vous nous partager votre conception de la souveraineté numérique ? Il s'agit d'une question rituelle que j'adresse à chaque personne auditionnée, et qui procède de la grande diversité de définitions qui peuvent être associées à cette notion. Comment appréhendez-vous donc ce concept et quelle peut être sa traduction concrète en termes de politiques publiques ?

Par ailleurs, nous souhaiterions connaître votre appréciation de la menace cyber et de ses différentes formes. Quel est l'état de la coopération en matière de cyberdéfense, qu'il s'agisse de coopérations bilatérales ou de la coopération au sein des instances de l'Union européenne ou de l'Organisation du traité de l'Atlantique nord (OTAN) ?

Enfin, comment jugez-vous le niveau de sensibilisation de la population ? Comment agissez-vous pour diffuser une culture de la protection contre le risque cyber au sein des acteurs publics ou privés ?

M. Margiris Abukevicius, vice-ministre de la défense nationale de la République de Lituanie. Merci beaucoup pour ces propos liminaires sympathiques. C'est un grand privilège d'être présent parmi vous au sein de l'Assemblée nationale et de vous faire part de notre point de vue sur la thématique de la cybersécurité. Nous venons récemment d'assister à une conférence dédiée à ce sujet, et je suis convaincu que vos travaux pourront bénéficier des différents points de vue exprimés par les autres pays de l'Union européenne.

Je commencerai par rappeler quelques définitions afin de répondre à votre première question relative à notre conception de la souveraineté numérique. De notre point de vue, trois éléments sont à prendre en compte pour répondre clairement à cette interrogation.

D'abord, quels sont les enjeux et de quoi parlons-nous ? Ici, le plus important est de bien comprendre les technologies dans le contexte de l'économie, de la concurrence, de la politique, mais aussi et surtout de la sécurité nationale. En effet, l'accès aux nouvelles technologies façonnera notre avenir et déterminera non seulement les avantages en termes technologiques, mais également le pouvoir économique et politique, ainsi que les structures

de puissance au niveau mondial. Ce premier élément permet déjà de répondre partiellement à cette question relative à la souveraineté numérique.

Ensuite, quels sont les acteurs principaux ? Ici, il est essentiel d'identifier clairement les interactions entre les différents acteurs impliqués, notamment au niveau européen. Aujourd'hui, la Chine est clairement le premier acteur et la première puissance remettant en question le *statu quo* et les structures de puissance et de pouvoir. C'est vrai dans le domaine technologique, mais également de manière plus générale, puisque la Chine et l'Occident se font concurrence jusque dans leurs systèmes politico-économiques. Pour le sujet qui nous intéresse aujourd'hui, nous devons évoquer la technosphère chinoise, qui se développe de manière très active, ainsi que la technosphère occidentale, à laquelle nous appartenons en tant qu'Européens.

J'en profite d'ailleurs pour expliquer ce que j'entends par Occident ou monde démocratique, même s'il est sans doute plus risqué de m'exprimer à ce sujet devant l'Assemblée nationale que dans le cadre d'une conférence moins formelle. Lorsque je fais référence à l'Occident, je pense bien entendu et avant tout aux États-Unis. La Chine et les États-Unis sont deux pôles de compétition technologique. De mon point de vue, l'Union européenne n'a d'autres choix que de travailler étroitement avec les Américains. Des voix s'élèvent parfois pour promouvoir une relation triangulaire entre les États-Unis, l'Europe et la Chine, mais cette stratégie me paraît plutôt risquée. La coopération avec les Américains paraît au contraire la seule option viable pour que l'Europe soit considérée comme un acteur crédible capable de peser globalement. En tout état de cause, le Parlement est probablement l'endroit idoine pour discuter de la manière dont nous pourrions garantir cette coopération entre Américains et Européens en matière de technologies. Dans cette perspective, l'initiative visant à instituer un conseil du commerce et de la technologie entre Européens et Américains – et qui est au cœur des préparatifs du prochain sommet de l'OTAN – semble particulièrement pertinente. Les détails de sa mise en œuvre restent encore à régler, mais le message politique envoyé par la création de cette instance me semble tout à fait clair et très important.

Enfin, nous devons nécessairement nous interroger sur la manière de procéder pour sécuriser notre accès aux technologies et préserver le *statu quo*. Plusieurs éléments sont à prendre en compte. En premier lieu, il est primordial de faire évoluer nos mentalités, et c'est sans doute le message le plus important que je m'efforce de promouvoir. La Chine a jusqu'ici fortement tiré parti de sa coopération étroite avec les États-Unis, et nous devons nous en accommoder. En revanche, je suis convaincu que davantage de coopération avec Pékin ne peut qu'être contreproductif pour l'Union européenne. Il est donc crucial que ce changement d'état d'esprit survienne dans les plus brefs délais.

Deuxièmement, nous devons avoir conscience de la dépendance de nos chaînes d'approvisionnement. Dans différents secteurs, et pas uniquement dans le domaine technologique, nos chaînes d'approvisionnement sont extrêmement dépendantes de la Chine, ce qui est facteur de risques économiques et sécuritaires. D'ailleurs, en matière de sécurité, plusieurs aspects sont à prendre en compte, notamment en termes de sécurité nationale. Lorsque l'on analyse l'environnement légal et juridique en Chine, on constate que les entreprises technologiques sont contraintes de coopérer avec le régime communiste. En parallèle, un certain nombre d'activités malveillantes ont pu être clairement imputées à la Chine, comme le vol d'adresses IP ou diverses opérations d'espionnage. La volonté de nuire est donc bien réelle. Ainsi, à mesure que notre dépendance vis-à-vis des technologies s'accroîtra, les cibles potentielles d'attaques seront de plus en plus nombreuses.

Nous devons également discuter des menaces très concrètes de cybersécurité auxquelles nous sommes exposés. À cet égard, je me permettrai d'évoquer plusieurs rapports

et analyses de sécurité produits par notre centre national de cybersécurité. Je pourrai d'ailleurs vous en laisser quelques exemplaires si vous souhaitez en apprendre davantage. L'année dernière, nos experts ont conduit une analyse de sécurité sur les caméras fabriquées en Chine. Cette année, ils publieront un autre rapport sur les téléphones fabriqués en Chine. Ces équipements sont source de multiples menaces en termes de cybersécurité. Il est par exemple possible d'intercepter le contenu des caméras, mais aussi de capter, utiliser et diffuser des informations sensibles stockées dans les téléphones, à partir de messages cryptés et d'applications intégrées dans les terminaux téléphoniques. Ces problématiques de cybersécurité associées et intégrées aux technologies sont donc parfaitement identifiées.

Au-delà du changement de mentalité nécessaire pour sécuriser l'accès aux technologies, nous devons également protéger les infrastructures critiques. Nous avons multiplié les échanges autour de la 5G et de la manière de garantir l'implication de fabrications et de fournisseurs de confiance dans la construction de nos réseaux. En Lituanie, le Parlement a récemment adopté une loi sur les communications électroniques, qui introduit des critères très précis pour identifier ces fabricants de confiance, que nous définissons comme des entreprises provenant des États membres de l'OTAN, de l'Union européenne ou de l'Organisation de coopération et de développement économique (OCDE). Ce genre d'initiative mériterait d'être reproduit dans d'autres domaines critiques, par exemple dans le secteur de l'énergie, marqué par une forte dépendance à l'égard des produits chinois pour ce qui relève de l'énergie solaire, mais aussi dans le secteur des transports et des villes intelligentes. À l'avenir, nos vies seront extrêmement dépendantes de ces technologies. Il est donc primordial de protéger ces infrastructures.

Pour en revenir à l'exemple lituanien, j'évoquerai deux manières de protéger ces infrastructures critiques. D'abord, nous avons mis en place un solide mécanisme de sélection dans le cas des investissements et des marchés publics. Néanmoins, dans la mesure où cet outil s'avère insuffisant pour protéger efficacement nos infrastructures, nous avons commencé à travailler sur une législation dédiée. Tout comme pour la 5G, nous introduirons un critère de sécurité nationale dans l'ensemble des marchés publics de construction des infrastructures critiques, qui seront réservés non seulement aux entreprises des pays membres de l'OTAN, de l'Union européenne et de l'OCDE, mais plus largement aux entreprises des pays partageant nos valeurs et principes démocratiques, avec qui nous collaborerons pour construire ces infrastructures.

Enfin, pour garantir cette protection et cet accès aux technologies, il me paraît essentiel de raccourcir, d'occidentaliser et d'européaniser nos chaînes d'approvisionnement, afin de nous prémunir des risques que nous venons d'évoquer.

Sur le plan politique, nous savons que l'Europe investira de manière significative et collective dans la transformation numérique et dans la transition énergétique. Logiquement, ces fonds devront naturellement bénéficier aux entreprises européennes. Cela dit, il est encore plus primordial que la Chine et les entreprises chinoises n'en bénéficient pas, étant entendu qu'elles en sont aujourd'hui bénéficiaires. Le changement de mentalités que nous appelons de nos vœux doit donc parallèlement s'accompagner de nouveaux paradigmes politiques.

Comme vous l'avez compris au travers de cette réponse relativement longue à votre question initiale, notre conception de la souveraineté numérique repose avant tout sur le primat de la coopération transatlantique. Nous privilégions les alliances technologiques occidentales, et non la souveraineté technologique de l'Europe.

Votre seconde question portait sur la coopération en matière de cyberdéfense. Il s'agit également d'un sujet extrêmement vaste, notamment si on pense à la coopération européenne,

qui vous intéresse plus particulièrement. En l'occurrence, la Lituanie est l'un des pays les plus ouverts à la coopération internationale en matière de cybersécurité. Dans ce domaine, j'évoquerai une initiative concrète que nous avons promue depuis près de deux ans.

En tant que pays européens, nous avons tous pris l'habitude d'échanger des informations de cybersécurité avec l'Union européenne et avons constitué des réseaux dédiés. Dans le même temps, de nombreux pays ont tendance à vouloir apporter des réponses nationales en matière de gestion des incidents de cybersécurité. Il n'est ainsi pas rare d'entendre des dirigeants français affirmer que ce sujet relève de prérogatives nationales. Pour notre part, nous considérons nécessaire de dépasser cette approche. Les investissements dans les capacités nationales sont évidemment nécessaires, mais cette stratégie plutôt facile à envisager pour les grands pays s'avère difficile à mettre en œuvre pour les petits États, dont les capacités nationales ne sont pas suffisantes pour faire face aux risques de cybersécurité.

Dans cette logique, nous avons piloté la création d'équipes d'intervention rapide en matière de cybersécurité (*Cyber Rapid Response Teams)* au niveau européen. Dans le format de l'Union européenne, la mise en place d'équipes opérationnelles à l'échelle communautaire s'avère toujours difficile et sensible. Malgré tout, nous sommes parvenus à trouver un compromis avec un certain nombre d'États membres à même de prendre des décisions, avec qui nous avons élaboré des capacités de réponse utilisables dans différents scénarios. Si nous sommes évidemment prêts à appuyer les institutions communautaires et les pays partenaires contribuant à cette initiative, nous sommes également disposés à assister d'autres États membres de l'Union européenne qui n'y sont pas associés.

Les deux dernières années ont été marquées par de véritables avancées pour ces équipes. Nous avons récemment conduit un exercice de déploiement en différents endroits pour aider à la résolution d'incidents de cybersécurité affectant plusieurs ambassades. En outre, et malgré le contexte pandémique Covid-19, nous avons élaboré des procédures logistiques permettant à ces équipes de gérer efficacement des incidents de cybersécurité. Enfin, nous avons mené plusieurs exercices de certification qui nous permettront de mettre en place des capacités d'intervention pleinement opérationnelles. En résumé, retenez que nous sommes parvenus à constituer une équipe multinationale de six États membres, qui peut être utilisée et déployée dans différents scénarios.

Bien entendu, d'autres initiatives de cyberdéfense reposent sur la coopération internationale. Néanmoins, l'initiative précitée est un projet phare et un projet européen, qui trouve son origine dans le dispositif de coopération structurée permanente (*Permanent Structured Cooperation, PESCO)* cadrant la coopération des États membres en matière de sécurité et de défense. Il s'avère que nous avons utilisé cet outil l'an dernier, en amont de nos élections parlementaires, afin de mettre à l'épreuve la résilience de nos réseaux. Comme me l'ont confirmé mes interlocuteurs français, la sécurité des élections est également un enjeu majeur dans votre pays, notamment en perspective de l'élection présidentielle de 2022. Nous sommes donc convenus d'approfondir nos discussions et de renforcer la coopération franco-lituanienne sur le sujet, avec l'objectif de sécuriser les processus électoraux, dans lesquels les questions de cybersécurité – mais aussi de désinformation – sont de plus en plus prégnantes.

J'en arrive à votre dernière question, qui est certainement la plus complexe à traiter. Quoi que l'on mette en œuvre, les menaces de cybersécurité sont une réalité avec laquelle nous devrons composer, puisqu'elles ne disparaîtront pas. À ce titre, je pense que le facteur humain et la sensibilisation sont des enjeux critiques en matière de cybersécurité. Il ne s'agit pas seulement d'investir dans les technologies et de protéger les infrastructures. Tout ceci ne sera d'aucune utilité si le grand public et les citoyens ne sont pas sensibilisés, puisqu'ils constitueront alors un maillon faible.

Dans cette perspective, nous avons récemment présenté notre rapport annuel sur le panorama des menaces de cybersécurité en Lituanie, en sensibilisant différents groupes et communautés – mais aussi la population générale – aux cybermenaces les plus actuelles. La publicité et la visibilité offertes par ce rapport nous permettent de promouvoir et de défendre nos messages. En guise de conclusion, ce rapport montre que les incidents de cybersécurité doivent être considérés comme une menace pérenne. Ceux-ci ont progressé de 25 % par rapport à l'an dernier, en lien avec l'utilisation accrue des infrastructures numériques dans le contexte de Covid-19 et de confinement. Nous avons également observé une corrélation avec l'actualité politique, et notamment avec nos dernières élections législatives, durant lesquelles nous avons connu un pic d'incidents de cybersécurité. À cet égard, il est toujours intéressant d'observer le pourcentage d'incidents ciblant les institutions étatiques, les secteurs critiques et la population générale. Selon nos analyses, 10 % des incidents enregistrés ciblaient les institutions étatiques et les secteurs critiques. Par ailleurs, lorsque l'on cherche à savoir qui se cache derrière ces incidents, la réponse est très claire dans notre cas : il s'agit de la Russie. L'État russe sponsorise les cybermenaces, ce qui constitue un véritable enjeu. La Chine se veut également de plus en plus influente en Lituanie et dans la Baltique, et nous nous efforçons désormais de mettre fin à cette dépendance technologique de longue date et de nous prémunir des activités malveillantes soutenues par Pékin.

M. Philippe Latombe, rapporteur. Vous avez souligné que la Chine constituait la principale menace que vous appréhendiez. Pensez-vous que tous les États européens partagent la même sensibilité et la même vision de la menace que représente la Chine ? À l'inverse, pensez-vous qu'il existerait une forme de tropisme pour certains pays qui ne percevraient pas pareillement la menace chinoise ?

Par ailleurs, vous avez évoqué le rôle de la plaque russe en matière de cybercriminalité, du moins en matière de cyberattaques. Existe-t-il donc, d'après vous, un risque géopolitique technologique avec la Russie ?

M. Margiris Abukevicius. C'est justement pour répondre à ce type de questions que nous sommes ravis de partager nos perspectives avec les autres pays et d'enrichir le débat national. De notre point de vue, la menace chinoise en Europe n'est pas encore bien comprise. En Lituanie même, la perception de la Chine en tant que menace est relativement récente. Il y a quelques années, notre présidente se rendait en Chine avec une délégation de chefs d'entreprise et d'industriels à la recherche d'opportunités commerciales pour notre pays. Désormais, notre perception a évolué en sens contraire. Comme vous l'avez probablement entendu, nous avons officiellement quitté le format 17+1. Nous commençons à appréhender la Chine au travers du prisme sécuritaire, alors même que de nombreux pays européens continuent de privilégier un équilibre entre opportunités économiques et sécurité. Avec notre nouveau gouvernement entré en fonction il y a six mois, nous avons pris la décision tout à fait consciente d'appréhender notre coopération avec la Chine par le prisme de la sécurité, incluant les volets de cybersécurité et de dépendance technologique. Il me semble que c'est un défi que nous devons relever dans toute l'Europe. Pour les Américains, qui comprennent parfaitement les défis de long terme avec la Chine, la stratégie est relativement claire. En Europe, nous accusons un certain retard. Sitôt que nous aurons réellement compris la nature de la menace chinoise, nous façonnerons nos politiques en conséquence et serons beaucoup mieux préparés pour relever ces différents challenges.

Vous m'interrogez ensuite sur la Russie. S'il peut être intéressant d'évoquer le cas russe dans un échange sur la souveraineté technologique, force est de constater que la Russie n'est qu'un acteur marginal dans ce débat. Qu'il s'agisse de souveraineté technologique ou de dépendance aux technologies, nous ne considérons pas la Russie comme un acteur de premier

plan, même si les Russes ont choisi de travailler avec la Chine dans ce domaine. Le fait est que la menace russe est parfaitement comprise – et depuis très longtemps – en Lituanie. Personne n'achète de technologies russes pour l'équipement des infrastructures critiques. À l'inverse, la Chine équipe toujours nos infrastructures, et nous devons nécessairement faire évoluer nos mentalités. Cela dit, la Russie joue bien un rôle majeur en matière d'activités cyber malveillantes et représente une réelle menace pour la Lituanie.

M. Philippe Latombe, rapporteur. Je reviendrai brièvement sur le sujet de la Russie pour compléter notre échange. Au-delà de l'activité cybercriminelle que vous venez d'évoquer, vous avez souligné que la notion de souveraineté numérique devait également s'entendre au sens des *fake news* et de la capacité à diffuser de fausses informations pour influer sur les scrutins, comme vous avez pu l'expérimenter lors de vos dernières élections législatives. Ce sujet fut également prégnant lors des élections présidentielles américaines de 2016 ayant porté Donald Trump au pouvoir. D'après vous, comment pouvons-nous concilier souveraineté numérique et vérification des informations ? Estimez-vous que l'Europe se donne suffisamment les moyens de travailler sur le sujet pour éviter que nos sociétés démocratiques soient influencées, en période électorale, par les *fake news* et le complotisme ?

M. Margiris Abukevicius. Selon nos analyses, les menaces de cybersécurité associées aux campagnes d'information ou de désinformation sont particulièrement prégnantes et de plus en plus récurrentes. Du point de vue de l'influence sur les processus électoraux, ces menaces sont aujourd'hui le premier risque à prendre en compte. De nos jours, de nombreux pays sont fortement dépendants des technologies pour l'organisation de leur processus électoral. Grâce à la technologie, il est désormais possible d'influencer ce processus. En Lituanie, la technologie est naturellement intégrée à notre processus électoral, mais elle ne remplit pas un rôle critique. Nous devons donc nous assurer que tout fonctionne bien et ne pas donner à nos ennemis l'occasion de manipuler nos élections.

Dans cette perspective, la diffusion de fausses informations dans un contexte électoral constitue un moyen d'influence de premier plan. Il s'agit d'un processus de long terme, auquel nos adversaires se préparent à l'approche de chaque scrutin. Ces stratégies peuvent sinon changer les résultats d'une élection, du moins changer l'attitude d'un gouvernement. En tout état de cause, la désinformation et l'orientation de l'opinion s'inscrivent toutes deux dans une logique de long terme.

À cet égard, je citerai le rapport de la société de sécurité FireEye sur la campagne de désinformation menée par la Russie, qui couvre une période de cinq ans. Dans cette campagne intitulée *Ghostwriter*, une trentaine d'actions malveillantes de désinformation ont été relevées dans plusieurs pays européens. Une vingtaine de cas ont été détectés en Lituanie, mais d'autres pays – Pays baltes, Pologne, Allemagne – ont également été impactés. Du point de vue narratif, le contenu de cette campagne de désinformation était parfaitement clair : des messages contre l'Union européenne, contre l'OTAN et contre la présence militaire internationale dans la région. Par ailleurs, ces messages tentaient d'exploiter un certain nombre de fractures sociales caractérisant les sociétés concernées. Dans la plupart des cas, la technologie cyber a été utilisée en tant que moyen pour compromettre différentes plateformes médiatiques qui ont diffusé de fausses informations. Dans d'autres cas, la technologie cyber a été utilisée en sus de la désinformation en préparation de futures cyberattaques.

En tout état de cause, les actions malveillantes de désinformation sont désormais parties intégrantes du processus électoral. Nous devons donc y prêter une grande attention et favoriser le partage de bonnes pratiques et d'expériences.

M. Philippe Latombe, rapporteur. Dans votre propos liminaire, vous mentionniez l'existence d'une *task force* spécialisée en cybersécurité constituée avec d'autres pays. Si j'ai bien compris, cette équipe a vocation à s'agrandir pour fédérer davantage de participants. D'après vous, quelle taille optimale devrait atteindre cette équipe pour collecter et partager un maximum d'informations sans perdre en souplesse de fonctionnement ? Par ailleurs, à qui cette équipe doit-elle s'adresser ? Doit-elle nécessairement cibler le secteur public et les institutions de l'Union européenne et des États membres ? Peut-elle éventuellement s'adresser aux entreprises du secteur privé, y compris aux plus petites ? Comment envisagez-vous le déploiement futur de cette équipe ?

M. Margiris Abukevicius. À ce stade, six États membres participent à cette initiative : la Lituanie, la Pologne, les Pays-Bas, la Roumanie, l'Estonie et la Croatie. D'autres pays ont quant à eux désigné des observateurs : s'ils ne participent pas activement à nos travaux et n'envoient pas d'experts, ces observateurs suivent attentivement nos débats et nos réflexions. La France figure d'ailleurs parmi ces pays observateurs avec qui nous partageons nos réflexions. En termes de dimensionnement, l'équipe elle-même n'est guère étoffée, puisqu'elle ne compte qu'une dizaine de membres, à savoir un représentant de chaque État membre et plusieurs experts. La direction opérationnelle du groupe est successivement assurée par chacun de ses membres, dans une direction annuelle tournante. Nous en sommes aujourd'hui à la deuxième mandature dirigée par la Pologne, sachant que la première était dirigée par la Lituanie. Nous ne chercherons pas à agrandir ce groupe à d'autres pays, puisque nous disposons précisément de la taille idoine pour fournir des réponses rapides dans le domaine de la cybersécurité. En revanche, si d'autres pays souhaitent nous rejoindre, nous pourrions créer plusieurs équipes distinctes, ce qui constitue un avantage non négligeable.

Sur le fond, nous nous interrogerons régulièrement sur la manière d'utiliser au mieux cet outil. Nous travaillons bien entendu avec les institutions européennes, non seulement au niveau politique, mais aussi de manière très concrète avec le personnel militaire afin de soutenir les opérations extérieures de l'Union européenne. Si nous disposions de plusieurs équipes, nous pourrions certainement en dédier certaines au volet militaire et d'autres au volet civil de la cybersécurité.

Nos partenaires en Europe sont évidemment les institutions communautaires et les États membres. Néanmoins, l'enjeu crucial demeure celui de notre relation avec les autres processus de l'Union européenne, qui n'est pas encore clairement établie. Bien entendu, notre équipe est encore très jeune, et nous tâchons de renforcer la visibilité de nos capacités. En tout état de cause, nous ambitionnons de nous intégrer pleinement aux mécanismes de réaction coordonnée de l'Union européenne face aux incidents de cybersécurité majeurs. La France et l'Italie jouent d'ailleurs un rôle moteur pour préparer l'Union européenne à ces incidents. Pour notre part, nous considérons notre équipe comme partie intégrante d'une boîte à outils plus large, vers laquelle l'Europe pourra naturellement se tourner pour avancer sur ce dossier.

Un autre élément majeur à prendre en compte est le fait que la Commission européenne a l'ambition politique de créer une unité commune de cybersécurité (*Joint Cyber Unit*). En l'occurrence, nous avons soutenu cette initiative depuis le début. Même si personne ne sait encore quelles seront précisément les attributions de cette unité commune de cybersécurité, il est certain qu'elle devrait faciliter l'échange d'informations relatives aux activités opérationnelles en matière de cybersécurité. Surtout, nous disposerons d'un bras armé et d'une équipe opérationnelle capable de soutenir les États membres. Dans ce contexte, nous devons éviter l'écueil des doublons et ne pas recréer, au niveau communautaire, des mécanismes déjà existants au niveau national. Au contraire, nous devons nous appuyer sur ce qui a déjà été mis en œuvre par les différents États membres. Avec un plus large soutien politique, nous pourrons

certainement obtenir des financements pour développer certaines initiatives. En tout cas, plusieurs mécanismes fonctionnels existent déjà au niveau national.

Au-delà des institutions et des pouvoirs publics, nous travaillons également avec le secteur privé, et notamment avec de nombreux industriels français. Cette collaboration s'inscrit dans le cadre de l'initiative PESCO, mais également dans le cadre du Fonds européen de la défense, qui promeut la coopération industrielle à l'échelle communautaire. Nous avons d'ailleurs soutenu une proposition qui consisterait, avec l'appui du Fonds européen de défense, à développer une boîte à outils pour les différentes équipes, sachant que chaque pays tend à développer ses propres outils, avec les problématiques d'interopérabilité que cela représente. Il s'agirait donc de standardiser la boîte à outils à disposition des équipes de réponse aux cyberattaques, qui pourrait alors être utilisée par notre groupe comme par d'autres équipes dédiées au sein de l'Europe. Nous avons de réels espoirs que notre consortium puisse mettre en œuvre ce projet, qui devrait normalement recevoir le feu vert de la Commission européenne dans le courant du mois. Pour information, ce consortium auquel est notamment associé le groupe français Thales est dirigé par la Lituanie et réunit d'autres entreprises de pays qui, s'ils ne sont pas associés aux équipes de réaction rapide, sont fortement intéressées par la coopération industrielle, comme l'entreprise italienne Leonardo. De fait, il s'agit d'un très bon exemple de coopération industrielle européenne dans le domaine de la cybersécurité et de la cyberdéfense.

M. Philippe Latombe, rapporteur. Dans votre propos liminaire, vous insistiez également sur l'importance accrue de la cybercriminalité, qui a pris de plus en plus d'ampleur en 2020, et qui prendra de plus en plus d'ampleur dans les années à venir. Vous avez justement rappelé que nous devions agir autant que faire se peut pour éviter que cette cybercriminalité n'affecte les réseaux critiques : 5G, transport, énergie. Dans ce contexte, comment pouvons-nous renforcer la robustesse de nos réseaux ? Savez-vous si d'autres pays ont suivi votre modèle en auditant leurs réseaux ? Quels sont aujourd'hui les risques dont l'Europe devrait se prémunir en priorité par rapport à ses réseaux critiques ?

Par ailleurs, comment devons-nous procéder pour endiguer les activités de cybercriminalité localisées à l'étranger, qu'elles proviennent de Russie, de Chine, de Corée du Nord ou d'ailleurs ? Démanteler une cellule ne revient-il pas à couper la tête d'une hydre qui repoussera nécessairement ailleurs ? Disposons-nous véritablement de moyens juridiques et technologiques pour endiguer définitivement ces menaces ? Avons-nous éventuellement besoin de nouveaux outils ?

M. Margiris Abukevicius. Il s'agit d'une question éminemment complexe, à laquelle nous pouvons répondre sous plusieurs angles. D'abord, comme je l'indiquais précédemment, il est impératif que nos réseaux soient construits et équipés par des fabricants de confiance si nous souhaitons véritablement réduire les risques. Par ailleurs, nous devons nous montrer intransigeants vis-à-vis des obligations des industriels en matière de conformité (*compliance*). En Lituanie, la législation impose aux industriels de respecter un certain nombre de critères en matière de cybersécurité. L'Europe s'oriente également dans cette direction grâce aux directives *Network and Information System Security (NIS)* 1 et 2. Les prérequis en matière de sécurité sont de plus en plus nombreux, mais il est toujours aussi difficile de s'assurer que les industriels s'y conforment totalement.

Plus largement, nous ne devons pas nous voiler la face et croire que nous serons en mesure de sécuriser totalement nos réseaux. Il est plus pertinent de se focaliser sur leur résilience en vue d'assurer la continuité des affaires. Nous ne pourrons jamais totalement endiguer les attaques de type rançongiciel (*ransomware*). En revanche, nous pouvons préparer

nos entreprises à y faire face pour qu'elles puissent rapidement reprendre leurs activités après une attaque. Nous en revenons ici à la question des prérequis en matière de cybersécurité.

Enfin, l'échange d'informations est absolument critique. Plus nous coopérerons, plus nous disposerons d'informations et mieux nous serons préparés aux cyberattaques. J'en profite d'ailleurs pour mentionner une autre initiative internationale dirigée par la Lituanie, à savoir le centre régional de cyberdéfense. Trois autres pays y sont aujourd'hui associés : les États-Unis, la Géorgie et l'Ukraine. Un pilote a été lancé au mois de mai, avec des experts américains, géorgiens et ukrainiens qui se sont déplacés jusqu'à Kaunas, deuxième ville de Lituanie, pour travailler, avec leurs homologues lituaniens, à la création d'une cellule multinationale de renseignements spécialisée en cybersécurité, qui centraliserait les différentes sources de renseignements en la matière au profit de différents pays. Bien qu'ayant une vocation régionale, ce centre implique des acteurs aussi différents que les Américains, les Géorgiens et les Ukrainiens, dans l'idée de répondre à la menace provenant de Russie. Plusieurs cyberattaques ont en effet été dirigées contre la Géorgie en 2008 et l'Ukraine en 2015, donnant ainsi l'occasion à notre ennemi de tester de nombreux outils tactiques dans cette région. Il s'agit donc d'amener ces pays particulièrement exposés à coopérer avec les pays de l'OTAN et de l'Union européenne pour mieux nous préparer à réagir à ces menaces.

M. Philippe Latombe, rapporteur. Nous sommes actuellement en phase de déconfinement et de reflux d'une pandémie contre laquelle nous disposons désormais d'un vaccin. Pensez-vous que cette période troublée de pandémie aura des effets bénéfiques sur la cybersécurité et sur la prise de conscience du risque cyber ? Les parties prenantes – les États, les entreprises et les citoyens – sont-elles désormais toutes convaincues que les avantages du numérique s'accompagnent d'un certain nombre de risques ? Y sont-elles plus sensibilisées ? Pensez-vous que cette évolution était nécessaire et qu'elle perdurera dans les années à venir ?

M. Margiris Abukevicius. Vous m'interrogez sur les liens entre la Covid-19, le confinement et les cybermenaces. En l'occurrence, notre rapport annuel sur les cybermenaces a mis en avant un pic significatif d'incidents de cybersécurité survenus durant le premier confinement, lorsque les populations utilisaient tous les outils de communication à disposition sans se préoccuper des risques de cybersécurité. Durant le deuxième confinement, les cyberattaques se sont poursuivies, mais à une plus petite échelle, étant entendu que nous y étions beaucoup mieux préparés suite à l'expérience du premier confinement.

En tout état de cause, le premier confinement a considérablement accéléré l'usage des différents outils et services numériques. Logiquement, nous continuerons de nous en servir à l'avenir, même si nous ignorons encore à quel rythme se propagera cet usage massif des technologies numériques. En revanche, nous savons que cette utilisation accrue de la technologie élargit le périmètre de la menace, accroît les possibilités d'influence et diminue l'efficacité des moyens de protection. De fait, dans notre agenda national, nous nous efforçons de concilier les impératifs de numérisation et de cybersécurité. Sans cybersécurité, nous ne serons pas en mesure de nous appuyer sur les technologies numériques.

Dans le contexte des nouvelles perspectives financières de l'Union européenne, nous savons que le plan de relance européen accorde une large place à la transformation numérique. Nous avons donc convenu qu'environ 10 % des investissements consacrés à cette transformation numérique seraient dédiés à la cybersécurité. Il s'agit d'un véritable changement, qui est évidemment bienvenu. Nous disposons en effet de nombreux systèmes d'information obsolètes, et nous passons notre temps à résoudre des incidents de cybersécurité affectant ces systèmes construits à une époque où personne ne se souciait de cette thématique. En tout état de cause, pour accompagner ce bond numérique, nous devons sérieusement penser aux impératifs de cybersécurité et intégrer cette dimension en amont de chaque projet.

M. Philippe Latombe, rapporteur. Plusieurs évolutions technologiques sont attendues dans les années à venir : Internet des objets ; voitures autonomes ou semi-autonomes ; avions presque exclusivement gérés par l'informatique ; automatisation et robotisation des procédés industriels ; etc. Quelles sont donc vos craintes ou vos perspectives en matière de cybersécurité ? Pensez-vous que ces évolutions contribueront à changer la manière dont les cybercriminels s'attaquent aux entreprises ou aux administrations ? Devons-nous nous attendre à des évolutions technologiques telles que nous devrons modifier notre manière de répondre aux attaques ? Au contraire, conserverons-nous les mêmes modes de fonctionnement et devrons-nous y apporter les mêmes réponses qu'aujourd'hui ?

M. Margiris Abukevicius. Les cybercriminels et les acteurs malveillants sauront s'adapter aux nouvelles technologies et aux nouvelles réalités. Si nous nous appuyons sur des systèmes autonomes ou semi-autonomes, ils chercheront nécessairement à exploiter les failles de nos systèmes de défense, qui devront eux-mêmes s'adapter. De nos jours, la question n'est plus de savoir si cette évolution se concrétisera, mais de savoir quand celle-ci se concrétisera. L'avenir sera certainement marqué par une dépendance à l'égard des technologies, et les impératifs de sécurité devront être pris en considération dès la phase de conception des différents systèmes, dans une logique de *security by design*.

Sur un plan plus personnel, bien que plutôt jeune et n'ayant jamais utilisé un téléphone avec des boutons, je refuse obstinément de connecter mon réfrigérateur au Wi-Fi ou d'accéder à distance aux systèmes de contrôle de ma voiture. *In fine*, je me protège et prends des décisions en toute conscience pour éviter toute sur-dépendance vis-à-vis des technologies numériques. Quoi qu'il en soit, dans la mesure où la société dans son ensemble sera de plus en plus dépendante des technologies, la prise en compte et l'intégration des mesures de sécurité constitueront des enjeux essentiels du débat public de demain.

M. Philippe Latombe, rapporteur. En conclusion, souhaiteriez-vous transmettre un dernier message aux parlementaires français en ce qui concerne la cybersécurité ? Considérez-vous qu'il existe un sujet sur lequel nous devrions absolument nous pencher ?

M. Margiris Abukevicius. Je souhaiterais évidemment insister sur la coopération transatlantique en matière de technologies et de cybersécurité, que j'ai évoquée à plusieurs reprises dans mon intervention. Il est absolument critique d'aller au-delà du périmètre de l'Union européenne. Bien entendu, il est logique de promouvoir l'usage de produits européens pour préserver notre industrie. Néanmoins, il me paraît primordial d'élargir le périmètre de notre stratégie en matière de cybersécurité et de la concevoir dans l'alliance transatlantique. Dans d'autres domaines, les exemples de coopération entre les États-Unis et l'Europe ne manquent pas, notamment en matière de sécurité. En tout cas, une alliance technologique entre les États-Unis et l'Europe aurait nécessairement un impact mondial. Dans cette alliance, chaque pays devrait promouvoir sa propre industrie et bâtir des chaînes d'approvisionnement efficaces. Notre vision doit toutefois porter au-delà de l'Union européenne pour inclure une dimension transatlantique, sachant qu'une coopération dans le domaine des technologies permettra certainement de revivifier cette alliance. Voilà donc le message que je souhaiterais faire passer aux députés français.

M. Philippe Latombe, rapporteur. M. le ministre, je vous remercie de votre message, de vos réponses et d'avoir consacré du temps à cette audition. Nous ne manquerons pas de relayer votre plaidoyer en faveur d'une coopération accrue avec les États-Unis en matière de cybersécurité, de même que votre message de vigilance à l'égard de la Chine.

Audition, ouverte à la presse, de M. Andres Sutt, ministre du commerce et des technologies de l'information de la République d'Estonie *(9 juin 2021)*

Présidence de M. Philippe Latombe, rapporteur.

M. Philippe Latombe, président et rapporteur. Nous avons l'honneur d'auditionner M. Andres Sutt, ministre du commerce et des technologies de l'information du Gouvernement de la République d'Estonie.

M. le ministre, la mission d'information qui vous reçoit aujourd'hui poursuit depuis près d'une année ses travaux sur les principaux enjeux de la souveraineté numérique, parmi lesquels la numérisation dans l'administration, le rôle de la commande publique pour aider la croissance des entreprises innovantes et la formation au numérique. Notre attention a été attirée sur l'avance dont peut se prévaloir l'Estonie sur le plan numérique. C'est la raison pour laquelle nous souhaitons particulièrement vous entendre à propos des politiques numériques dont vous avez la responsabilité.

Je voudrais évoquer avec vous trois sujets dont, en premier lieu, votre conception de la souveraineté numérique. Il s'agit d'une question rituelle lors de nos auditions, liée à la grande diversité des définitions de cette notion. Comment, M. le ministre, appréhendez-vous ce concept et quelle peut être sa traduction concrète en termes de politiques publiques ?

Je souhaite également vous entendre sur les politiques numériques menées en Estonie. Quelles conditions vous semble-t-il indispensable de remplir pour obtenir l'adhésion des administrés, citoyens comme entreprises, aux démarches de transformation numérique dans leurs relations avec l'administration ? Comment la numérisation s'inscrit-elle dans la gouvernance des politiques de la fonction publique et de réforme administrative ? Comment appréhendez-vous les enjeux de formation aux savoir-faire numériques ? Ceux-ci revêtent un caractère primordial pour permettre aux citoyens de se saisir du numérique afin d'en faire un atout dans leur vie personnelle mais aussi dans leur vie professionnelle. Pouvez-vous enfin nous dire un mot sur la façon dont le numérique a constitué, en Estonie, un vecteur de résilience durant la crise sanitaire du covid ?

En dernier point, j'aimerais échanger avec vous sur l'actualité de l'Union européenne en matière de numérique. Quel regard portez-vous sur les nombreux projets portés par la Commission européenne, notamment en matière de circulation des données avec le *Data governance Act (DGA)* ? Comment L'Europe peut-elle être un levier de souveraineté numérique pour les différents États membres qui la composent ?

M. Andres Sutt, ministre du commerce et des technologies de l'information de la République d'Estonie. Le sujet du numérique prend effectivement une importance croissante et la covid est d'ailleurs à l'origine d'une utilisation nettement plus large du numérique de notre part. Cette évolution va de pair avec un plus grand besoin de cybersécurité.

Je souhaite d'abord présenter le contexte de mon pays et les étapes que nous avons franchies en Estonie. L'Estonie est célèbre pour son développement numérique et elle accorde une grande importance à ce sujet. Notre population est peu nombreuse. Nous sommes convaincus que le numérique constitue un moteur de la croissance non seulement pour nos entreprises mais aussi pour notre société.

En Estonie, la société numérique et le numérique ne se sont évidemment pas construits en une journée. Ce long processus s'est développé au cours des vingt dernières années, de façon graduelle, permettant à la société et aux entreprises de devenir beaucoup plus efficaces. Actuellement, 99 % des services publics sont en ligne en Estonie. Il s'agit d'un point très important pour le développement du pays. Cette évolution a fait entrer la population estonienne dans un monde numérique. Cette transformation numérique et technologique est bénéfique pour tous.

Plus généralement, si nous voulons que l'Union européenne devienne un leader mondial dans le domaine du numérique, il faut absolument faire en sorte que nous disposions d'un marché unique numérique. La souveraineté numérique est également essentielle et il nous faut identifier les technologies clés et les domaines d'action fondamentaux de manière à pouvoir être innovants dans tous ces domaines.

Il est également important que notre positionnement soit équilibré, que nous connaissions nos forces et nos faiblesses et que nous bénéficiions d'un environnement où l'innovation soit favorisée par l'Union européenne. Cela signifie en particulier que notre souveraineté dans le domaine du numérique doit nous aider à accroître encore notre compétitivité. Nous ne devons pas nous isoler mais nous appuyer sur nos forces pour construire une compétitivité européenne par rapport au reste du monde.

Nous devons aussi nous assurer d'être correctement positionnés dans la chaîne mondiale d'approvisionnement. Nous connaissons tous les avantages de disposer d'un marché libre, équilibré et ouvert. Un tel marché doit exister dans le domaine des services numériques. Plus nous pourrons progresser au niveau européen sur ce point, plus nos entreprises, nos villes et nos citoyens pourront en bénéficier. Nous disposerons ainsi d'une position compétitive dans le monde.

Les Premiers ministres du Danemark, de l'Allemagne, de la Finlande et de l'Estonie ont envoyé une lettre au président de la Commission pour proposer de renforcer et d'accélérer la souveraineté numérique de l'Union européenne. De plus, une bonne et solide coopération avec nos alliés stratégiques dans le reste du monde constitue un point très important.

Nous nous sommes beaucoup préoccupés de la numérisation des services publics. La pierre angulaire de notre politique a été la création de systèmes de communication extrêmement résistants, avec une colonne vertébrale juridique vraiment solide.

Par exemple, en Estonie, la carte d'identité est obligatoire et nous l'avons rendue numérique. Notre « mantra » pour réaliser cette numérisation a consisté à utiliser des systèmes simples et non une grande base de données qui se serait avérée extrêmement lourde. La simplicité est en effet essentielle, ainsi que la rapidité et l'interopérabilité des différentes bases. Des milliers d'organisations privées et publiques utilisent ce système pour échanger des données.

La cybersécurité représente une autre priorité. En tant que ministre, l'une de mes priorités vise précisément à assurer que tous nos systèmes fonctionnent bien et en toute sécurité. Dans ce sens, nous avons suivi un certain nombre de principes clés. En particulier, nous avons évité l'existence de doublons. Avons-nous réussi à 100 % à créer un système simple et efficace ? Probablement pas et il reste bien entendu des améliorations à opérer.

Dans le passage des anciens aux nouveaux systèmes et dans la transition vers les nouveaux services numériques, la transparence et la confiance du public étaient nécessaires. De même, il était indispensable que les entreprises et les citoyens retrouvent leurs données et

y accèdent sans difficulté et que nous nous appuyions sur un environnement ouvert qui puisse facilement être utilisé par le Gouvernement, les citoyens et les entreprises.

Enfin, une valeur clé de notre point de vue tenait au fait que le système devait être centré sur l'utilisateur : son utilisation devait être facile et il devait permettre d'améliorer la vie quotidienne de nos citoyens et de nos entreprises.

Nous avons tiré de notre expérience un certain nombre de leçons. La première est l'importance de la simplicité. Pour cette raison, nous avons dû progresser étape après étape, en évitant le développement d'un énorme système qui serait très lourd et probablement peu efficace. Avancer petit à petit est une méthode qui s'est révélée efficace, mais il est essentiel qu'au final, le design soit bon et le système globalement bien conçu. Les plateformes partagées ont permis une implémentation plus rapide et efficace. Enfin, la confiance du public et la transparence sont des points clés.

La coopération entre le privé et le public a, elle aussi, été fondamentale dans ce domaine du numérique. Nous pensons qu'il s'agit de l'un de moteurs du développement d'une société numérique. Des amendements ont récemment été apportés à notre législation de manière à ce que le Gouvernement puisse mettre à disposition de tous des logiciels libres pour travailler. Les codes sont ainsi totalement ouverts : les entreprises les connaissent, peuvent les utiliser et les modifier pour participer au développement de nouvelles solutions et de nouveaux produits. Nous avons besoin de cette souplesse. En particulier, dans les processus d'achat, ces partenariats nous permettent de travailler ensemble à des solutions conceptuelles. Tous les codes sont stockés dans des bases de données. Ils peuvent être utilisées aussi bien par les services publics que par des organismes privés. Les entreprises conservent les références de leur travail qui peut bénéficier à tous et être utilisé pour tous les développements ultérieurs.

Nous pensons qu'il est essentiel de construire un service numérique public qui ne s'assimile pas à « une énorme machine » mais un service qui bénéficie de la coopération avec le privé et l'industrie. Cette coopération entre le public et le privé nous permettra en effet d'aboutir à de meilleures solutions.

En ce qui concerne l'éducation et les compétences dans le domaine numérique, nous devons nous assurer que le plus grand nombre de citoyens puisse apprendre à utiliser le numérique et les technologies modernes. Nous travaillons à inclure dans ces démarches le plus grand nombre de personnes, par exemple en apprenant la robotique aux enfants. Ceux-ci sont, certes, habitués à se servir du numérique mais il ne s'agit pas uniquement de l'utiliser à des fins ludiques : ils doivent en réalité en avoir une compréhension qui leur permette également de créer et d'innover. Nous avons également mis en place des initiatives telles que le *Digital girls squad* : il s'agit d'une association qui encourage les jeunes filles à travailler dans le domaine du numérique et les aide à se familiariser avec ce secteur.

L'Intelligence artificielle prend de plus en plus d'importance. Nous devons donc nous y adapter. Nous avons besoin de connexions Internet extrêmement rapides et efficaces. En Estonie, la densité de population est très faible et nous voulons être certains que toutes les écoles, toutes les maisons, tous les appartements, tous les ménages aient accès à une connexion de qualité et rapide.

L'apprentissage tout au long de la vie est fondamental. Nos concitoyens doivent comprendre qu'ils devront apprendre durant toute leur vie. La société numérique ne sera une réussite que si les citoyens peuvent utiliser tous les moyens numériques existants. Nous avons donc mis en place des programmes d'enseignement tout au long de la vie.

En ce qui concerne l'initiative européenne de *Data governance Act (DGA)*, *Digital market Act (DMA)* et *Digital services Act (DSA)*, nous approuvons totalement la création d'une économie européenne des données numériques. Nous avons en effet besoin d'être compétitifs à l'échelle mondiale et de telles initiatives peuvent nous permettre de l'être.

Nous exprimons toutefois quelques préoccupations. En particulier, cette approche européenne doit bien prendre en compte la gouvernance des données et nous offrir l'occasion d'innover. Il convient d'éviter un excès de réglementations mais plutôt d'assurer une fluidité qui permette l'efficacité. Nous devons également être certains que le système ne désavantage pas les petites et moyennes entreprises (PME), qu'il ne décourage pas les *start-up*. Les PME et les *start-up* sont en effet des éléments critiques pour le développement de notre économie et pour sa croissance.

L'ensemble du développement du système numérique doit avoir lieu horizontalement, c'est-à-dire en tenant compte de tous les aspects de notre économie et en créant des incitations – telles que des instruments financiers – pour encourager l'adoption de solutions numériques.

L'interopérabilité des données au niveau européen est aussi importante. Nous serons forts si nous parvenons à créer une économie numérique solide qui s'applique à l'ensemble de l'Union européenne. Nous approuvons le *DSA* qui constitue à notre avis un moyen d'harmoniser tous les services au niveau de l'Union européenne. Il est également essentiel pour nous que nous puissions éliminer les contenus illégaux sur la toile et ailleurs. La clarté et la transparence juridique sont nécessaires pour y parvenir. Nous sommes prêts à coopérer avec tous les États membres pour renforcer le principe du pays d'origine.

Même si tous les États membres ne partagent pas cette opinion, nous pensons important d'établir un lien entre la taille des entreprises et les règles applicables de manière à ce que les PME et les *start-up* ne soient pas pénalisées par un fardeau administratif excessif qui entraverait leur utilisation du numérique. De façon générale, un bon équilibre est nécessaire entre la taille des entreprises, leur capacité à accéder à des marchés plus lointains et plus grands et leur responsabilité en matière de sécurité. Le secteur du marché numérique doit se protéger, offrir un niveau de sécurité satisfaisant pour être bien utilisé, tout ceci devant se fonder sur des preuves et des éléments probants. La protection des données est essentielle pour la réussite.

Les *gate keepers* ont un rôle important à jouer pour la confiance, la sécurité, la protection des données et l'adoption par les utilisateurs de ces moyens en ligne dans un monde qui devient de plus en plus électronique.

Comme dans tout domaine, le secteur du numérique devra être doté d'une réglementation évolutive, qui tienne compte des changements extrêmement rapides qui se produisent dans ce domaine. Sur un marché qui évolue très vite, la réglementation doit elle-même s'adapter en conséquence. Les réglementations doivent donc être dynamiques et à l'écoute de l'évolution du marché numérique.

Enfin, nous devons travailler à une large harmonisation au sein de l'Union européenne. Si le marché européen du numérique est fragmenté, ses avantages seront dilués. Nous avons aussi besoin de construire nos forces et de tirer parti de nos avantages dans le marché du numérique en Europe. L'Union européenne constitue en effet un marché de 500 millions d'habitants. Elle représente ainsi un très grand bloc commercial – le troisième au monde – et nous devons être leaders dans ce secteur du numérique.

M. Philippe Latombe, rapporteur. Nous avons reçu hier le vice-ministre de la défense de Lituanie qui nous a expliqué sa vision géopolitique et géostratégique du numérique.

Pour lui, la menace principale est constituée par la Chine tandis que la menace principale en matière de cybercriminalité provient plutôt de la Russie. Il considère qu'il est absolument nécessaire que l'ensemble des pays européens coopèrent de façon très étroite avec les États-Unis pour défendre la vision démocratique de l'Occident dans le monde.

Partagez-vous totalement cette vision ou avez-vous une position plus proche de celle de certains pays qui souhaitent que l'Europe suive une troisième voie, entre la Chine et les États-Unis ? Cette troisième voie se rapprocherait évidemment de celle des États-Unis, mais tout en s'assortissant d'une certaine indépendance.

M. Andres Sutt. La géopolitique s'applique bien entendu aussi aux domaines du numérique et de la cybersécurité. Les liens transatlantiques entre l'Union européenne et les États-Unis sont extrêmement forts et ces liens sont à l'avantage des deux parties. L'ordre mondial a bénéficié au monde entier et à tous les pays au cours de ces trente dernières années. Nous avons beaucoup à gagner à poursuivre cette alliance stratégique avec les États-Unis. Certes, nous avons parfois des différends et sommes concurrents dans certains domaines, mais nous sommes fondamentalement du même côté. Ce lien transatlantique fort va dans l'intérêt de l'Union européenne dans son ensemble mais aussi de chacun de ses membres.

Dans le domaine de la cybersécurité, nous constatons un nombre croissant d'attaques, celles-ci étant de plus en plus sophistiquées. Nous approuvons en matière de défense la définition d'une cible de dépenses de 2 %. De même, nous sommes également d'accord avec le principe qui consisterait à nous doter d'un objectif de dépenses de cybersécurité. Il serait vraiment formidable que nous partagions un même objectif.

M. Philippe Latombe, rapporteur. Ma deuxième question porte sur vos projets en matière d'administration et d'e-administration. Vous avez été les pionniers de l'e-identité et de l'e-administration. D'autres pays européens comme le Luxembourg ont, eux aussi, innové en créant des e-ambassades. Quels sont aujourd'hui les projets de l'Estonie pour continuer à se trouver au sommet de l'état de l'art sur ces sujets ? La *blockchain* par exemple est-elle un outil que vous développerez pour améliorer encore l'efficacité de votre administration ?

Je sais que vous avez échangé hier avec Mme Amélie de Montchalin, ministre de la transformation et de la fonction publiques. Sans dévoiler des secrets, avez-vous évoqué avec elle des sujets et des bonnes pratiques que nous pourrions élaborer ensemble ?

M. Andres Sutt. Effectivement, nous avons eu une discussion très intéressante avec la ministre, Mme Amélie de Montchalin, et j'ai été très heureux de voir tout ce que nous avons en commun. Par exemple, 99 % de tous nos services publics sont en ligne, tandis qu'en France, 87 % le sont : en particulier, 250 services publics utilisés très fréquemment sont déjà en ligne.

Nous partageons la même manière d'appréhender la question et de traiter les services existants. Nous devons cependant encore nous améliorer sur ce point en Estonie : nous devons en effet refaçonner un certain nombre d'anciens systèmes puisque, le temps passant, ces systèmes ont fini par vieillir depuis vingt ans. En outre, nous souhaitons investir davantage dans l'aspect opérationnel et non simplement dans le développement. Nous devons faire en sorte que les services existants soient faciles à utiliser et fonctionnent bien.

La cybersécurité représente une question très importante. Nos services publics sont maintenant basés sur l'Intelligence artificielle et la reconnaissance vocale. Par exemple, les citoyens reçoivent des messages pour les avertir que leur permis de conduire a expiré ou qu'ils doivent renouveler certaines demandes. Votre système de déclaration d'impôts préremplie ressemble à ce que nous faisons en Estonie. Nous devons maintenant faire en sorte que les

services publics soient plus faciles à utiliser pour les citoyens, faute de quoi ils se plaignent, sont découragés et n'ont pas envie d'utiliser ces services.

L'interopérabilité des données est essentielle, en particulier le fait que les bases de données du Gouvernement soient partagées. Même si une donnée ne se trouve pas dans telle base, les citoyens doivent pouvoir l'obtenir grâce aux liens entre les différentes bases de données.

Nous devons également passer à une économie en temps réel grâce à l'Intelligence artificielle, ce qui pourrait nous permettre d'économiser 200 millions d'euros par an, soit 14 millions d'heures travaillées pour une population de 1,3 million de personnes.

Il nous reste donc encore beaucoup à accomplir pour que ces services soient vraiment réactifs et que l'Intelligence artificielle réalise un certain nombre de tâches que les citoyens n'auront alors plus à effectuer.

M. Philippe Latombe, rapporteur. Je poserai une dernière question qui s'adresse véritablement au ministère du commerce et des technologies de l'information de la République d'Estonie. Dans le domaine juridique, la Cour de justice de l'Union européenne a fait l'actualité depuis un peu plus d'an en invalidant par l'arrêt Schrems II, le *Privacy Shield* pour contrer le *Cloud Act* puis avec l'arrêt Prokuratuur dans votre pays et l'arrêt « La Quadrature du Net » en France.

Sans que ma question concerne cet arrêt en particulier, comment appréhendez-vous l'intégration du droit proposé par la Cour de justice de l'Union dans votre droit national ? Suivez-vous ce problème au quotidien en l'intégrant directement dans votre droit ou prenez-vous un peu de temps avant de procéder à cette intégration ?

La question s'est notamment posée en France avec l'arrêt « La Quadrature du Net » ou Prokuratuur. Nous savons que la Cour de justice veut s'exprimer de plus en plus sur le droit et harmoniser autant que possible les différents droits au sein de l'Union. Cela est-il une source de préoccupations pour vous ? Cela monopolise-t-il une partie de votre temps ?

M. Andres Sutt. L'intégration de la législation au niveau européen fait l'objet d'un accord accepté par tous, États membres et Parlement européen. Nous intégrons donc, comme vous, la législation européenne dans notre législation nationale et nous respectons les délais : c'est une simple question de bonne intendance.

Je répondrai, si vous me le permettez, par écrit à votre question sur la Cour européenne de justice.

Mme Marietta Karamanli. Lorsque j'étais présidente de la mission d'information sur l'identité numérique, nous avons suivi les projets que vous avez portés au sein de votre pays. Vous êtes pour nous un exemple. Je suis actuellement rapporteure sur la décision de la Cour de justice en tant que secrétaire de la commission des affaires européennes et nous avons justement rapporté la semaine dernière sur cette décision. Je serais intéressée par votre point de vue sur l'intégration du droit européen sachant que, pour nous, en tant que membres de la commission des lois, le droit de l'Union est juridiquement supérieur. Il s'inspire de la jurisprudence des uns et des autres, ce qui permet d'améliorer les réponses apportées.

Je reviens à ce que vous avez expliqué de manière très détaillée sur le développement de la souveraineté numérique que vous avez mis en œuvre dans votre pays. De manière opérationnelle, quelles sont les personnes qui ont développé le service et la plateforme

numérique en Estonie, au plan national ? Qui conserve les données ? Quelles sont les garanties données aux citoyens pour assurer la confiance et la transparence ?

M. Andres Sutt. Je répondrai tout d'abord à vos dernières questions. Le point le plus fondamental tient au fait que les données doivent être la propriété des citoyens. La confiance des citoyens est essentielle et nécessite une totale transparence : chacun doit voir qui a accès à son dossier, à ses fichiers

Par exemple, je vis à Tallinn où la municipalité met en place une carte de transport réservée aux habitants de la ville. Il faut donc être inscrit comme habitant de la ville de Tallinn pour en bénéficier. Si je consulte mes dossiers, j'y verrai que la municipalité de Tallinn a vérifié que je suis bien habitant de cette ville. De la même manière, vous pouvez bloquer l'accès à votre dossier médical si vous souhaitez que personne ne voie vos données médicales, pas même votre docteur. Vous en avez la possibilité parce que ce sont véritablement vos données. C'est là un point extrêmement important.

Autre aspect essentiel, tout incident doit être signalé publiquement. Nous avons par exemple connu des incidents avec le système de carte d'identité numérique et nous avons toujours rendu ces incidents publics de manière à ce que nos concitoyens en aient connaissance et sachent également que le risque a été éliminé. Cela participe de la confiance que le citoyen accorde au système.

Qui a développé le système ? Ce projet a été partagé entre le secteur privé et le secteur public. Les sociétés de technologie ont apporté une aide importante. Au départ, les deux forces motrices étaient les banques et les sociétés de télécommunications qui voulaient numériser une très large partie de leurs services et les mettre en ligne pour améliorer la qualité de vie des citoyens.

Quoi que nous fassions, il reste fondamental que les citoyens soient au centre du projet. Il faut que la numérisation apporte un avantage au citoyen et que celui-ci bénéficie de systèmes plus rapides et meilleurs.

Je souligne que notre expérimentation a représenté un véritable cheminement et ne s'est donc pas construite en un jour. Pour être franc, nous n'avions pas planifié, voici vingt-cinq ans, que nous aboutirions aujourd'hui à 99 % de nos services publics en ligne. Cette évolution a été progressive et, au fur et à mesure que nous avons progressé, nous avons rencontré des problèmes que nous avons résolus. Tout cela s'est fait au fil de l'eau avec une grande coopération entre public et privé.

Ce principe a fonctionné en Estonie et je crois que d'autres pays y sont aussi parvenus. Nous serions très heureux de coopérer avec vous.

Pouvez-vous dupliquer le même système ? Il faut tenir compte des cultures, des préférences mais, d'un point de vue conceptuel, nous pouvons tout à fait partager notre expérience comme nous l'avons déjà fait avec d'autres pays, notamment des pays en voie de développement, pour les aider à construire une société numérique.

Je suis aussi ici pour apprendre de vous, apprendre de ce que vous avez pu faire mieux que nous et, également, apprendre des erreurs que vous avez commises et que nous pourrions éviter en les partageant. Il s'agit donc, pour moi, d'un dialogue dans les deux sens.

M. Philippe Latombe, rapporteur. Je vous remercie, M. le ministre, d'être venu répondre à nos questions dans votre agenda contraint. Vous êtes pour nous une sorte de

boussole, grâce à ce que vous avez construit et au cheminement de votre e-administration. Je vous laisse le mot de la fin, si vous souhaitez porter des points particuliers à notre attention.

M. Andres Sutt. C'est pour moi un honneur d'être présent ici aujourd'hui, alors que nous fêtons le centième anniversaire des relations diplomatiques entre la France et l'Estonie. C'est un événement très important pour moi et je suis donc personnellement très content de me trouver en France.

La France est un allié fondamental pour l'Estonie. Nous coopérons d'une excellente manière dans le domaine de la défense et dans celui du numérique. Nous devons poursuivre et développer nos échanges, de même que nos investissements réciproques ou les flux touristiques entre nos deux pays. Les temps actuels sont singuliers, mais nous allons dans la bonne direction.

Être présent à Paris est pour moi très important car la France est un membre fondateur de l'Union européenne. Elle est au centre de l'Europe alors que nous nous trouvons à l'extrémité nord-est de notre continent. Je pense que nous devrions être forts, unis, ambitieux à l'échelle mondiale, pour le plus grand bien de nos citoyens.