N° 7

SÉNAT

SESSION ORDINAIRE DE 2019-2020

Rapport remis à M. le Président du Sénat le 1er octobre 2019

Enregistré à la Présidence du Sénat le 1er octobre 2019

RAPPORT

FAIT

au nom de la commission d'enquête (1) sur la **souveraineté numérique**,

Président
M. Franck MONTAUGÉ,

Rapporteur
Par M. Gérard LONGUET,

Sénateurs

Tome II : Comptes rendus

(1) Cette commission est composée de : M. Franck Montaugé, *président* ; M. Gérard Longuet, *rapporteur* ; M. Patrick Chaize, Mmes Sylvie Robert, Catherine Morin-Desailly, MM. Yvon Collin, M. André Gattolin, MM. Pierre Ouzoulias et Jérôme Bignon, *vice-présidents* ; Mme Viviane Artigalas, MM. Jérôme Bascher, Bernard Bonne, Mme Martine Filleul, MM. Christophe-André Frassa, Loïc Hervé, Laurent Lafon, Rachel Mazuir, Stéphane Piednoir, Mmes Sophie Primas, Frédérique Puissat et M. Hugues Saury.

S O M M A I R E

Pages

COMPTE RENDUS DES AUDITIONS

Audition de M. Pierre Bellanger, président-directeur général de SKYROCK, le 16 mai 2019

M. Franck Montaugé, président. - Notre commission d'enquête poursuit ses travaux avec l'audition de M. Pierre Bellanger, président-directeur général de Skyrock.

Cette audition sera diffusée en direct sur le site Internet du Sénat et fera l'objet d'un compte rendu publié.

Enfin, je rappelle, pour la forme, qu'un faux témoignage devant notre commission d'enquête serait passible des peines prévues aux articles 434-13, 434-14 et 434-15 du code pénal. Je vous invite à prêter serment de dire toute la vérité, rien que la vérité, levez la main droite et dites : « Je le jure. »

Conformément à la procédure applicable aux commissions d'enquête, M. Pierre Bellanger prête serment.

Je vais tout d'abord vous citer : « Notre pays a livré sa souveraineté numérique sans débat et sans combat ». Vous avez même parlé de renoncement. C'est un constat que vous avez renouvelé dans de nombreuses enceintes !

En janvier 2014, vous publiiez La Souveraineté numérique, prônant alors la création d'un Commissariat numérique qui devait développer un système d'exploitation souverain. Ni l'un ni l'autre n'ont finalement vu le jour. La situation s'est-elle aggravée ?

Sommes-nous devenus les vassaux inconscients d'un cyber-empire américain dont la monnaie illimitée serait le dollar et la monnaie réelle les données que la France braderait à tout va ? L'État a-t-il fait tout ce qu'il devait pour défendre la souveraineté numérique de notre pays ?

Vos constats sont sévères, nous souhaitons vous entendre les expliciter. Vos pistes de réflexions et recommandations d'action seront sans doute débattues.

M. Pierre Bellanger, PDG de Skyrock. - Je suis très honoré d'être devant vous, d'autant que j'espère ce moment depuis plus de 25 ans. En 1993, après avoir découvert les réseaux d'ordinateurs et leurs possibilités, je proposais à France Télécom de créer sa première société de services internet, France en ligne, sur le modèle d'un service existant aux États-Unis. J'ai choisi un opérateur public parce que le réseau est, à mes yeux, une affaire publique.

Je n'ai eu de cesse, depuis lors, de rencontrer les élites de ce pays, des associations pour leur exposer le concept de souveraineté numérique que j'ai développé. Vous imaginez l'émotion qui m'anime aujourd'hui, en prêtant

serment devant cette commission dotée de pouvoirs d'enquête, créée par le Sénat dont l'indépendance est reconnue.

Lorsqu'internet est arrivé en France, c'était en passager clandestin, une sorte de liseron dans le grand chêne de la nation. Il a été toléré, décrié, puis il a fallu s'adapter et il est devenu plus gros que l'arbre ; mais une méfiance devant le réseau subsiste. Avec le réseau, la rationalité n'a pas prévalu : on continue à se raconter des histoires, comme celle de ces adolescents en T-shirt dans un garage californien. C'est que nous avons été surpris par internet : nous étions comme le hérisson dans les phares, qui n'a pas le temps de raisonner sur le moteur à explosion avant l'impact.

Au contraire du cinéma, de la télé, de la radio, le réseau ne vient pas s'additionner au monde réel, mais le remplacer. Nous y avons donc tout mis, à l'exception de la République. Les machines multiplient leur capacité par un million tous les vingt ans. La progression des logiciels va 43 fois plus vite que celle des matériels. Au total, donc, l'efficacité du système est multipliée par 43 000 milliards tous les vingt ans ! À cela s'ajoute l'effet réseau, selon lequel la valeur d'une machine est proportionnelle au carré du nombre de machines auquel elle se connecte. Dans un réseau de dix machines, chaque machine a une valeur de 10^2, soit 100. Si vous y ajoutez une machine, la valeur de chaque machine passe à 11^2, soit 121. En d'autres termes, la valeur de chaque machine augmente de 21 % alors que la taille du réseau a augmenté de 10 %. C'est une source de productivité sans précédent, un effet levier ahurissant. Des centaines de milliers de machines rejoignent le réseau chaque jour.

Associée à la croissance des logiciels, des machines, des réseaux, la puissance des données va nourrir les machines apprenantes. Imaginons une course de voitures où la puissance du moteur est proportionnelle à la taille du réservoir - les données - de chaque voiture. Cela crée un effet de puissance que nous sommes incapables de mesurer : c'est une progression exponentielle d'exponentiel. Tout migre sur le réseau, parce que c'est là que la productivité est la plus forte, tout y transite, tout s'y affiche.

En France, l'internet est arrivé par effraction ; il y avait le Minitel, le réseau Cyclades imaginé par Louis Pouzin, qui n'a pas été mis en place en France mais dont se sont inspirés les Américains. C'est un système nerveux exogène qui s'est greffé sur l'existant.

Les données servent à se prémunir contre l'incertitude. Il y a deux moyens de le faire : par la mutualisation des risques ou le gaspillage. Pour couvrir le risque, on distribuera un journal dans tous les kiosques, avec 40 % d'invendus. Selon la même logique de précaution, la moitié de la nourriture se perd de la fourche à la fourchette, ou encore 20 % de l'eau dans les canalisations. Au total, 10 à 15 % de la valeur des administrations et entreprises part dans ce combat contre l'incertitude.

Mais au XXIe siècle le gaspillage n'a plus cours, et l'on remplace l'incertitude par la certitude des données. Celles-ci pèsent, en valeur, 10 à 15 % du PNB. Ce nouveau monde est notre plus grande chance car il offre de nouveaux outils qui changent la donne et nous aident à résoudre des problèmes que nous affrontions depuis des décennies.

C'est notre chance mais aussi notre principal risque de régression. Ce que la mondialisation a fait aux classes populaires, le réseau le fera aux classes moyennes à cause de la mutation, de l'automatisation complète du monde du travail. Moi-même fervent technophile, lorsque j'alertais sur ces risques, on m'opposait toujours la destruction créatrice conceptualisée par Schumpeter. Pourquoi pas, mais dans notre monde mondialisé, la destruction peut avoir lieu dans un endroit et la création dans un autre. J'ai coutume de dire que les réseaux sociaux sont en Californie et les plans sociaux en Picardie. Toute la création de valeur du réseau migre, comme nos données, nos savoir-faire, nos secrets. Notre grande nation, dotée d'une véritable puissance militaire, est incapable de garantir le secret de la correspondance. Nous sommes dans une situation de nudité, de vulnérabilité, d'appauvrissement généralisés. Machines, réseaux, programmes, services ne répondent pas de nos lois.

Un exemple : à l'été 2016, quelques dizaines de Français ont été mis à mort sur une messagerie chiffrée. L'État français a tenté de faire interdire ce service, de faire retirer la liste, mais les plateformes ont refusé de fermer l'application. L'État s'est trouvé démuni face à la mise en danger de ses citoyens.

Face à cette situation, nous cherchons des accommodements, dans une logique de réparation plutôt que d'affrontement. L'affrontement est pourtant réel : l'internet ne répond pas aux rêves que l'on nous a présentés. Il est né des travaux de l'armée américaine, dans une logique de guerre froide. Pour utiliser une image, ce fameux garage avec ses deux adolescents est sur le pont d'envol d'un porte-avion. Nous n'avons pas vu le complexe militaro-numérique derrière cette image. L'internet est un projet politique, une affaire d'État, et dans notre société un sujet majeur parce qu'aucun secteur n'est épargné. J'ai rencontré médecins, avocats, pharmaciens, architectes qui m'ont présenté à tour de rôle leur vision du problème. Le rôle des pouvoirs publics est de donner la vision de grand angle.

L'internet n'est pas un territoire, ce n'est pas un lieu mais un lien. Tout ce qui fait la puissance publique - la liberté, garantie par la loi, qui est garantie par l'ordre public, à son tour garanti par la souveraineté - nécessite trois choses : une population, un territoire avec des frontières, une règle commune. Rien de cela sur le réseau. Nous n'avons aucun moyen de maîtriser ce nouvel outil qui change tout.

Il a donc fallu réfléchir. J'ai reçu une bonne écoute de l'institution militaire, qui comprend ces difficultés. Tout le monde commence à se rende

compte, aujourd'hui, que cette question est capitale, que face à de véritables empires cyber nous n'avons pas de moyen de réponse.

La prise de conscience a progressé. La constitution de votre commission est déjà un pas en avant considérable. La notion de souveraineté entre dans les éléments de langage, reprise par tous les partis politiques car, fort heureusement, elle n'est ni de gauche ni de droite.

Le réseau est une rupture de continuité de la nation. Si pour une raison ou pour une autre, l'application que vous avez développée est retirée de la plateforme, c'est le tribunal de Sacramento, en Californie qui est compétent. Les conditions d'utilisation ont plus d'importance que les lois de la nation.

À l'affaire Snowden de 2013 ont succédé des attaques cyber en série, puis l'affaire Cambridge Analytica. C'est maintenant que le travail commence. Tout est à faire, mais je ne verse pas dans l'alarmisme : j'ai quelques solutions à proposer.

M. Gérard Longuet, rapporteur. - Monsieur Bellanger, vous êtes la première personne que nous entendons. La mondialisation au rythme des avions ou de la fibre optique n'entraînait pas, en elle-même, la dématérialisation des États. Mais nous sommes entrés dans un système où la puissance des réseaux et des logiciels - vous proposez d'ailleurs le néologisme « résogiciels » - est une réalité politique. Après la dernière élection présidentielle américaine, on s'est ainsi demandé si le résultat n'avait pas été biaisé par une manipulation des réseaux venue de Russie. Le plus grand pays du monde pouvait être déstabilisé par une puissance bien plus modeste. Deuxième exemple, l'impuissance des pays européens à mettre sur pied une fiscalité des Gafa. Dans la mesure où la matérialisation géographique - puisque l'État, ce sont avant tout des frontières - est menacée, ce sont nos impôts, c'est-à-dire notre gagne-pain, qui sont menacés. Nous avons choisi de donner ce nom à notre commission d'enquête parce que c'est bien la souveraineté des États et des systèmes politiques qui est en cause.

Il y a une contradiction, dans vos propos, entre l'idée d'un réseau mondial, où l'individu participe à une information qui le déconnecte du territoire, et la réalité du complexe militaro-numérique américain qui fournit l'infrastructure. Existe-t-il vraiment un lien structurel entre les Gafa et ce système que vous évoquez, ou les États-Unis eux-mêmes peuvent-ils être dépassés par la dimension mondiale de cette puissance économique ?

S'appuyant sur une culture originale et un système politique centralisé et autoritaire, les Chinois ont adopté la stratégie nationale de formation d'une bulle à l'intérieur du système internet. Vous opposez ce système à la stratégie, moins autoritaire mais tout aussi volontariste, de la Russie qui a pénétré à l'intérieur du système internet. Un État peut-il se tenir hors de ce système ? Sans doute, s'il compte 1,3 milliard d'habitants. Dans le cas contraire, l'absorption est inévitable.

M. Pierre Bellanger. - Il y a des États souverains sur le réseau, à commencer par les États-Unis. Ils ont trois systèmes d'exploitation utilisés partout, y compris dans cette salle, qui définissent les règles et répondent des tribunaux américains. Les Chinois font de même, mais avec l'effet de bulle qui induit une forte vulnérabilité : le réseau fermé perd toujours face au réseau ouvert. Certes, le réseau ouvert est vulnérable, mais il s'est constitué en premier et sous la forme d'un empire, agrégeant des vassalités par la vertu de sa puissance. L'Europe est l'une de ces vassalités. La Russie tente de le déstabiliser, et un empire chinois s'est également constitué de son côté.

Pour ce qui nous concerne, il est hors de question de constituer une bulle : c'est une mauvaise stratégie et elle ne correspond pas à notre nature démocratique. La Corée du Nord, après tout, est souveraine. Il faut donc inventer une souveraineté ouverte. La souveraineté n'est pas la liberté mais une condition. Renoncer à la souveraineté numérique, c'est renoncer à nous-mêmes. Ce pays qui a forgé son indépendance dans le sang, avec son génie, sa force, ses talents, doit-il devenir une province d'un autre ? Nous ne pouvons pas céder, pour les générations passées comme pour les futures. Nous sommes à une de ces époques, rares, de grands choix, et c'est à notre génération qu'ils incombent. Les données du débat sont proches de celles du débat sur la communauté européenne de défense, dans les années 1950.

Les grandes sociétés américaines ont été aidées. Un grand réseau social nominatif a brûlé un milliard d'euros avant d'avoir un plan d'affaires : essayez donc de faire cela avec votre banque... Ce réseau avait à sa libre disposition toutes les données recueillies.

M. Gérard Longuet, rapporteur. - Aux États-Unis, la Standard Oil au début du XXe siècle, et plus récemment AT&T, la société quasi-monopolistique de télécom, ont été démantelées grâce à la législation anti-trust. Les Gafa pourraient-ils faire l'objet de mesures similaires ?

M. Pierre Bellanger. - Je ne le pense pas. On peut faire un parallèle avec la Compagnie des Indes. Le lien, le réseau, dans cet exemple, est la mer. Les Anglais prétendaient garantir la liberté des mers, parce qu'ils les contrôlaient. Les Américains font de même aujourd'hui. Les Compagnies des Indes étaient des sociétés hybrides possédant leurs propres forces militaires, des délégations de pouvoir, à l'occasion réajustées ou semoncées par le pouvoir. Les opérateurs numériques globaux ont un lien organique avec les États. Et bien sûr, l'Europe tient la place des Indes !

Comment réagir ? D'abord nous avons tout pour réussir. La taille n'entre pas en ligne de compte. La Corée du Sud est souveraine, Israël également, même en ayant passé des alliances. C'est donc une question de volonté politique. Comment la construire ? Ce n'est pas une question d'ingénieurs, d'argent, de ressources puisque nous avons tout cela en France, avec Bpifrance, l'Agence de l'innovation de défense, d'énormes capacités

d'investissement. Pourquoi, dans ce cas, rien ne s'est passé ? Lorsque l'on construit une maison, il faut commencer par les fondations, c'est-à-dire ici, par le droit et la République.

Une République a besoin d'un territoire, avec une règle commune et des frontières. Sur l'internet, il faut partir des données. La donnée personnelle a été consacrée dans le droit par la loi de 1978. Dans cette définition, une donnée personnelle renseignait exclusivement sur sa source. Aujourd'hui, il n'y en a plus. En effet, un rendez-vous que vous prenez concerne nécessairement plusieurs personnes. Les données sont en réalité un réseau par lequel tous les citoyens d'une nation sont liés ou, si l'on veut, une pelote de laine. Mon carnet d'adresses contient les adresses de mes amis, de ma famille, etc. Qu'est-ce que cette donnée au point de vue juridique ? Son possesseur conserve les droits individuels d'oubli, de rétractation, de modification, mais elle est indissociable des droits d'autrui. C'est une sorte de bien commun souverain. Notre rôle est de la créer juridiquement.

Il s'ensuit que le territoire est constitué des données en réseau de tous les citoyens d'une nation. Il est indissociable de la nation qui est étymologiquement, à la fois un lieu et ceux qui y naissent. Nous retrouvons ce mélange intime avec les données.

Ce territoire a besoin d'une frontière qui, sur le réseau, est constituée par le chiffrement : en d'autres termes, une donnée captée sur le territoire doit répondre à des protocoles de chiffrement souverain. Ce chiffrement peut être partiel ou total, porter sur l'action et le profil. Tout cela est défini par le droit.

Il y a enfin la règle commune, notre Constitution, qu'en l'espèce est comparable à un système d'exploitation dont tout dérive. Dans ce système, nous ne nous priverions pas de téléphones américains ou chinois, mais demanderions aux opérateurs d'inclure nos règles dans leurs systèmes d'exploitation.

D'aucuns pourraient comparer ce système au village d'Astérix. Il n'en est rien, parce qu'il serait tout à fait possible de passer des accords de souveraineté avec nos amis allemands ou espagnols. La mondialisation résulte non d'une universalisation, mais d'accords entre souverainetés.

Dans ce monde mondialisé, le premier domino doit être la socialisation ou la nationalisation des données, c'est-à-dire la création d'un bien commun souverain protégé par une frontière et administré par une règle commune imposée aux acteurs entrants. Un jouet venant de Chine, vendu par un magasin américain et acheté ici porte un label Union européenne. Il est possible d'agir de même dans le monde numérique.

Les données seraient stockées sur notre territoire et en sortiraient chiffrées. Pourquoi, dans une affaire qui concerne un algorithme, celui-ci ne pourrait-il être examiné par un juge d'instruction au prétexte qu'il n'est pas sur le territoire ? C'est inacceptable. L'impôt sera, lui, prélevé là où sont

collectées les données. C'est la logique du fisc français. Ces données doivent être sous notre droit. Il y a par exemple des algorithmes racistes dont les auteurs doivent être présentés devant nos tribunaux.

M. Rachel Mazuir. - Vous avez dit que la souveraineté américaine pouvait être comparée à celle des Chinois et de la Corée. Donald Trump n'a pas la même analyse, puisqu'il estime que les grands groupes en font trop à leur guise. Est-elle réelle, cette souveraineté ?

L'Europe a tenté de mettre en place une approche européenne de cette souveraineté. La France également, avec, en 2013, un plan de création d'une filière « Big Data » sur cinq ans par le ministre du redressement productif d'alors, Arnaud Montebourg. Qu'en a-t-il été ?

Vous assurez enfin que nous n'avons pas de problème d'ingénieurs, or ces formations ne sont menées à terme qu'à 70 % et les agences qui ont besoin d'ingénieurs ont beaucoup de mal à recruter. En avons-nous vraiment assez ?

M. Patrick Chaize. - À vous écouter, la solution serait simple : définir un cloud sur le territoire national, un lieu de stockage des données. Nous avons déjà tenté de le faire, avec un investissement lourd, mais nous avons échoué. Pourquoi ? Comment éviter que l'échec ne se reproduise ?

Le chiffrement alourdit les communications et pose un problème environnemental, car sa généralisation engendrerait une énorme consommation d'énergie énormes. Le confirmez-vous ? N'y a-t-il pas une cible à rechercher dans le chiffrement ?

Mme Sylvie Robert. - Vous avez commencé par nous alarmer, mais vous avez aussi mis en évidence une prise de conscience collective et proposé des solutions. L'idée qu'il n'existe pas de données personnelles est très intéressante : nous participons d'un bien commun souverain, ce qui réclame une prise de conscience individuelle. En termes d'usage, de pratique, de valeurs et de principes, nous devrons respecter des règles. Sommes-nous à ce niveau, de prise de conscience individuelle, nous porteurs de données, et quelles sont les solutions pour y parvenir ?

M. Pierre Bellanger. - Y a-t-il une souveraineté réelle des États-Unis ? Oui. Cette souveraineté n'exclut pas les conflits avec ces entreprises, les rapports de force, les coups de force, les oppositions, les alliances. Globalement, le système ne cesse de se renforcer, de progresser et de se développer. L'une de ces sociétés a une trésorerie supérieure à l'État fédéral. Un transporteur vient d'entrer en bourse avec une valorisation de 100 milliards de dollars, équivalente à celle de l'ensemble du transport dans le monde. Cette valorisation est soutenue par tout un système. Il n'y a pas de chef d'orchestre, mais des musiciens qui s'entendent bien.

L'Europe, elle, a très peu à voir avec la souveraineté. Elle fait du droit, elle administre. On peut comparer cela à la construction d'un château

de cartes en commençant par celles du haut, sans les fondations que sont le territoire, la frontière et la règle. Le Règlement général sur la protection des données (RGPD) est le fruit d'une formidable prise de conscience, mais comment l'appliquer ? La captation des données est fondée sur le consentement individuel, or vous comme moi-même y consentons tous les jours à de nombreuses reprises, distraitement, pour accéder au contenu. C'est une parodie, une fantasmatique de droit, sans les bases solides de la souveraineté. C'est bien, mais insuffisant. Le RGPD donne certes la possibilité de taxer des entreprises sur leur chiffre d'affaires, mais sera-t-il reconnu à l'extérieur des frontières européennes ?

Je ne sais pas quel a été le résultat des initiatives d'Arnaud Montebourg, mais il a contribué, avec son panache, à la prise de conscience.

En affirmant que nous n'avons pas de problème d'ingénieurs, je voulais dire que nous n'avons pas besoin de confier nos protocoles de chiffrement à des acteurs étrangers. L'Agence nationale de sécurité des systèmes d'information en est tout à fait capable, pour la défense de la nation.

Le cloud national m'inspire les mêmes réserves que le RGPD. Nous utilisons pour cela des serveurs de marque étrangère, qui relèvent du Patriot Act, du Cloud Act. Rien ne protège les données ni ne fonde leur statut : c'est incantatoire.

Je ne crois pas que le grand public ait pris conscience du problème. Le peuple français est habitué aux règles en tout genre : un décret fixe la hauteur des margelles dans les piscines municipales... Le citoyen se sent en confiance dans cet environnement. L'internet est perçu sous cet angle : il est légal, donc il est sans doute protégé. Il appartient à l'État de garantir la sécurité de tous dans cet espace, ce qui ressort du droit. Il devrait être interdit de donner accès à son carnet d'adresses à une application, sauf si celle-ci a été expressément autorisée à demander cet accès.

Le plus dur est la prise de conscience. De plus en plus d'événements nous obligeront pourtant à mettre en place cette souveraineté numérique : il faudra protéger nos centrales, nos infrastructures. Avoir recours à des systèmes d'exploitation étrangers pour les protéger revient à sous-traiter les douanes. Il deviendra inacceptable pour la population que des données aussi cruciales ne soient pas protégées.

D'après les études, ce sentiment est en train de monter. Un tiers des citoyens sont inquiets : cela constitue un socle d'opinion publique. Il y a également une prise de conscience des élites. Il y a enfin un moment politique, et ce moment est maintenant, pour créer le premier domino du bien commun souverain. À l'image du pâté d'alouette, il suffit d'un peu de souverain dans le réseau pour que tout le devienne. Rien ne nous empêche de nouer des alliances internationales : Thierry Breton a évoqué un Schengen des données.

Enfin, toutes ces données doivent être stockées dans nos serveurs. On crée ainsi un socle et une industrie. En Allemagne, pays le plus protecteur des données au monde, les sociétés américaines font appel à des prestataires allemands pour garantir que les données captées seront protégées.

Voyez les enceintes connectées : elles sont très utiles, mais en échange, nous acceptons des micros chez nous. Ne renonçons pas à ces services qui améliorent notre vie, mais ne les payons pas de notre vie privée, car un opérateur pourra s'en servir pour orienter nos choix.

M. Hugues Saury. -Vous avez dit que le réseau pouvait être notre plus grande chance et notre principale régression. C'est finalement le propre de l'homme, qui peut le meilleur et le pire à la fois.

L'histoire du réseau est celle d'une conquête. Aujourd'hui, c'est l'argent qui est au pouvoir. Recherche-t-on le passage du principe de l'argent roi à un système où les États reprennent leur souveraineté pour empêcher que tout soit libre d'accès ?

M. Pierre Bellanger. - C'est l'inaction des gouvernements successifs qui a abouti à cet abandon. Voyez L'Étrange défaite, de Marc Bloch. Pourquoi est-ce arrivé ? Pourquoi autant de gens intelligents, respectables sont-ils arrivés à ce consensus consistant à choisir ne rien faire ? Oui, l'État doit revenir en force. Là où il n'y a pas de secret, de sphère privée garantie par l'État, nous sommes dans une situation de transparence forcée. Il n'y a pas d'isoloir sur l'internet. Votre vision, monsieur Saury, est juste.

C'est le bitcoin qui a de fortes implications environnementales, car ce système consiste à créer d'énormes rouleaux de données virtuelles qui s'allongent à chaque transaction. C'est à mon sens intenable car seulement possible dans un environnement fermé. Certes, le chiffrement consomme de l'énergie, mais ce sont les données cryptées de type bitcoin qui alertent véritablement. Avec une puissance informatique qui double chaque année, le surcroît de consommation est absorbable.

M. Gérard Longuet, rapporteur. - Pour que la sphère privée soit garantie par l'État, il faut que les usagers le souhaitent. Or ils vont chercher une satisfaction sur le réseau, et ils choisiront l'offre qui leur paraît la plus généreuse, la plus diversifiée. Nous acceptons de bon cœur, en cliquant, de livrer nos données parce que le ratio entre un risque mal identifié et l'avantage de l'accès immédiat nous conduit à sacrifier la propriété de nos données.

Dans votre esprit, ce bien commun souverain revêt-il un caractère obligatoire ou est-il une option ?

M. Pierre Bellanger. - Nous sommes en permanence tentés par la facilité : ne pas mettre de ceinture, de casque, ne pas se vacciner. En démocratie, on a le droit de se faire du mal, mais pas d'en faire aux autres.

La collecte de nos données de santé permet, par exemple, de constituer des échantillons avec des personnes présentant un profil similaire et, à partir de là, de concevoir une police d'assurance.

Mme Sylvie Robert. - Mais le RGPD offre une protection.

M. Pierre Bellanger. - Il est aujourd'hui possible de prédire une occurrence de cancer du côlon d'un individu à partir de ses tickets de caisse. Le cancer est purement personnel, mais les tickets de caisse ne le sont pas.

M. Gérard Longuet, rapporteur. - Ce que vous appelez de vos voeux serait une révolution culturelle.

M. Pierre Bellanger. - Nous avons changé d'heure, de monnaie, modifié nos régions... Avoir un statut des données qui protègera chacun est important.

M. Gérard Longuet, rapporteur. - Pour le fondateur d'une radio libre, vous êtes particulièrement confiant dans l'État !

M. Pierre Bellanger. - Je le suis parce que je mets mes enfants à l'école publique, que je me fais soigner à l'hôpital public. Il n'est pas d'internet hors sol, et je préfère être sous le contrôle d'un État où j'ai le droit de vote.

M. Gérard Longuet, rapporteur. - On va pourtant chercher de l'information dans le monde entier.

M. Pierre Bellanger. - Où sont les serveurs, quel est le protocole ? Il y a toujours une souveraineté en jeu, il est par conséquent préférable que ce soit la nôtre.

J'apprécie particulièrement votre travail, car nous arrivons au moment des fondations, après une période d'aveuglement. À chaque élection, nous nous demanderons qui nous manipule, entre un serveur américain, un terminal chinois et des informations russes. C'est votre commission d'enquête qui ouvre ce débat.

M. Franck Montaugé, président. - Faut-il comprendre de vos propos que tout échange ou utilisation d'une information produite sur le territoire allemand donne lieu à un contrat avec l'entreprise qui voulait commercialiser les données, tout lien avec l'extérieur se faisant par l'intermédiaire du contrat.

M. Pierre Bellanger. - Si notre Commission nationale de l'informatique et des libertés devenait une sorte d'agence des données, une entreprise allemande voulant faire des affaires en France devrait solliciter un accord entre notre agence et son homologue allemande, qui créerait une passerelle de règles communes. Ce n'est pas encore le cas en Allemagne, puisque nous sommes sous la logique globale du RGPD.

Pour le moment, chacun fait à sa guise et la plupart d'entre nous sont sous contrôle étranger. L'application numérique d'une grande banque a

récemment vu sa mise à jour refusée par la plateforme : de Dublin est arrivé un message l'informant que son protocole de chiffrement n'était pas accessible... Il n'y a plus de secret bancaire !

Tout part de la donnée : c'est elle qui fait la taxe. Je l'ai d'ailleurs appelée la « dataxe » dans un document.

M. Franck Montaugé, président. - Qu'en est-il du volet de la culture et de l'éducation ?

M. Pierre Bellanger. - Si les données des élèves sont collectées pour être vendues, ils sont mis en danger car chacun de leurs actes le suivra tout au long de sa vie. Il faut une étanchéité absolue des parcours scolaires. Rien ne remplace le professeur, et l'utilisation des supports numériques de travail pourrait être dévoyée. Pour l'éviter, il revient à l'Éducation nationale de générer ses propres outils. La gendarmerie nationale a développé des outils à partir de logiciels libres : voilà un excellent modèle.

Nous sommes dans une culture de captation de données qui met en danger les acteurs nationaux. Ceux-ci n'ont pas les mêmes capacités de captation, parce que les données sont captées ailleurs. La situation de la France est celle d'une équipe de football qui joue sur un terrain qui penche vers son but. Il faut le remettre droit, et c'est la loi qui le fera. Ne surestimons pas la résistance des acteurs étrangers, car ceux-ci l'ont accepté dans tous les autres pays où cela leur a été demandé.

M. Franck Montaugé, président. - Merci de cet exposé très intéressant.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible *en ligne sur le site du Sénat*.

Audition de Mme Claire Landais, secrétaire générale du Secrétariat général de la défense et de la sécurité nationale (SGDSN), de M. Julien Barnu, conseiller pour les questions industrielles et numériques et de M. Gwenaël Jezequel, conseiller pour les relations internationales, le 23 mai 2019

M. Franck Montaugé, président. - Mes chers collègues, notre commission d'enquête poursuit ses travaux avec l'audition de Madame la secrétaire générale de la défense et de la sécurité nationale, Claire Landais. Elle est accompagnée ce matin de Julien Barnu, conseiller pour les questions industrielles et numériques, et de Gwenael Jezequel, conseiller pour les relations institutionnelles.

Cette audition sera diffusée en direct sur le site Internet du Sénat. Elle fera également l'objet d'un compte rendu publié.

Enfin, je rappelle, pour la forme, qu'un faux témoignage devant notre commission d'enquête serait passible des peines prévues aux articles 434-13, 434-14 et 434-15 du code pénal. J'invite chacun d'entre vous à prêter serment de dire toute la vérité, rien que la vérité ; levez la main droite et dites : « Je le jure. ».

Conformément à la procédure applicable aux commissions d'enquête, Mme Claire Landais, M. Julien Barnu et M. Gwenael Jezequel, prêtent serment.

Placé auprès du Premier Ministre, le secrétariat général de la défense et de la sécurité nationale (SGDSN) est chargé aussi bien d'anticiper les risques et les menaces, que de suivre les questions de relations internationales, préparer les réponses aux crises, et assurer la cyber défense entre autre. C'est un organisme interministériel - vous nous l'expliquerez.

Il a également présenté en février 2018 la revue stratégique de cyberdéfense, sous l'égide de votre prédécesseur, Louis Gautier, qui s'appuyait notamment sur une étude prospective à l'horizon 2030, « Chocs futurs », passant au crible les impacts des transformations et ruptures technologiques sur notre environnement stratégique et de sécurité.

Pour toutes ces raisons, il nous a semblé essentiel de vous entendre au début des travaux de notre commission d'enquête. Je crois savoir que vous avez réalisé en vue de cette audition un réel travail conceptuel sur la souveraineté numérique, je vous propose de nous le présenter avant d'engager le débat.

Mme Claire Landais, Secrétaire générale de la défense et de la sécurité nationale. - Les réflexions que je vais vous présenter sont le fruit d'un travail collectif. Pour avoir une vision globale d'ensemble sur notre souveraineté numérique, nous avons besoin de connaissances techniques pointues de certains secteurs, les personnes qui m'accompagnent aujourd'hui en témoignent. Je vous propose de vous livrer notre vision des grands enjeux

de la souveraineté numérique et de répondre à toutes vos interrogations sur la manière dont le SGDSN, acteur de coordination, intervient sur cette problématique.

La souveraineté numérique - c'est-à-dire notre capacité à rester maître de nos choix, de nos décisions et de nos valeurs dans une société numérisée - recouvre trois aspects complémentaires.

Première composante, la souveraineté à l'ère numérique : comment préserver les composantes traditionnelles de notre souveraineté, dans un contexte où le numérique remet en question les monopoles régaliens, parce qu'il crée des acteurs de substitution ou parce qu'il fragilise les outils des activités monopolistiques régaliennes ?

Deuxième dimension, la souveraineté dans l'espace numérique : comment conserver notre capacité autonome d'appréciation, de décision et d'action dans le cyberespace ? C'est la thématique abordée par la revue de cyberdéfense que vous évoquiez dans votre propos introductif ;

Enfin, troisième enjeu, la souveraineté des outils numériques : comment maîtriser nos réseaux, nos communications électroniques et nos données, publiques ou personnelles ?

Comment, d'abord, préserver les composantes traditionnelles de notre souveraineté, dans un contexte où le numérique remet en question les monopoles régaliens ?

Les nouvelles technologies ont progressivement permis à des acteurs privés de rivaliser avec les États, en assumant des fonctions faisant historiquement et sans conteste jusqu'alors l'objet de monopoles régaliens. Cette tendance est en partie irréversible, ce qui ne signifie pas qu'il faille renoncer à en organiser les modalités. Chaque État se voit ainsi conduit à arbitrer entre les attributs de souveraineté qu'il choisit de préserver en priorité, et ceux qu'il peut accepter de déléguer à la sphère privée, le cas échéant de façon encadrée.

Je n'évoquerai pas devant vous l'attribut régalien, pourtant historiquement important, que constitue le privilège de battre monnaie ni sa remise en cause par les crypto-monnaies, du type Bitcoin, car nous dépasserions de beaucoup le champ de compétence du SGDSN.

Parmi ces grands monopoles régaliens aujourd'hui contestés, citons d'abord l'identification officielle, le privilège d'authentifier les personnes. Les États ne sont aujourd'hui plus, de fait, les seuls à pouvoir délivrer des titres attestant de l'identité de quelqu'un : de grands acteurs privés comme les réseaux sociaux, au premier rang desquels Facebook -avec Facebook Connect -, jouent dorénavant le rôle de fournisseurs d'identité. Les services d'authentification qu'ils proposent sont déjà largement utilisés, à ce stade par des sites Internet privés et pour des utilisations non sensibles. Le risque est réel que, sans réponse des États, de telles solutions puissent, à moyen terme,

devenir de fait les identités numériques d'usage, évinçant le rôle des pouvoirs public.

L'Europe et la France ont apporté d'ores et déjà certaines réponses : La loi du 7 octobre 2016 pour une République numérique prévoit ainsi d'encadrer la fourniture d'identité numérique par le secteur privé, une identité numérique étant présumée fiable uniquement si elle répond à un cahier des charges établi par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Sont également développés, d'une part, un service d'authentification national - la plateforme FranceConnect conçue par la direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC) -, et d'autre part une identité numérique souveraine - via le projet ALICEM (Authentification en ligne certifiée sur mobile) du ministère de l'Intérieur -, en cours d'évaluation par l'ANSSI. Enfin, au niveau européen, a été introduit un cadre juridique commun, avec le règlement adopté en 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, dit « eIDAS », qui prévoit la reconnaissance entre les États membres et l'interopérabilité des méthodes nationales d'identifications numériques.

Autre monopole régalien par excellence, celui de la violence légitime : attaquer et défendre. Face à une menace cyber qui ne cesse de croître, certains acteurs, essentiellement étatsuniens, remettent en cause le monopole des États dans l'usage de la violence légitime. Se fondant sur une interprétation discutable du droit à la légitime défense dans l'espace cyber, qui n'est pas la nôtre, ils font la promotion d'une doctrine offensive de réponse aux attaques, autorisant une riposte par les acteurs privés eux-mêmes (« hack back ») qui va au-delà de la simple protection de leurs propres systèmes d'information, autorisant par exemple des intrusions dans les systèmes adverses pour les détruire. Les risques que voit la France à une telle légalisation de pratiques dans certains pays et à leur diffusion au niveau international sont bien réels : risque d'erreur d'attribution, d'abord, car face à la difficulté pour obtenir une identification fiable de l'origine de l'attaque - et à ce titre, une action de riposte non encadrée pourrait prendre pour cible un tiers innocent ; risque de dommage collatéral et de riposte incontrôlée, d'autre part, de nature à aggraver l'instabilité du cyberespace.

Dans ce contexte, la France a choisi de maintenir l'interdiction actuellement en vigueur de cette pratique en droit français et de prôner activement son interdiction au niveau international. Ainsi, l'Appel de Paris pour la confiance et la sécurité dans le cyberespace, rendu public par le ministre de l'Europe et des affaires étrangères le 12 novembre dernier au Forum de Paris sur la Paix, et soutenu par le Président de la République à l'occasion de son discours à l'UNESCO devant le Forum sur la gouvernance de l'Internet, a été l'occasion de réaffirmer le monopole étatique de la violence légitime. Cette initiative se décline aujourd'hui de façon opérationnelle dans différents fora, notamment à l'OCDE et à l'ONU.

Dernier attribut régalien contesté : assurer la sécurité intérieure. Il s'agit là moins de lutter contre la substitution d'acteurs privés que de répondre à l'affaiblissement des outils de l'action régalienne. L'efficacité de nos services d'enquête judiciaire et de renseignement repose dorénavant sur des technologies numériques pour lesquelles les offres nationale et européenne sont lacunaires, ce qui nous conduit à dépendre d'offres étrangères, par exemple pour le traitement de données massives et l'acquisition de capacités vulnérabilités informatiques. Il est donc essentiel que l'État travaille de concert avec l'industrie pour faire émerger des solutions nationales ou européennes. Il nous faut, en outre, pouvoir correctement faire face à l'évolution constante des normes et des outils technologiques, par exemple dans le domaine de la surveillance légale des communications pour ne pas être pris de court par le développement des réseaux 5G.

Deuxième aspect de la souveraineté numérique : Comment conserver notre capacité autonome d'appréciation, de décision et d'action dans le cyberespace ? Ce second volet de notre souveraineté numérique concerne le maintien de la capacité de l'État et, dans un certain sens, de nos entreprises et citoyens, à disposer d'une autonomie d'appréciation, de décision et d'action dans le cyberespace.

En ce qui concerne l'État, la France a fait le choix de conserver une autonomie de décision en matière de défense et de sécurité du cyberespace. Atteindre cet objectif repose sur une capacité souveraine à détecter les attaques informatiques qui affectent l'État et les infrastructures critiques - je pense aux opérateurs d'importance vitale (OIV), notamment. À ce titre, l'ANSSI développe ses propres systèmes de détection pour la supervision des administrations, et ses travaux ont permis de faire émerger des solutions industrielles de confiance pour la France au profit des entreprises. L'agence a ainsi qualifié en avril 2019 les sondes de détection de deux industriels français.

En outre, nos capacités nationales de détection ont été significativement renforcées par la loi de programmation militaire pour 2019-2025. Ses dispositions permettent aux opérateurs télécoms de mettre en oeuvre des dispositifs de détection au sein de leur réseau pour mieux repérer les attaques informatiques, autorisent l'ANSSI à donner à ces opérateurs des marqueurs ou signatures d'attaques informatiques pour les aider à les repérer, et ont ouvert la voie au déploiement de sondes par l'agence en cas de risque pour les systèmes informatiques de l'État, d'opérateurs d'importance vitale ou d'opérateurs de services essentiels.

Enfin la France souhaite garder une capacité souveraine à attribuer les cyberattaques. Développer et maintenir une telle capacité est un choix d'engagement majeur, qui implique de ne pas dépendre de certains de nos grands partenaires. Au vu des investissements nécessaires, la maîtrise de telles capacités ne sera accessible à terme qu'à un nombre très limité de pays

qui auront fait le choix stratégique de les détenir. La France a bien l'intention d'en faire partie.

La France développe une doctrine nationale de découragement et de réaction dans le cyberespace. Elle repose sur une méthode nationale d'évaluation de la gravité d'une cyberattaque et un schéma de classement des cyberattaques qui intègre toute la palette des outils et normes mobilisables - et cela implique de faire se parler des acteurs de cultures parfois différentes. La réponse peut passer par la judiciarisation, se traduire par une attribution publique (« *name and shame* » en vue d'un impact réputationnel), voire - dans la mesure où il n'est pas exclu qu'une cyberattaque puisse atteindre le seuil de l'agression armée au sens de l'article 51 de la Charte des Nations Unies - par la mobilisation de capacités offensives dans le milieu cyber comme dans les autres milieux. Ce dernier point relève principalement du ministère des armées, et je renvoie au discours de Mme Florence Parly en février dernier. L'arme cyber est aujourd'hui pleinement intégrée parmi les capacités opérationnelles des armées et fait l'objet d'une doctrine qui encadre son emploi dans les opérations militaires sur les théâtres d'opération extérieurs, dans le respect du droit international.

Fruit également de la revue cyber et de la réflexion sur la gouvernance, l'articulation entre dimensions défensive et offensive obéit à une doctrine qui donne la priorité à la première, tout en privilégiant le dialogue entre acteurs responsables des deux chaînes.

La France promeut, enfin, à l'international sa vision selon laquelle le droit international est applicable au cyberespace et l'attribution publique reste une décision politique qui relève de la souveraineté et ne peut donc être déléguée à une organisation internationale. Dans ce domaine, notre pays souhaite garder la main.

Pour nos entreprises, il s'agit de préserver une capacité à innover dans un contexte d'hégémonie des géants américains du numérique - mais nous sommes là sur des questions hors du champ de compétence SGDSN.

L'autonomie d'appréciation et de décision de nos citoyens passe par la préservation de la sincérité du débat démocratique, face au phénomène émergent de manipulation de l'information par des puissances étrangères. Le rôle de la société civile reste essentiel, l'État pouvant fournir des outils pour lutter contre ces manipulations, notamment en période électorale. L'Union européenne a créé un réseau d'alerte en ce sens à l'occasion des élections.

Troisième aspect de la souveraineté numérique : Comment maîtriser nos réseaux, nos communications électroniques et nos données ? Notre souveraineté numérique passe en effet par notre capacité à protéger nos réseaux de télécommunication - et les données qui y transitent - des actions d'espionnage et de sabotage.

En matière de sécurité et de résilience des réseaux, des dispositions législatives existent déjà, dans notre code pénal notamment. Celles figurant aux articles R. 226-1 et suivants permettent un contrôle des équipements qui constituent le coeur des réseaux, pour préserver l'impératif de la protection de la vie privée et du secret des correspondances. Les demandes sont aujourd'hui instruites par l'ANSSI. Toutefois, au regard de l'importance croissante prise par les réseaux mobiles, notamment par la 5G et les nouveaux usages qu'elle permettra dans un futur bien plus proche que prévu, il paraît nécessaire d'apporter rapidement des évolutions au cadre juridique actuel, tant dans ses modalités que pour consacrer une finalité de protection de la sécurité nationale. Nous souhaiterions dès lors que puisse être soumise à autorisation préalable du Premier ministre - déléguée au SGDSN après instruction par l'ANSSI - l'exploitation de certains équipements des réseaux mobiles pour les opérateurs télécoms qui sont opérateurs d'importance vitale. Un amendement en ce sens avait été déposé, sans suite, dans la loi « PACTE », dispositions désormais reprises par une proposition de loi en cours d'examen devant le Parlement.

La protection des réseaux passe également par celle de nos câbles sous-marins, essentiels dans l'architecture des réseaux actuels. La problématique de la résilience se double d'un enjeu d'attractivité pour notre territoire, et nos réflexions en la matière mobilisent plusieurs départements ministériels, afin que nous soyons compétitifs, notamment en termes de normes et d'interconnections.

En matière de protection des données et des communications, les exigences sont graduées, dans une logique de cercles concentriques. Au coeur, pour les données et communications classifiées, nous devons viser une obligation de résultat, garantissant leur protection contre des attaques ciblées des adversaires les plus compétents. Cette ambition implique la maîtrise nationale de certaines technologies, au premier rang desquelles le chiffrement des communications. La France possède dans ce domaine une industrie de confiance, apte à fournir des équipements de très haut niveau de sécurité.

Pour le champ médian des données et communications sensibles, des exigences impératives doivent pouvoir être fixées, sous forme de label de l'État.

Cette déclinaison en plusieurs sphères s'applique pleinement à la question du cloud. Ainsi, pour ses données stratégiques classifiées, l'État aura recours exclusivement à un cloud interne. En revanche, pour d'autres données publiques et pour les besoins des entreprises, la qualification des clouds par l'ANSSI permettra d'identifier les offres qui apportent des garanties suffisantes vis-à-vis des risques tant techniques et que juridiques. Les entreprises doivent elles-mêmes faire l'effort de segmenter leurs données en fonction de leur caractère stratégique ou sensible.

Sur cette question du cloud, notre environnement juridique mérite également d'être adapté au rapport de force qui s'engage actuellement avec certains de nos partenaires tentés par une application extraterritoriale de leur droit. Dans la perspective de tels conflits de normes, il est essentiel pour rester crédibles de pouvoir leur opposer des outils comme le règlement général sur la protection des données (RGPD) ou une « loi de blocage » rénovée. Ces textes normatifs auront, d'une part, un effet incitatif dans les négociations qui doivent s'engager entre États et, d'autre part, un effet dissuasif sur les sociétés étrangères concernées, exposées au risque d'être en infraction avec nos normes.

M. Stéphane Piednoir. - Dans ce champ cyber très concurrentiel, où les hackers ont toujours un temps d'avance, comment s'assurer de conserver les meilleures compétences et d'attirer les talents ?

M. Jérôme Bascher. - Dans le monde physique, en cas d'incident, les États n'hésitent pas à nommer la provenance d'un navire ou d'un avion étranger violant l'intégrité du territoire national. Pourquoi une telle discrétion en cas de cyber-attaques ? De mémoire, il y a deux ans, seule la Finlande a identifié publiquement le grand pays voisin source, selon elle, d'une telle attaque...

M. Rachel Mazuir. - Quelques remarques seulement. Concernant d'abord l'ANSSI - que je connais bien pour avoir été, avec mon collègue Olivier Cadic, co-rapporteur délégué sur le volet cybersécurité lors de l'examen de la loi de programmation militaire pour 2019-2025- personne ne peut dire, hélas, que l'agence ait aujourd'hui trop de moyens, même si je note les engagements du Président de la République en la matière !

Je relève aussi dans vos propos la particulière difficulté des opérations d'attribution des cyberattaques : c'est un processus complexe et bien long. J'ai le sentiment qu'une réponse plus vigoureuse reste indispensable en la matière. Nous ne sommes pas épargnés, nous avons tous entendu parler de la dernière en date, qui concernait la plateforme du service « ARIANE » du ministère de l'Europe et des affaires étrangères.

S'agissant de l'articulation nécessaire entre moyens défensifs et offensifs, je note que les premiers existent bien, alors que les seconds me semblent moins performants.

M. Hugues Saury. - Tout en faisant le constat de la grande intelligence de nos systèmes d'attaque et de défense cyber, n'y a-t-il pas un paradoxe à ce qu'ils passent tous par des câbles sous-marins - notamment ceux au large de Djibouti - constituant ainsi autant de points de faiblesses et de dépendances dans le système ?

Mme Claire Landais. - Concernant la concurrence dans le recrutement des talents, le principal obstacle reste, du point de vue de l'État, un problème de salaire. Nous souffrons souvent de la comparaison avec le privé pour conserver nos ingénieurs et les profils industriels qui nous

intéressent. Une réflexion est cependant en cours, vous le savez, sur l'évolution du droit de la fonction publique, qui devrait nous donner ces capacités de souplesse nécessaires aux recrutements dans un secteur particulièrement tendu. La DINSIC a récemment diffusé une circulaire qui rappelle la panoplie des outils de recrutement déjà utilisables. Ne négligeons pas non plus l'attrait du drapeau et la renommée de l'ANSSI, dont la réputation d'excellence permet de recruter les meilleurs éléments. Le passage par l'agence reste pour beaucoup une garantie ultérieure de reconversion ou de passerelle réussie dans le privé.

Concernant les moyens de l'ANSSI, je partage votre diagnostic, tout en constatant que la trajectoire d'emploi est positive. Mettre des moyens dans la cyberdéfense est une priorité assumée de l'État.

La discrétion dans l'attribution des cyberattaques et la faible publicité qui leur est ainsi donnée tient d'abord, à la difficulté technique inhérente au mécanisme d'identification des responsabilités. La méthode reste celle du faisceau d'indices, et l'entraide judiciaire est compliquée, soit par mauvaise volonté, soit tout simplement par manque de compétences techniques de certains pays. Sans jamais s'interdire de donner un caractère public à l'attribution, le mécanisme est jusqu'à présent pas ou peu utilisé car il est mis en balance avec l'efficacité réelle des messages passés à titre confidentiel. Dans une matière aussi délicate, rendre public un nom c'est aussi prendre le risque de figer les positions et de compliquer l'engagement d'un dialogue. Mais je peux comprendre la frustration des parlementaires et du public face à cette apparente réserve dictée par l'efficacité.

Concernant le bon équilibre de nos moyens entre les dimensions défensives et offensives, une même discrétion rend peut-être ici moins visible l'ampleur des ressources déployés dans la seconde catégorie. La loi de programmation militaire prévoit bien des engagements sur ce point, rappelés encore récemment par la ministre. Le modèle français prévoit à cet égard une séparation spécifique entre les deux chaînes, qui doivent être bien articulées.

M. Gérard Longuet, rapporteur. - Madame la secrétaire générale, vous avez une formation de juriste, vous êtes conseillère d'État, vous savez donc que l'autorité de l'État s'exerce sur un territoire défini par des frontières, sur lequel vivent des citoyens, et qui est doté du monopole de l'usage de la force pour trancher un éventuel conflit ou pour protéger sa population. Dans l'espace numérique, y a-t-il des frontières et avez-vous le sentiment que l'État soit en mesure de les définir ? Les entreprises ne peuvent-elles pas aujourd'hui être tentées d'organiser leur riposte et donc de priver l'État du monopole de la force pour trancher un conflit ? En somme, c'est l'assise traditionnelle de la souveraineté qui est sérieusement ébranlée dans l'espace numérique, qui est virtuel et insaisissable.

Mme Claire Landais. - L'ère numérique fragilise effectivement ces monopoles régaliens. Des acteurs privés peuvent aujourd'hui se substituer à

l'État ou, à tout le moins, le concurrencer en se dotant parfois plus facilement ou plus rapidement que lui, des outils classiques de la souveraineté.

Les frontières sont à repenser mais peuvent être reconstituées. Je parlais des cercles concentriques, qui vont du plus au moins sensible. C'est aussi à l'État de repenser ces frontières logiques, au-delà des frontières physiques. Certains sont capables de penser au-delà de leur sphère normale d'influence et de juridiction. On pense notamment à l'extra territorialité de la législation. Il nous - Français et plus probablement Européens - faut également savoir recréer des frontières. Par ailleurs, certains États ont su se fermer au monde numérique extérieur. C'est donc possible, mais je ne suis pas certaine que ces États soient porteurs de modèles que nous souhaiterions suivre. Le numérique n'est donc pas exclusif de capacités de souveraineté, y compris robustes, si ce n'est autoritaires.

Je vous rejoins en revanche parfaitement sur le monopole de la violence légitime. Les acteurs privés pourraient en effet se faire justice eux-mêmes, en pénétrant dans les systèmes d'information de l'attaquant pour aller détruire l'origine de l'attaque, prenant le risque de se tromper d'attaquant ou de générer des dommages collatéraux, pour reprendre les termes du droit international humanitaire - qui s'applique bien au monde numérique -, avec des risques d'effets de bord si ce n'est d'effet boomerang. D'où l'idée que l'État doit garder ce monopole de la violence légitime.

M. Gérard Longuet, rapporteur. - Pensez-vous que le lieu de stockage des données constitue un trait d'union entre la souveraineté traditionnelle des États et la réalité numérique ? Le support matériel est-il le point d'ancrage permettant à un État de faire usage de ses prérogatives de souveraineté ?

Mme Claire Landais. - Le régime applicable au mode de stockage des données est évidemment important. Cela se constate dans la stratégie de cloud de l'État, qui conduit à stocker les données protégées par le secret de la défense nationale dans un cloud interne à l'Etat. Mais on ne peut pas imposer à certains acteurs privés un mode de stockage sans leur offrir des solutions industrielles qui répondent à leurs besoins. On sait que le stockage est aujourd'hui moins important que les services qui y sont liés, lesquels sont offerts par des géants du numérique en face desquels, actuellement, nous ne disposons pas nécessairement de concurrents potentiels. Nous réfléchissons très activement aux voies et moyens de faire émerger des solutions associant stockage, hébergement et services. C'est un préalable avant d'envisager de recourir à des modes d'action plus autoritaires, tels que les régimes des opérateurs d'importance vitale ou des opérateurs de services essentiels. La loi de programmation militaire de 2013 et la transposition de la directive NIS (Network and Information System Security) sont autant de jalons récents dans notre histoire, où les pouvoirs publics ont considéré que le moment était venu d'imposer à des opérateurs critiques certaines obligations en termes de sécurité physique ou logique de leurs systèmes d'informations. On

ne peut envisager le recours à ce type de solutions que si l'on est certain que ces acteurs disposent de solutions industrielles qui leur permettent de ne pas en pâtir.

M. Laurent Lafon. - Y a-t-il eu des tentatives de perturbation des élections européennes sur les réseaux sociaux ?

Mme Claire Landais. - Je peux vous dire que nous avons nettement progressé sur ce sujet, à travers la mise en place de capteurs et en utilisant tous les réseaux de veille disponibles. Jusqu'à présent, ces derniers étaient dispersés, parfois redondants sur certains aspects et notre dispositif pouvait comporter certains angles morts. Nous avons donc essayé de rationaliser notre vision d'ensemble afin de créer un réseau sans angles mort, d'améliorer nos capacités de détection, et de renforcer nos interactions avec les plateformes en leur signalant les éléments artificiels que nous pouvons repérer, les mettant ainsi en capacité d'en tirer les conséquences. Nous avons donc réellement accru notre sensibilité, notre visibilité et notre capacité à avoir des relais dans le monde de la société civile, des grandes plateformes, pour lutter contre les risques de remise en cause de la sincérité du débat électoral.

M. Jérôme Bascher. - Avez-vous une stratégie pour vous doter d'un réseau de fibre optique indépendant du monde civil ? Sur les équipements actifs, le fait qu'il n'y ait que très peu de fournisseurs dans le monde et qu'ils ne soient pas tous basés en France - ou à Balard ! - pose-t-il problème ? Même question sur la téléphonie car un très grand pays outre-Atlantique érige actuellement des barrières à la pénétration de téléphones chinois qui, parfois, équipent les hauts gradés du ministère des Armées.

Mme Claire Landais. - Le SGDSN est un service du Premier ministre. Nous travaillons évidemment très étroitement avec le ministère des Armées car le Premier ministre est responsable de la défense nationale et, si l'ordonnance de 1959 distingue bien défense civile et défense militaire, nous travaillons souvent sur des sujets qui exigent d'articuler défense civile et défense militaire.

La protection des communications classifiées correspond bien aux activités du SGDSN, avec, d'une part, le centre de transmissions gouvernementales (CTG), unité militaire gouvernementale logée au sein de notre secrétariat général et, d'autre part, l'ANSSI. S'agissant de la protection des communications relevant du secret de la défense nationale, le besoin de systèmes d'informations qui assurent la confidentialité, la résilience, à travers, par exemple, du chiffrement et des solutions souveraines est essentiel et nous y veillons très sérieusement. Nous menons actuellement une réflexion sur les réseaux de transport, pour lesquels la nécessité d'un réseau dédié distinct du reste du monde de l'internet reste à démontrer. Il est possible aussi de se dire que la résilience et la confidentialité passent davantage par les systèmes d'informations posés sur ces réseaux de

transport, ou que ces réseaux de transports soient redondés, voire triplés, voire que sur telle ou telle portion on utilise à la fois du câble et du satellitaire, ou parfois des moyens radios de tel ou tel ministère... Cette réflexion nous conduit à penser que, plutôt que de procéder par cloisonnement et de déployer des réseaux dédiés, il conviendrait de multiplier les capacités, ce qui rejoint ce que nous avons pu évoquer à propos des câbles sous-marins.

M. Franck Montaugé, président. - La nation qui, la première, accèdera à l'ordinateur quantique, aura très probablement une avance sur les autres, notamment sur le chiffrement et le déchiffrement. L'enjeu est considérable. Où en est la recherche française sur ce sujet ? Les moyens qui y sont consacrés sont-ils suffisants ?

Le livre blanc de 2013 avait fixé des objectifs ambitieux en termes de politique de sécurité des systèmes d'information. Y figuraient notamment des obligations d'audit, de cartographie de systèmes d'informations... Votre secrétariat suit-il le développement de ces dispositifs ? Le fait-il pour l'ensemble des entreprises ou uniquement pour certaines filières considérées prioritaires ? Avez-vous des indicateurs quantitatifs et qualitatifs ? Quel est l'état des lieux ?

M. Rachel Mazuir. - Pouvez-vous évoquer plus précisément les enjeux autour de la proposition de loi visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles ?

M. Julien Barnu, conseiller pour les questions industrielles et numériques. - La recherche en est encore à un stade très amont en matière d'ordinateur quantique. Il pourra effectivement calculer beaucoup plus vite et donc casser les systèmes de chiffrement. En revanche, les travaux - au niveau international, dans les organismes de normalisation, auxquels l'ANSSI participe activement - sont déjà très avancés sur la définition de nouvelles primitives cryptographiques, c'est-à-dire de nouveaux algorithmes de chiffrement qui permettront même de résister à un ordinateur quantique. La question est aujourd'hui de savoir quand s'effectuera cette bascule des primitives cryptographiques actuelles à ces nouvelles primitives, appelées « post-quantiques » ? Contrairement à la position américaine, qui encourage à basculer très vite sur ces nouvelles primitives, l'ANSSI a plutôt un message de prudence, considérant que les primitives actuelles seront encore résistantes pendant un certain temps, même s'il faut parallèlement réfléchir au calendrier de cette bascule. Nous ne sommes donc pas inquiets sur la capacité du chiffrement à résister aux ordinateurs quantiques. La capacité, de la France, à maîtriser la technologie quantique reste, en revanche, un enjeu majeur de souveraineté technologique et industrielle.

Mme Claire Landais. - La loi de programmation militaire de 2013 a bien tiré les enseignements du Livre blanc de 2013, dans lequel figurait l'idée de contraindre certains acteurs stratégiques à prendre des mesures de

protection de leurs systèmes d'informations critiques. Les opérateurs d'importance vitale qui ont, en conséquence, été identifiés, sont des opérateurs publics ou privés dont le fonctionnement est considéré comme essentiel à la vie de la nation. L'ANSSI a été chargée de la rédaction d'une forme de cahier des charges des obligations imposées à ces opérateurs et les a accompagnés dans ce processus. L'approche de l'ANSSI est d'ailleurs très intéressante : parallèlement à l'usage de la contrainte législative et réglementaire, elle a adopté une démarche pédagogique, d'accompagnement des opérateurs - car une mise à niveau de ce type est coûteuse -, via des audits et des inspections, et en répondant aux alertes. Depuis février dernier, s'ajoute aux opérateurs d'importance vitale la catégorie des opérateurs de services essentiels, qui dépasse ce premier cercle, avec davantage de secteurs impliqués, qui se voient imposer certaines obligations. On peut notamment citer le champ de la santé. Nous faisons monter les systèmes d'information de ces opérateurs de services essentiels en compétence et en exigence en termes de sécurité.

M. Rachel Mazuir. - Voyez ce qui s'est passé au Royaume-Uni !

M. Franck Montaugé, président. - La souveraineté peut aussi s'entendre comme prenant en compte l'ensemble des entreprises, au regard de leur productivité, des emplois qu'elles créent, de leur efficacité... sans se restreindre à ces opérateurs d'importance vitale ou de services essentiels. Y a-t-il une politique de sensibilisation de l'ensemble des entreprises sur la sécurité des systèmes d'information ?

Mme Claire Landais. - Les opérateurs d'importance vitale et davantage encore les opérateurs de services essentiels comprennent bien des opérateurs privés.

M. Franck Montaugé, président. - L'Etat se protège-t-il correctement ? Par exemple, quels enseignements tirez-vous de l'attaque de la plateforme Ariane ?

Mme Claire Landais. - Je ne peux pas vous dire qu'on se protège totalement correctement. Le niveau de sécurité est encore assez variable dans la sphère publique. Les investissements sont difficiles à consentir pour des ministères qui, parfois, concentrent leurs moyens sur leurs coeurs de métiers et ont un peu de mal à penser, en tout cas immédiatement, aux enjeux de sécurité. C'est l'enjeu de la revue stratégique de cyber défense, de son suivi et de l'identification d'actions structurantes, de les contraindre à penser en termes de sécurité et à investir dans ce domaine. L'idée de cercles concentriques et d'acteurs pour lesquels toute attaque, exfiltration, compromission de données serait un drame pour la nation, permet de consentir des investissements à un niveau tel qu'on peut être relativement sereins. Mais nous sommes encore en phase de prise de conscience généralisée et de mise en cohérence des investissements.

M. Julien Barnu. - Depuis 2013, la nature de la menace à l'encontre des entreprises a radicalement changé. À l'époque, la plupart des attaques relevaient de l'espionnage, du siphonage discret de données sensibles. L'ANSSI rencontrait alors des difficultés à convaincre les entreprises - qui pouvaient considérer que le risque était davantage couru par l'Etat en raison de la faible sensibilité des données qu'elles hébergeaient - d'investir pour se protéger d'une menace en quelque sorte invisible. Depuis 2015-2016, on est passé à une menace de sabotage, à travers par exemple des « rançongiciels » qui chiffrent l'ensemble des données des entreprises et donc les exposent à des risques de pertes colossales, et même de disparition pour des PME. En conséquence, la perception de la menace cyber a complètement changé. Les entreprises ne s'interrogent plus sur la question de savoir si elles doivent se protéger, mais plutôt quelle est la meilleure façon de le faire.

La réponse de l'État est organisée en cercles concentriques. Pour les opérateurs d'importance vitale, l'ANSSI impose des règles, très précises et très techniques. Elle accompagne également les autres entreprises, mais à travers la production de guides et de recommandations. L'idée est aujourd'hui de faire en sorte qu'elle étende de plus en plus la certification des produits. Historiquement, elle certifiait principalement des solutions spécialisées en cybersécurité, dorénavant elle certifie des solutions de cloud. Demain, nous souhaitons étendre cette certification, en nous appuyant sur le secteur privé et sur des partenaires européens, aux nouvelles solutions numériques, tels que les objets connectés, les solutions virtualisées... L'objectif est de pouvoir classer l'ensemble des solutions numériques en fonction de leur degré de confiance.

M. Franck Montaugé, président. - Comment considérez-vous les normes ISO en la matière ? Disposez-vous d'une évaluation chiffrée au niveau national de ces certifications ?

M. Julien Barnu. - Toutes les règles de sécurité de l'ANSSI sont conformes à ces normes techniques internationales. Nous avons cependant constaté que ce ne sont que des grands principes, une sorte de code de la route de la sécurité informatique désignant ce qui est obligatoire et exigeant de motiver les dérogations. S'agissant des opérateurs d'importance vitale, la démarche consistant à édicter des exigences plus précises, plus techniques, adaptées au secteur car étudiées avec les opérateurs eux-mêmes, nous est apparue plus efficace.

M. Franck Montaugé, président. - Merci de cet exposé très intéressant.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible *en ligne sur le site du Sénat*.

Audition conjointe de MM. Nicolas Mazzuchi, chargé de recherche à la Fondation pour la recherche stratégique, Julien Nocetti, chercheur à l'Institut français des relations internationales et Christian Harbulot, directeur de l'École de guerre économique,
le 23 mai 2019

M. Franck Montaugé, président. - Notre commission d'enquête poursuit ses travaux avec l'audition commune de MM. Nicolas Mazzucchi, chargé de recherche à la Fondation pour la recherche stratégique, Julien Nocetti, chercheur à l'Institut français des relations internationales (IFRI) et Christian Harbulot, directeur de l'École de guerre économique, spécialiste d'intelligence économique.

Cette audition sera diffusée en direct sur le site Internet du Sénat. Elle fera également l'objet d'un compte rendu publié.

Enfin, je rappelle, pour la forme, qu'un faux témoignage devant notre commission d'enquête serait passible des peines prévues aux articles 434-13, 434-14 et 434-15 du code pénal. J'invite chacun d'entre vous à prêter serment de dire toute la vérité, rien que la vérité, levez la main droite et dites : « Je le jure. ».

Conformément à la procédure applicable aux commissions d'enquête, MM. Nicolas Mazucchi, Julien Nocetti et Christian Harbulot prêtent serment.

M. Franck Montaugé, président. - Une partie non négligeable de nos vies se joue désormais dans l'espace numérique. Si cela représente pour nos sociétés et nos économies de réelles opportunités, les défis sont considérables, et se déploient dans le domaine des relations internationales et géostratégiques. Comment la souveraineté numérique a-t-elle émergé peu à peu sur la scène internationale ? Comment influe-t-elle sur les relations internationales ? Induit-elle des stratégies nationales ou multilatérales ? Sont-elles concurrentes ?

Nous avons compris que trois modèles émergent : le modèle américain ultra-libéral, porté et portant ses acteurs privés. Ce modèle est souverain, dominant les secteurs clés, imposant ses normes et ses choix stratégiques qui affectent toute la société.

S'y oppose le modèle chinois, autoritaire, segmentant l'espace numérique pour en avoir un parfait contrôle sur son sol, interdisant aux entreprises étrangères de transférer leurs données électroniques vers leurs sièges nationaux, utilisant les données personnelles de ses citoyens pour asseoir la domination du parti communiste chinois. Ce modèle est-il réellement souverain ? Enfin, un modèle européen, tentant de proposer une alternative à cet antagonisme, et de protéger les droits fondamentaux qui sont son socle.

C'est une forme d'affrontement géostratégique et économique intense que se livrent les protagonistes. M. Harbulot parle même de guerre économique.

M. Nicolas Mazzuchi, chargé de recherche à la Fondation pour la recherche stratégique. - Le cyberespace est le seul espace stratégique artificiel créé de la main de l'homme. Il se compose d'une couche matérielle qui correspond à l'ensemble des appareils, serveurs, routeurs, ordinateurs qui permettent l'interconnexion des machines ; d'une couche logique ou logicielle qui couvre les éléments de communication entre les machines elles-mêmes, autrement dit les protocoles, ou bien entre les humains et les machines, c'est-à-dire les logiciels. Ces deux premières couches forment l'organisation technique du cyberespace et définissent la manière dont les réseaux fonctionnent. La troisième couche, dite sémantique, correspond à l'ensemble des informations qui transitent au travers des deux premières.

Cette segmentation en trois couches justifie une différence d'approches nationales selon la culture du cyberespace que l'on choisit de privilégier. Les pays de l'espace euro-Atlantique, se sont concentrés depuis la fin des années 80 sur l'architecture technique du cyberespace, définie par les deux premières couches. Ils ont négligé l'importance de la couche sémantique qui a fait un retour fracassant, avec l'invasion de la Crimée par la Russie, puis les élections américaines. D'autres pays ont développé une vision différente, comme les Russes qui ont parié sur la couche sémantique au point de parler d' « espace informationnel » pour désigner le cyberespace.

À cette approche par couches correspond une approche par attaques, avec trois types de cyber conflits, le sabotage, l'espionnage et la subversion. La vision américaine est structurée par les infrastructures, avec 90 % des communications dans le cyberespace circulant de manière sous-marine via des câbles, et un recours aux serveurs racines pour faire fonctionner Internet. C'est une vision libérale, avec des segments fixes détenus par le *Department of Defense* sur les serveurs racines, comme le serveur qui appartient au laboratoire de recherche de l'armée américaine, ou le serveur propriété de la NASA. L'État américain exerce ainsi un contrôle matériel très fort, l'action privée s'exerçant surtout sur les couches logicielle et sémantique.

Cette vision euro-Atlantique correspond à celle des pays du Nord, comme en témoigne l'architecture des câbles sous-marins, élaborée dans les années 90, qui privilégie un axe passant par l'Amérique du Nord et l'Europe pour aller jusqu'au Japon. Les autres pays ne sont pas exclus du système de communication, mais doivent le plus souvent avoir recours aux câbles qui desservent ces trois ensembles géographiques. La vision française et plus largement européenne s'est construite autour de cet arc euro-Atlantique étendu jusqu'au Japon, dont elle a hérité. L'émergence de la Chine est venue remettre en cause cette prégnance des pays du Nord, tout en se heurtant aux réalités techniques.

L'information et les données sont au coeur de la souveraineté du cyberespace, de sorte que la détention des infrastructures offre une capacité stratégique extrêmement forte. La dématérialisation du *cloud computing* s'opère à l'avantage des pays qui sont le plus ancrés dans le cyberespace : pas moins de 40 % des capacités mondiales se trouvent ainsi sur le territoire américain, la porosité extra-territoriale se limitant aux *data centers* que les grandes entreprises américaines comme Microsoft ou Apple déportent dans certains pays européens. La Chine qui arrive en seconde position connaît une croissance d'activité extrêmement forte, de sorte qu'elle tend à remettre en cause la toute-puissance américaine dans le champ du *cloud computing*. Les Chinois ont su mesurer l'importance de stocker des données sur leur territoire.

La capacité pour un État à détenir les données sur son sol, à être souverain en termes de données est au cœur du développement de l'IA.

Entre 2013 et 2018, le nombre de tweets à la minute a quasiment doublé. La création de données, quasi exponentielle, est au cœur de la souveraineté et de la puissance actuelle mais surtout future des États. La grande vogue de l'intelligence artificielle limitée ne peut se comprendre que si l'on prend en compte d'une part, la baisse du coût des capacités de calcul grâce à la performance des processeurs, qui suit peu ou prou la loi de Moore, et d'autre part, la disponibilité en masse de données variées qui a permis de sortir de ce qu'on a appelé les hivers de l'Intelligence artificielle. La puissance d'un État, qu'elle soit actuelle ou en germe, dépend étroitement de sa capacité à édicter une forme de géopolitique des données. L'entreprise est complexe, car les grands textes internationaux qui régissent le cyberespace sont rares, si l'on excepte le règlement international des télécommunications qui date de 1988.

La question financière pèse aussi. Le développement de l'intelligence artificielle attire beaucoup d'investissements, à cause des enjeux stratégiques qu'il porte. Les entreprises américaines et chinoises, dont la proximité avec leur État est encore plus importante que celles des entreprises américaines, sont les plus en pointe dans ce champ, grâce à la capacité qu'elles ont d'injecter des sommes colossales dans la recherche et le développement, mais aussi parce qu'elles ont les moyens d'aller racheter des pépites technologiques sur leur propre sol et à l'étranger. L'intégration transnationale par l'argent peut servir à asseoir la souveraineté d'un État, qu'il s'agisse de rapatrier une entreprise sur son territoire ou de la vider de sa substance, en recrutant ses chercheurs ou en s'appropriant ses brevets. Par rapport à l'évolution du nombre de dépôts de brevets en Chine, la capacité en la matière des pays de l'Union européenne reste extrêmement limitée.

La Chine est venue au cyberespace dans la seconde moitié des années 90, à ses propres conditions. Elle a d'emblée adopté la segmentation du cyberespace en trois couches et a décidé de devenir souveraine sur ces trois couches, tout au moins dans son propre espace national. La Grande

Muraille dorée opère un contrôle des données sur la première couche, sous la forme d'un gigantesque pare-feu permettant à l'État chinois de contrôler, avec une efficacité importante, tout ce qui entre et sort de l'espace informationnel chinois.

Au niveau de la deuxième couche, la population chinoise peut bénéficier des services d'opérateurs nationaux qui offrent en version locale et facilement contrôlable, avec une législation obligeant à stocker les données sur le territoire national, l'équivalent de ce que proposent les opérateurs internationaux. On retrouve ainsi répliqués les grands GAFAM (Google, Apple, Facebook, Amazon, Microsoft), avec, par exemple, Baidu pour Google, Alibaba pour Amazon, ou Sina Weibo comme Twitter local.

Pour ce qui est de la couche sémantique, une armée d'opérateurs sont payés pour effectuer des contrôles destinés à empêcher l'émergence de critiques sur le système politique et social chinois. L'État chinois affiche ainsi sa volonté de garder la mainmise sur toute l'architecture de son cyberespace, permettant à la Chine de s'insérer dans le cyberespace à ses propres conditions.

La France occupe la première place au niveau européen dans le classement des plus grandes entreprises mondiales des technologies de l'information et de la communication. Ce classement reste néanmoins tout relatif, car la capacité européenne à édicter la norme au travers d'un développement très fort de ces technologies reste extrêmement faible. La puissance normative des grandes entreprises américaines, et la croissance forte des grandes entreprises chinoises, les BATX (Baidu, Alibaba, Tencent, Xiaodu), risquent d'affaiblir encore nos capacités.

Quant au modèle russe, il se concentre sur la capacité d'avoir des opérateurs informationnels qui émettent en langue russe, au-delà des frontières russes, dans un espace post-soviétique relativement étendu. Ce modèle fait force de sa faiblesse en se concentrant sur la couche internationale au détriment des deux couches techniques.

La souveraineté numérique reste complémentaire d'autres types de souveraineté dans les stratégies étatiques. Le développement de l'Internet des objets par exemple ne peut se faire sans prendre en compte l'empreinte énergétique extrêmement forte des transitions numériques dans le monde. La Chine l'a parfaitement compris, qui travaille à mettre en place un système extrêmement complexe où une route de la soie électrique est accolée à une route de la soie numérique, les deux fonctionnant de la même manière. Pékin anticipe ainsi l'évolution des réseaux électriques mondiaux appelés à devenir la base des réseaux numériques mondiaux fonctionnant grâce à la 5G fournie par Huawei. La Chine investit aussi énormément dans les batteries qui seront le coeur de la transition énergétique et de la transition numérique.

M. Julien Nocetti, chercheur à l'Institut français des relations internationales (IFRI). - Depuis les derniers travaux du Sénat sur la

souveraineté numérique, en 2014, les paramètres ont évolué. Il y a cinq ans, le contexte était marqué par l'affaire Snowden et la fin de l'innocence en matière numérique. Nous découvrions alors que la souveraineté numérique n'était pas l'apanage des régimes autoritaires. Cinq ans plus tard, nous connaissons tous l'ambiguïté de la technologie, qu'il s'agisse de la prolifération des cyber menaces, de l'accroissement des vulnérabilités liées au numérique, ou de l'extension de cette matière dans les technologies de rupture comme l'IA et la 5G. Dans tous ces domaines, des logiques de souveraineté sont à l'œuvre, qui peuvent favoriser des tensions entre les États à cause d'enjeux économiques forts. La complexité technologique d'Internet va de pair avec l'exacerbation des luttes de pouvoir à l'échelle globale.

L'actualité immédiate est riche d'enseignements. À analyser les tensions entre la Chine et les États-Unis autour de Huawei, la technologie semble être un prétexte assez commode pour justifier le repli des États sur eux-mêmes. En 2010, Hillary Clinton, alors secrétaire d'État, promettait d'abattre le rideau de fer numérique, en référence au vaste système de censure en ligne chinois qui était déployé. En 2019, il n'est plus question de censure, mais d'un décret présidentiel et de guerre technologique. En décidant de bannir le géant chinois Huawei du sol américain et en intimant aux plus puissantes des plateformes américaines de cesser toute relation d'affaires avec la firme chinoise, le président Trump a conféré aux États-Unis des pouvoirs exorbitants sur toutes les chaînes de valeur technologique de la planète.

C'est un changement crucial de stratégie. L'affaire Huawei montre de manière frappante le repli américain sur le plan technologique. Elle tranche avec la doctrine historique des États-Unis en matière numérique et révèle la crainte de Washington de perdre sa supériorité technologique face à Pékin.

Depuis deux décennies, Washington avait fait du contrôle des données l'axe prioritaire de sa stratégie économique et de sa stratégie de sécurité. Les Américains s'appuyaient pour cela sur les géants de la tech, les fameux GAFAM, et sur les pouvoirs très importants confiés à la National security agency (NSA) en matière de surveillance. Ces deux éléments se conjuguaient dans une longue tradition d'open policy qui visait à l'ouverture du marché et au maintien d'une prééminence américaine à la fois militaire et économique, les deux dimensions étant inséparables. Cette politique qui était celle de Barack Obama entre 2008 et 2016 est plus ou moins remise en cause par Donald Trump.

L'affaire Huawei est typique de la stratégie qui consiste à affaiblir son adversaire en tissant avec lui des liens d'interdépendance. C'est un cas typique de militarisation de l'interdépencance. Cette interdépendance technologique et numérique entre la Chine et les États-Unis avait été largement sous-estimée, avec les conséquences que l'on constate désormais.

L'industrie des semi-conducteurs, par exemple, pour le moins confidentielle et très technique, mais aussi très mondialisée, est devenue l'otage des tensions sino-américaines, avec le risque de déstabiliser la quasi-totalité des chaînes de valeur à l'échelle mondiale. Cela pose une lumière crue sur l'absence totale de souveraineté européenne en matière de semi-conducteurs.

Il y a quelques années, les services de renseignement américains s'étaient alarmés des velléités de Huawei de construire des câbles sous-marins, craignant que les Américains ne perdent leur prééminence en matière de renseignement d'origine électromagnétique. Les points d'atterrage et d'interconnexion des câbles sont un enjeu stratégique, qui permettent aux États de conduire des opérations d'espionnage, de piratage et d'intimidation. Certains pays, tels que la Russie, ne se privent pas d'exploiter la dimension physique d'Internet sous un angle stratégique. C'est un enjeu de souveraineté majeur pour l'Union européenne.

Les tensions entre Pékin et Washington autour de Huawei illustrent en accéléré toutes les logiques de fragmentation dans l'univers numérique que l'on constate depuis une dizaine d'années. Nous assistons à la fin de l'ère de la global tech, caractérisée aujourd'hui par un vif rejet du multilatéralisme et par la croyance en l'effacement des frontières, et en l'avènement d'acteurs économiques internationaux qui s'affranchissent des États au profit d'une logique de blocs. Tout ceci est remplacé par un protectionnisme exacerbé.

L'affrontement numérique entre les États-Unis et la Chine a pour objet le leadership technologique, avec l'Europe pour théâtre principal, et au-delà l'Afrique et l'Asie du Sud-Est. C'est sur le vieux continent que Huawei tire l'essentiel de sa croissance, notamment en 2018. L'Europe constitue le principal marché de la firme après la Chine depuis 2013. Cela symbolise la nouvelle orientation économique chinoise. Les dirigeants chinois privilégient une démarche qualitative plutôt que quantitative. Plutôt que d'être l'atelier du monde, la Chine veut montrer qu'elle est le bureau d'ingénierie de la planète, rivalisant ainsi avec les États-Unis.

Les Américains cherchent à contrer ces ambitions chinoises qui les inquiètent en conservant l'Europe dans leur giron numérique. L'ambition de Trump est d'aboutir à un découplage entre le client et la Chine. Du côté européen, l'oukase de Donald Trump risque de créer un précédent, puisque l'Europe réalise que l'avenir de ses propres fleurons industriels tient à l'humeur du président américain. Celui-ci joue sur une ligne de crête, en adoptant une stratégie extrêmement risquée. Il donne paradoxalement aux Européens l'opportunité d'affronter leur propre vulnérabilité. Le politique devrait s'en saisir.

L'Europe avance sur de multiples fronts numériques. Le règlement général sur la protection des données (RGPD) adopté en mai dernier ouvre une troisième voie, comme vous le rappeliez Monsieur le Président, entre les modèles californien et chinois. Cependant, Bruxelles continue d'agir de

manière défensive en s'instituant comme le gardien des valeurs. Dans le même temps, nos concurrents collectent des milliards de données sans se soucier des paramètres qui nous sont chers en Europe. La question se pose, face à cette réalité de savoir si l'Europe peut fonder sa politique sur la seule morale.

L'affirmation européenne en matière de maîtrise des données ne doit pas occulter les contre-réactions inévitables : juste avant l'adoption du RGPD, les Américains ont voté le Cloud Act qui permet aux autorités américaines d'exiger des opérateurs numériques qu'ils livrent les opérations personnelles de leurs utilisateurs sans les en informer, ni devoir passer par les tribunaux, même lorsque ces données ne sont pas stockées sur le territoire américain.

Quant à la Chine, son projet des nouvelles routes de la soie a pour ambition de maîtriser la totalité des infrastructures numériques du territoire chinois jusqu'à l'Europe, en passant par l'Afrique, à la fois en matière de cloud, de data centers, de câbles sous-marins et de réseaux 5G. Rappelons que Huawei a construit plus de 70 % du réseau 4G en Afrique.

Enfin, on ne peut pas dissocier le numérique du financement de l'innovation et de la formation du capital humain. C'est en évitant la fuite des cerveaux et en formant massivement ses propres experts que l'Europe pourra surmonter ses vulnérabilités.

M. Christian Harbulot, directeur de l'École de guerre économique, spécialiste d'intelligence économique. - La notion de guerre économique explique la manière dont les pays s'affrontent depuis la nuit des temps pour accroître leur puissance grâce à l'économie. L'économie n'est pas seulement liée à la créativité humaine et aux échanges, mais aussi aux affrontements qui ne sont pas que concurrentiels. Pour comprendre la notion d'intelligence économique, je vais vous proposer d'explorer certains mots clés. Le premier est celui de suprématie.

Le monde immatériel, ou cyberespace, est un monde à conquérir, au même titre que le monde matériel l'a été, avec des siècles d'affrontements pour la suprématie. Pourquoi le monde immatériel échapperait-il à ces luttes ?

La recherche de la suprématie découle d'un premier principe : quand les États-Unis créent l'architecture du cyberespace, ce n'est pas seulement pour prolonger leur communication dans un contexte de guerre froide, mais c'est aussi pour occuper les meilleures positions dans ce monde en devenir qui ne cesse de prendre forme. Aussi inavouable soit-il, préserver sa suprématie est un enjeu stratégique évident, et la dépendance technologique en est la conséquence et l'arme.

S'est-on déjà posé la question de la suprématie en France ? Le général de Gaulle, de retour aux affaires en 1958, avait compris que l'informatique allait devenir un enjeu majeur dans le développement de

l'économie française. Il avait même, à en croire les écrits d'Alain Peyrefitte, développé une vision de la souveraineté numérique qui dépassait même le cadre de la souveraineté, puisqu'il souhaitait que les entreprises françaises conquièrent des marchés. Malheureusement les plans du président de la République n'ont pas reçu le soutien du monde de l'entreprise, resté focalisé sur les notions de marché propres à l'époque. Il s'agit là d'un dysfonctionnement classique dans le système français, où s'opposent d'un côté une vision politique, et de l'autre un écosystème pas forcément en phase avec cette vision.

Ce dysfonctionnement a laissé des traces, puisque lorsqu'ont émergé l'Internet et la puissance technologique américaine, ainsi que le marché qui en découlait, la plupart des chefs d'entreprise français ont accepté très vite la notion de dépendance, en se disant qu'il était déjà trop tard. Cela a eu et a des implications dans le domaine de l'intelligence économique.

L'intelligence économique examine en quoi l'information peut être utile en termes de développement et de compétition. On constate qu'en France, dès lors qu'une très grosse entreprise de technologie expose à la Porte de Versailles, pas moins de 2 000 entreprises se déplacent ; un syndicat d'entreprises françaises qui tente de faire de l'innovation n'arriverait pas à en réunir 100. La différence est significative. Elle montre la difficulté qu'ont les entreprises françaises à s'emparer du concept de souveraineté, à lui accorder le poids qu'il mérite et à prendre en compte les dynamiques de puissance.

J'ai participé, il y a quelques années, à un colloque de responsables des systèmes d'information. Au lendemain de l'affaire Snowden, des comités exécutifs ont fait machine arrière sur des décisions d'externalisation qui avaient été prises en fonction de critères de marché et de rentabilité. Il suffisait qu'une affaire éclate, mettant en cause les décisions prises montrant que les problématiques de puissance avaient été occultées pour mettre en péril la notoriété du chef d'entreprise. Le problème n'est pas évident. Il n'y a pas sur une question aussi importante d'harmonie de pensée qui prévaut en France entre le monde politique et celui de l'entreprise.

La première urgence face à ce phénomène consisterait à mettre le monde des entreprises devant ses responsabilités. Lors d'une rencontre organisée par le Medef sur la souveraineté numérique, j'ai été très étonné d'entendre les chefs d'entreprise déclarer qu'ils attendaient la feuille de route du politique. On n'aurait jamais entendu telle réaction aux États-Unis. Les entreprises françaises souffrent d'un refus d'entrer dans le paysage des rapports de force entre puissances. D'où le désarroi actuel. Ainsi, le système de cloud français a échoué parce que les groupes français ne se sont pas mis d'accord pour travailler selon une logique d'intérêt national, voire européen.

Mettre le monde de l'entreprise français devant ses responsabilités, c'est le conduire à réfléchir sur le devenir de notre pays dans le monde du cyberespace et son action. Conquérir ce fameux monde immatériel c'est

conquérir des parts de marché. Nous ne pouvons pas nous contenter de petits segments. Nous avons une très forte valeur ajoutée en génie logiciel. C'est un problème vital que de savoir l'exploiter à la hauteur de nos ambitions.

La deuxième urgence se situe au niveau européen, car l'Europe est dépendante du monde américain. La stratégie doit-elle consister à ouvrir la porte aux Chinois pour jouer sur les tensions sino-américaines, au risque de créer une double dépendance ? Lorsqu'il était à la tête de la petite structure d'intelligence économique au Secrétariat général à la Défense (SGDN), Alain Juillet disait que nous gagnerions déjà à récupérer les petites marges de manœuvre qui nous restent. On ne peut rester sur un constat aussi modeste, dès lors qu'il y a tout un monde à conquérir. Le dialogue est encore possible dans le cadre européen. À Milan, il y a deux mois, des chefs d'entreprise constataient les nombreuses contradictions qui les opposaient en matière d'intelligence économique. En revanche, ils étaient d'accord sur la nécessité d'instaurer un dialogue entre eux sur la question de l'économie numérique, pour éviter d'instaurer une dépendance qu'elle soit double aux conséquences néfastes en termes industriels et en termes de tassement économique.

Il y a des marges de manœuvre dans le dialogue au niveau européen sur ce sujet stratégique. Les Allemands eux-mêmes en ont pris conscience face à l'agressivité de M. Trump.

J'en reviens à l'essence du monde économique. La troisième urgence est la prise en considération de l'enjeu majeur de l'organisation du commerce des données. Quand nous mettrons-nous en ordre de bataille pour conquérir des marchés de données ? J'ai fourni dans un document écrit un exemple très précis de ce que j'appelle un encerclement cognitif classique venant de la puissance qui a la suprématie, c'est-à-dire les États-Unis d'Amérique. Ils prennent nos données et en font du business. Leur présence dans notre propre système de sécurisation des technologies bancaires est trop forte. Ils nous disent : « Prenez nos technologies pour lutter contre les économies criminelles et le terrorisme ! » mais ainsi, nous perdons nos données.

Le RGPD ne suffit pas. On ne peut pas en rester à un simple problème moral. Nous devons élever la barre au niveau stratégique. Le commerce des données est une piste très intéressante pour créer des activités et des emplois.

M. Franck Montaugé, président. - Merci.

M. Gérard Longuet, rapporteur. - Le sujet de la nationalité des entreprises est délicat. Les entreprises françaises n'ont pas d'autre nationalité que celle de leurs clients et de leurs actionnaires, qui sont de moins en moins français ou que s'ils le sont ont les mêmes attentes que les non français. De plus, le marché national est significatif mais pas décisif.

Dans le secteur des télécommunications, il y a quarante ans aux États-Unis, comme dans les années 1950 dans le secteur pétrolier, des

politiques visant à casser des monopoles ont été menées. AT&T a été cassé et divisé en une dizaine de sociétés distinctes, comme Standard Oil auparavant. Cette perspective est-elle envisageable ? Ou à l'inverse, le marché étant mondial, les États-Unis ont conscience qu'une entreprise n'est importante que si elle est mondiale, et si elle est première, comme le dit l'expression, le gagnant qui prend tout ?

L'aspect matériel des réseaux constitue-t-il un point de faiblesse ou bien cela pourrait-il être finalement la porte d'entrée vers une régulation stratégique mondiale ?

Mme Catherine Morin-Desailly. - J'ai été très intéressée par la carte des infrastructures dans le monde présentée par M. Mazzucchi. Pourriez-vous en dire plus sur les organismes de régulation d'Internet, qui sont américains : Internet engineering task force (IETF), Internet corporation for assigned names and numbers (Icann) et World wide web consortium (W3C) ? Que pensez-vous du retrait d'Orange de W3C ? N'est-ce pas un renoncement en matière de souveraineté ?

M. Nocetti explique que les choses ont évolué depuis 2014. Mais déjà à cette date, en constatant que l'Europe était déficitaire dans ce nouveau système. Les services over the top (OTT) sont aux États-Unis, les équipements en Chine... L'Europe faillit par son déficit de volonté d'une politique industrielle, même si le RGPD a été une immense avancée. L'absence de volonté est peut-être liée aux conditions structurelles de l'Union européenne. En effet, les règles de la concurrence sont tout à fait à notre désavantage. Il y a aussi une absence de schéma de croissance ou d'investissement massif dans certains secteurs clés tels que l'énergie, l'environnement, la santé. L'offensive ne passerait-elle pas par un changement de ces règles ? A contrario, ne faut-il pas démanteler les GAFAM qui défient l'Europe mais aussi les États-Unis et en fait plus généralement les États-nation ce qui pose des questions en termes de souveraineté.

M. Rachel Mazuir. - Les États-Unis, l'Australie et la Nouvelle-Zélande ont interdit l'intervention de Huawei pour le déploiement de la 5G. Le Royaume-Uni, au contraire, a contractualisé avec cette entreprise. Que penser de cette situation ?

On entend des avis divergents sur la propriété des données personnelles. Certains sont favorables à leur monétisation et d'autres disent que ce serait subir une dépendance supplémentaire. Quelle est votre analyse en la matière ? Enfin, la France peut-elle encore prendre une place industrielle dans cette compétition, comme l'a fait la Chine ?

M. Nicolas Mazzucchi. - Standard Oil a été démantelé par le Sherman Act de 1890, ce qui n'a pas empêché les compagnies pétrolières américaines de s'entendre en 1928 dans l'accord d'Achnacarry pour se partager à nouveau le monde. Quand il y a une nécessité de s'entendre, il y a

toujours des capacités. Les entreprises américaines des télécommunications et du numérique sont tout à fait capable de s'entendre entre elles. Je rappelle qu'AT&T est peu présente hors du territoire américain contrairement à Orange qui a une stratégie d'expansion internationale.

Nous constatons aujourd'hui des dissensions entre les GAFAM et l'État américain, qui les a beaucoup soutenus, notamment Google, car ils étaient un élément de puissance. Il y a une opposition très nette entre les chercheurs de Google et la *Defense advanced research projects agency* (Darpa). Ils sont en concurrence pour attirer les meilleurs ingénieurs et Google refuse de continuer à collaborer avec la Darpa et le Department of defense américain. L'actuelle remise en cause du modèle américain de coopération entre le public et le privé n'apparaît pas dans le modèle chinois où il y a concordance parfaite des intérêts publics et privés.

La géopolitique du cyberespace est double. D'une part, la localisation d'un serveur décide du droit dont il ressort. Ainsi, la Russie contraint les données russes à être sur le territoire russe et exclut des entreprises - Linkedin n'a pas droit de cité. Les éléments matériels sont les seuls à partir desquels faire appliquer le droit. D'autre part, les éléments immatériels relèvent de la norme. La puissance américaine est fondée sur ces deux aspects. La grande force des États-Unis est d'avoir la main sur l'ensemble des organismes, qui sont de gestion privée. Icann est une société de droit californien : l'entité qui gère l'architecture d'Internet, soit une partie du cyberespace, est privée. C'est ce qui empêche aujourd'hui une véritable régulation internationale par les acteurs étatiques.

En décembre 2012, lors de la réunion de l'Union internationale des télécoms (UIT) à Dubaï destinée à faire évoluer la régulation internationale de l'Internet, la question de laisser la gestion à Icann ou de la transférer à l'UIT, donc aux Nations unies, a été posée. Tous les pays du Nord, dont la France, ont refusé ce transfert auquel tous les pays du Sud étaient favorables. Nous avons raté le coche.

Il est intéressant aujourd'hui de relever la présence des acteurs chinois dans la normalisation de l'intelligence artificielle. Ils trustent les postes de présidents ou secrétaires généraux de groupes de recherche et de réflexion, au sein de *l'Institute of Electrical and Electronics Engineers* (IEEE), de *l'International Society of Automation* (ISA) et de *l'International Organization for Standardization* (ISO), car aujourd'hui dans le monde numérique, c'est la technologie qui dicte la norme et donc la puissance.

Ce serait une erreur de monétiser la propriété des données personnelles. Elles ne sont pas du pétrole. Une donnée, c'est une rencontre entre un acteur et une plateforme. Si l'on entrait dans une relation économique avec un acteur de gestion des données, nous perdrions le droit d'exercer un certain nombre de garde-fous. La donnée seule ne vaut rien. Elle ne vaut que parce qu'elle est agrégée à d'autres données, dans des

volumes extrêmement importants. La monétisation ne ferait qu'entrer l'utilisateur dans une dépendance bien plus grande.

J'en viens à la 5G au Royaume-Uni, dont l'impact politique est extrêmement important. Il faut bien comprendre l'ensemble de la dépendance de l'économie britannique à la Chine, y compris dans le domaine énergétique. Ces deux économies sont très imbriquées. Cette présence chinoise très forte oblige le Royaume-Uni à tenir compte de la Chine. Cela fragmente le bloc euro-atlantique, y compris sur des questions de renseignement.

Quant au retrait d'Orange, la politique de la chaise vide est toujours une erreur.

M. Christian Harbulot. - Le problème n'est plus la nationalité des entreprises. Une entreprise américaine est une entreprise qui sert les intérêts américains. Idem pour la Chine, la Russie, la Turquie, l'Iran. En 2019, il est temps de comprendre pourquoi un petit État comme Israël, qui subit une hémorragie constante de ses start-ups, a pris la décision de mener une politique de puissance pour créer de la dépendance dans la dépendance, sur des logiques technologiques. Ne reproduisons pas les mêmes erreurs. Une politique de puissance n'est pas l'addition des nationalités inscrites sur les cartes d'identité des actionnaires.

M. Julien Nocetti. - Nous percevons souvent les États-Unis comme une scène numérique monolithique. C'est loin d'être le cas. Les relations entre M. Trump et les GAFAM sont mauvaises. On a vu des passes d'armes entre M. Trump et Google sur Twitter. Le président américain a ainsi rappelé à Google de ne pas collaborer avec des laboratoires d'intelligence artificielle chinois ; il considère aussi que Facebook est à la solde du parti démocrate. La candidate à l'investiture démocrate Elizabeth Warren plaide pour une plus grande régulation des GAFAM. Elle appuie son argumentaire sur le respect des règles anti-concurrentielles. Le milieu des think tanks universitaires américains joue aussi un rôle moteur dans le débat.

Je souhaite nuancer les propos de Nicolas Mazzucchi sur les alliances. Elles ont été à géométrie variables. L'Inde, acteur majeur du numérique, avait rejoint le camp occidental en 2012 lors de la réunion de l'UIT à Dubaï en 2012 et s'est opposé au document final de la conférence du NETmundial à Sao Paulo en 2014. Autre exemple, la Biélorussie ne s'est pas rallié à la Russie au cours de ces années.

Très peu de choses ont changé dans les grandes instances techniques. Icann est revenu au *statu quo* et à la gestion par la technique du nommage et de l'adressage. Ce n'est pas du tout le guichet unique de la gouvernance mondiale. Le centre de gravité numérique de la planète se déplace inexorablement vers des instances plus politiques et vers la Chine, qui cherche à dupliquer cette gouvernance internationale numérique en sa

faveur. Chaque année se tient en Chine une réunion de grands acteurs nationaux et internationaux du Net autour du président chinois.

Il faut rappeler la très forte porosité du Royaume-Uni aux équipements de Huawei, qui ne date pas d'aujourd'hui. Nombre d'anciens du renseignement britannique collaborent avec cette entreprise. C'est extrêmement dommageable. L'exemple britannique n'est pas forcément à suivre.

Pour revenir à l'aspect normatif, nous mentionnions des instances telles qu'ISO : sachez que son représentant français travaille chez Microsoft. Il y a une porosité entre public et privé qui ne joue pas forcément en faveur du pays.

M. Jérôme Bascher. - Monsieur Harbulot, vous faites une distinction entre souveraineté et puissance. Si l'on peut comprendre que la souveraineté numérique telle qu'elle nous intéresse semble à ce jour hors de portée, comment envisagez-vous que la France et l'Europe puissent redevenir une puissance numérique ?

M. Christian Harbulot. - En France, le pétrole a, pendant plusieurs décennies, été un problème stratégique auquel les gouvernements n'ont pas su trouver de réponse. À l'époque du retour du général de Gaulle, la France était complètement dépendante des sept grandes compagnies pétrolières anglo-saxonnes. C'est alors qu'Elf-Aquitaine a été créé.

Il existe deux façons de reprendre les choses en main. La première est de rattraper le temps perdu en copiant ce que d'autres ont fait. Nous avons démontré dans le passé que c'était possible en ciblant bien les domaines où l'on pouvait exister réellement, par exemple en reprenant la technologie américaine sur le nucléaire. La seconde est de mener la stratégie du grain de sable, que l'Union européenne sait très bien faire, en grippant les mécanismes. Voyons comment, sur des éléments très précis de notre savoir-faire industriel et technologique, nous pouvons nous repositionner et soyons très présents à l'échelle européenne pour devenir ce grain de sable face à deux blocs très solides.

M. Julien Nocetti. - Je note un changement sémantique significatif : on parle bien moins de souveraineté numérique et bien plus d'autonomie stratégique. Encore faut-il assurer une présence française suffisamment importante pour que la vision française soit représentée.

M. Nicolas Mazzucchi. - Nous devons disposer de *hedge funding*. Nous avons un problème structurel car nous sommes capables de financer l'innovation au premier stade mais pas d'aider les entreprises à croître. C'est le *hedge funding* qui a permis aux grandes entreprises chinoises et américaines d'exister.

Nous avons, avec l'Agence nationale de la sécurité des systèmes d'information (Anssi), l'une des meilleures agences de certification au

monde, dont il faut renforcer les capacités à refuser les produits qui ne nous conviennent pas.

Troisièmement, il faut instaurer une préférence européenne pour certaines applications critiques - à condition que les produits répondent à des exigences fortes de performance.

Mme Catherine Morin-Desailly. - Que pensez-vous du fait qu'Orange renonce à participer à l'élaboration des standards et des protocoles ? L'Internet des objets est aussi un défi : les objets connectés vont se multiplier et incorporer toujours plus de données.

M. Nicolas Mazzucchi. - C'est un énorme sujet : c'est même le Far West du numérique. Il y a actuellement un foisonnement de technologies et de protocoles qui ne sont pas harmonisés les uns avec les autres. La sécurité de l'Internet des objets est un problème majeur, car la sécurité est la couche qui a été ajoutée en dernier sur ces objets, ce qui fait qu'ils sont, pour la plupart, très poreux et dangereux. Les éoliennes, notamment, sont extrêmement vulnérables. La confidentialité des données pose problème, car l'éthique by design n'a pas été configurée, et les protocoles de communication sont en concurrence les uns avec les autres. En fait, celui qui remporte le marché est le mieux disant sur le plus grand volume d'objets avec le prix le plus bas - c'est-à-dire, pour la 5 G, Huawei, qui propose un équilibre optimal entre distance de communication et volume de transfert de données, qui est le point de bascule pour l'adoption des différents protocoles.

M. Franck Montaugé, président. - La relocalisation physique des données sur le continent, en Europe, est-ce important ?

M. Julien Nocetti. - J'ai beaucoup travaillé sur ce que font les Russes en la matière. C'est un bon exemple de ce qu'il ne faut pas faire. Les Russes nationalisent le système de nommage et d'adressage - le DNS - tout en essayant de rediriger le routage vers leur territoire, en coupant les ponts avec l'étranger. Pour autant, la Russie n'est pas souveraine comme la Chine, qui a très tôt « souverainisé » son propre espace numérique. Elle dépend très largement de serveurs basés à l'étranger et d'infrastructures liées à d'autres pays. Elle cherche à mettre un terme à cette situation. Pour un pays qui s'étend sur onze fuseaux horaires, c'est peu réaliste. En Europe, l'échelle géographique est plus réduite, mais il y a des polémiques sur l'exploitation des données relocalisées. Les acteurs privés américains insistent sur le risque en termes de libertés publiques.

M. Franck Montaugé, président. - Cela peut les garantir.

M. Christian Harbulot. - Nous pouvons aussi nous tenir en alerte sur l'évolution des technologies de stockage : là aussi, rien n'est immuable, et il n'est pas impossible que de nouvelles technologies nous permettent de reprendre la main sur le sujet. L'essentiel est de développer une stratégie de puissance. Si nous avons deux chercheurs isolés, très bons, qui font des

découvertes sur une nouvelle forme de stockage, et que nous les laissons partir aux États-Unis, il ne faudra pas venir pleurer ! Il faut une vision stratégique décidée au plus haut niveau de l'État, comme c'est le cas ailleurs.

M. Franck Montaugé, président. - Merci.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible *en ligne sur le site du Sénat*.

Audition de M. Benoît Thieulin, ancien président du Conseil national du numérique, rapporteur de l'avis « Pour une politique de souveraineté européenne du numérique » adopté au Conseil économique, social et environnemental,
le 23 mai 2019

M. Franck Montaugé, président. - Cette audition sera diffusée en direct sur le site Internet du Sénat. Elle fera également l'objet d'un compte rendu publié. Je rappelle, pour la forme, qu'un faux témoignage devant notre commission d'enquête serait passible des peines prévues aux articles 434-13, 434-14 et 434-15 du code pénal. Je vous invite à prêter serment de dire toute la vérité, rien que la vérité ; levez la main droite et dites : « Je le jure. ».

Conformément à la procédure applicable aux commissions d'enquête, M. Benoît Thieulin prête serment.

M. Franck Montaugé, président. - Président du Conseil national du numérique de 2013 à 2016, vous avez contribué à asseoir cet organisme consultatif dans le paysage institutionnel français, et à inspirer la loi pour une République numérique de 2016. Vous êtes désormais membre du Conseil économique, social et environnemental, où vous avez été rapporteur d'un avis adopté le 13 mars dernier et intitulé « Pour une politique de souveraineté européenne du numérique ».

Nous réfléchissons à la souveraineté et à son exercice, plutôt dans le cadre national qu'avec une dimension européenne mais nous sommes heureux d'élargir avec vous notre approche. Dans votre avis, vous soulignez la dépendance économique de l'Union européenne vis-à-vis des géants américains et chinois de l'internet. Quelles sont les conséquences en termes de souveraineté ? Au-delà de l'économie et de la sécurité informatique, c'est l'État de droit, la démocratie, les droits fondamentaux qui sont menacés.

Quels sont les principaux constats de votre rapport ? Vous proposez notamment un renforcement de la régulation des plateformes en Europe et le soutien à l'émergence d'un écosystème numérique conforme aux principes et aux valeurs européennes.

M. Benoît Thieulin, ancien président du Conseil national du numérique, rapporteur de l'avis « Pour une politique de souveraineté européenne du numérique » adopté au Conseil économique, social et environnemental. - Voilà près de vingt ans que j'ai la chance de travailler dans le numérique, où j'essaie de promouvoir une vision politique, et même géopolitique, en démystifiant la technologie pour déceler les enjeux politiques de plus en plus prégnants, et que la technologie tend à masquer.

Au cours de la première décennie, pour un *geek* passionné de politique comme moi, le but était surtout de trancher la querelle des Anciens et des Modernes de l'époque, c'est-à-dire de faire prendre au sérieux à nos

élites économiques et politiques ce que l'on n'appelait pas encore la transformation numérique du monde. On a d'abord voulu la minimiser, la voir comme l'émergence d'un média de plus, coincé entre la télévision et la presse. Puis, voyant l'ampleur de cette transformation numérique se développer, on a voulu y voir l'émergence d'un secteur économique particulier. C'était l'époque de la première vague des start-up, celle de la bulle des années 2000 et de la résurrection qui a suivi. Cette décennie s'est soldée, disons-le, par notre victoire intellectuelle : cette querelle des Anciens et des Modernes est tranchée, et plus personne ne doute que la transformation numérique du monde est l'un des enjeux les plus considérables auxquels l'humanité doit faire face. Ma conviction profonde est même qu'il faut la placer au même niveau que la transition écologique. C'est un des paradoxes de notre situation historique que d'avoir à repenser à la fois notre rapport à la nature, avec la transition écologique, et à la culture, qui est l'enjeu de la transformation numérique du monde.

La décennie suivante, celle des années 2010, nous l'avons surtout consacrée à faire passer une idée plus subtile. Le numérique était devenu important, c'était acquis. Il fallait désormais le penser, et se doter d'une vraie stratégie, au lieu de le regarder comme une succession d'inventions plus ou moins fortuites, qui nous tomberaient du ciel et que l'on n'aurait qu'à adopter, vu leur importance et l'incroyable rapidité avec laquelle elles se diffusent - bref, au lieu de le regarder bouche bée, comme un acquis sur lequel on ne peut pas peser. Nous avons été plus ou moins efficaces pour faire passer cette idée. Il fallait bien montrer que la révolution numérique n'était pas californienne et que ce n'était pas à la Silicon Valley de penser la manière dont elle devait se structurer.

Au fond, l'informatique est encore récente, elle a tout juste 70 ans, et son évolution n'a pas été linéaire, ni continue. Le mot de disruption est récent, mais il aurait pu s'appliquer dès la fin des années 1960. Internet, en fait, a été la première grande disruption, promue par des ingénieurs jeunes et dotés d'une vision politique des innovations technologiques. Leur choix a été de démocratiser l'informatique en construisant un réseau hyper-égalitaire. C'est ainsi qu'ils inventèrent Internet, sur des crédits militaires américains, certes, mais ils étaient surtout des étudiants et des professeurs. Le réseau distribué hyper-égalitaire ouvert qu'ils inventent sera l'épine dorsale de la révolution numérique que nous vivons aujourd'hui, et dont nous mesurons les conséquences politiques à l'aune des choix d'architecture technique qui, dès ce moment, comportaient des choix politiques. Il ne faut pas voir les technologies comme quelque chose de transcendant mais, au contraire, décoder les lignes de clivage et les enjeux politiques qui s'y cachent et qui sont devenus extrêmement structurants.

J'ai présidé le Conseil national du numérique, qui a produit 17 ou 18 rapports sur des sujets comme la fiscalité du numérique, la neutralité du Net, la loyauté des plateformes, la réforme de l'enseignement supérieur,

l'enseignement du code à l'école, etc. Mes conclusions reposent donc tout autant sur ces rapports que sur le dernier travail que j'ai eu la chance de diriger au Conseil économique, social et environnemental.

Pourquoi parle-t-on de souveraineté numérique, nationale ou européenne ? Prenons quelques exemples. Vous utilisez tous un GPS, je suppose : Waze, Maps, Coyotte... Cet outil vous donne un itinéraire mais, surtout, il vous indique le chemin le plus court en fonction du trafic, mesuré en temps réel. Si vous êtes sur l'autoroute de Normandie et qu'un embouteillage se forme à Mantes-la-Jolie, les GPS vous font prendre la sortie n° 9, continuer pendant dix ou quinze kilomètres, et reprendre l'autoroute. *Quid* s'ils font faire la même chose à 20 000 véhicules ? Tous vont sortir par la même sortie, traverser le même village, dont la route n'a pas été conçue pour un tel flux. Résultat : la route va s'user en quelques semaines, il y aura des accidents d'enfants qui traversent la rue, et la pollution va s'accroître considérablement dans ce petit village. Au final, les gens vont chercher à partir et le prix des logements va s'effondrer. Voilà, en d'autres termes, une politique d'aménagement du territoire maîtrisée par une application sans qu'aucune puissance publique n'intervienne. C'est qu'une infrastructure immatérielle est venue s'ajouter aux infrastructures physiques que sont les réseaux routiers et autoroutiers. Ni Waze, ni Google Maps ni Coyote n'ont jamais investi dans une route, ni décidé d'aucune signalisation routière. Pourtant, ils ont entre leurs mains une partie de la gestion de la mobilité et des flux sur une partie de notre territoire.

Même chose pour un plan local d'urbanisme. Un maire peut organiser son territoire en regroupant les hôtels près des musées et des monuments à visiter, et les résidences là où il y a des parcs - respectant ce qu'a accumulé l'histoire et nos politiques d'aménagement du territoire, décidées collectivement et démocratiquement depuis deux siècles. Et, d'un coup, une plateforme propose de louer des chambres disponibles. Après quelques années, alors que certains quartiers avaient été pensés pour des activités commerciales et d'autres pour du logement résidentiel, on constate un détricotage complet du plan local d'urbanisme - sans la moindre pelleteuse, et sans changement de plan local d'urbanisme. Simplement, les plateformes numériques ajoutent une couche applicative et logicielle sur des infrastructures physiques qui demandent, elles, des dizaines d'années d'investissement - et il suffit d'une couche de logiciels et d'applications qui offrent des services différents vous en modifier profondément l'usage.

On pourrait multiplier de tels exemples à l'envi, dans presque tous les domaines d'activité. La transformation numérique est un phénomène général de transformation de la société, de la politique et de l'économie. Aucun secteur économique n'est totalement épargné. Il y a bien des marchés quelque peu protégés par des barrières réglementaires, comme la santé, l'éducation, la banque ou les assurances. Mais on sent bien les coups de

butoir de la révolution numérique sur tous les secteurs. Cette révolution est engagée et elle ne s'arrêtera pas.

Près de deux millions d'entreprises européennes sont directement dépendantes du numérique, que ce soit pour leur publicité en ligne ou pour leur plateforme de vente. Prenez l'exemple de *Booking.com*, aussi. Son arrivée a correspondu à une vague de profonde démocratisation et de soutien à l'innovation. *Booking.com* a permis tout d'un coup à nombre de petits hôtels qui étaient perdus et avaient du mal à communiquer - bref, qui avaient des problèmes d'accès au marché - d'avoir d'un coup des millions de clients potentiels. Dans un premier temps, ces hôtels ont bénéficié d'un flux continu de clients. Mais dans un second temps, ils sont devenus tellement dépendants de ce flux de clients que la plateforme en vient à capter une part grandissante de la valeur ajoutée qu'ils produisent. Et certaines analyses économiques révèlent une tendance à ce que les comparateurs de prix où les enchères des mots-clés ont comme conséquence d'absorber la valeur ajoutée d'à peu près tous les secteurs économiques, ne laissant aux acteurs économiques juste que ce qu'il faut pour survivre.

En politique, la puissance horizontale de déverrouillage de l'innovation a, dans un premier temps, fait tomber des dictateurs - en tous cas le numérique y a contribué - et aidé M. Obama, ou notre actuel président de la République, à se faire élire. Ces technologies d'organisation très décentralisée permettent en effet de créer un parti politique en partant presque de zéro, de manière extrêmement rapide, de lever de l'argent et de diffuser de l'information à des coûts ridicules et en un temps record. Mais, dans une seconde phase, on a aussi pris conscience que la même technologie a contribué à faire élire le successeur de M. Obama. Et si les activistes du monde entier ont d'abord vu dans Internet un moyen de se renforcer, en rassemblant rapidement des foules nombreuses, on sait aujourd'hui que, sans le numérique, Daech n'aurait pas existé, puisqu'il n'aurait pas pu recruter des jeunes en les manipulant à distance, ni organiser leur flux vers l'État islamique.

Néanmoins, la révolution numérique a été, et est toujours, un moyen incroyable de démocratiser notre société et notre économie et de relancer l'innovation en injectant dans de nombreux secteurs une saine concurrence. Pour les taxis, par exemple, après une phase où la concurrence a fait monter tous les acteurs en gamme, et où l'arrivée des plateformes a créé des emplois, souvent dans des bassins qui en étaient assez éloignés, ce qu'on appelle les travailleurs indépendants sont en réalité placés dans une double subordination.

Il faut également garder à l'esprit la subordination que subissent ces prétendus travailleurs indépendants envers les utilisateurs. L'obséquiosité des chauffeurs de VTC ne vous a-t-elle jamais choqués ?

M. Gérard Longuet, rapporteur. - Certains diraient qu'ils ressemblent à des candidats aux élections...

M. Benoît Thieulin. - Absolument, et pour cause : s'ils ont trop de mauvaises notes, ils sont renvoyés. Rarement une situation économique aura été marquée par une telle dépendance.

Je ne cherche pas à donner une image apocalyptique de la situation : le numérique est une chance pour la démocratie, mais des choix politiques et géopolitiques s'imposent. Il s'agit de savoir quels usages nous voulons, ou non, pour le numérique.

À cet égard, nos préconisations sont de quatre ordres.

Premièrement, il convient de savoir précisément ce qui se passe dans ces boîtes noires que sont les plateformes. Qui sait quels types de produits sont vendus, après la saisie de quels mots-clefs ? Quel produit est favorisé, pour quelles raisons ? Pour se faire une idée de la situation, il faut imaginer Bercy mettant en oeuvre des politiques macroéconomiques sans l'aide de l'Insee, sur la seule base de quelques cas litigieux dont les tribunaux se sont saisis. Avant tout, il est donc indispensable de réarmer la puissance publique, en réunissant des équipes d'ingénieurs au sein d'une agence européenne d'évaluation des plateformes. Les plateformes ne sont pas censées fournir leurs algorithmes, qu'elles adaptent sans cesse et qui relèvent du secret industriel. En revanche, étant donné l'importance qu'elles ont prise dans nos vies, nous devons être en mesure de surveiller leur activité en permanence. Sinon, les États se contenteront demain de gérer des infrastructures physiques qui leur échapperont de plus en plus. Dans dix ou vingt ans, ils seront totalement désarmés.

Mme Catherine Morin-Desailly. - C'est déjà le cas.

M. Benoît Thieulin. - Certes, mais il est encore temps de réagir. Si l'on ne réarme pas la puissance publique, les utilisateurs devront exiger un droit de vote chez Google, Facebook ou Amazon : telle est, à mon sens, l'alternative. Ces plateformes sont très puissantes, mais les Européens représentent un tiers des 1,5 milliard d'individus qui ont recours à elles : et cette clientèle est sans doute celle qui leur rapporte le plus d'argent.

Deuxièmement, il faut assurer une régulation. Avec le RGPD, l'Europe a accompli une très grande avancée. Ce succès prouve que, malgré leurs cris d'orfraie, les plateformes étaient tout à fait prêtes à négocier - elles sont presque embarrassées par le pouvoir qu'elles ont gagné. On sait qu'elles ont pu contribuer à perturber des élections et elles se trouvent, de ce fait, dans une situation délicate. Pour l'heure, on se contente de discuter, avec Mark Zuckerberg ou avec d'autres : c'est nécessaire, mais ce n'est pas suffisant. Au cours des derniers mois, en modifiant son algorithme, Facebook aurait retiré 1 milliard de contenus haineux : ces chiffres sont vertigineux. Mais cette méthode ne peut qu'être transitoire. La puissance publique, démocratiquement élue, doit assumer la régulation le plus vite

possible. Voilà pourquoi le RGPD doit être étendu aux médias et à l'économie.

Troisièmement, nous formulons une recommandation d'ordre stratégique : on ne pense pas suffisamment le numérique en Europe. Après la chute du mur de Berlin, les États-Unis ont réuni de nombreux experts, universitaires, militaires, politiques, pour penser la puissance au XXIe siècle. Les experts ont abouti à cette conclusion : la puissance sera fondée sur les infrastructures immatérielles. La politique poursuivie depuis lors par les Américains se fonde sur ce principe. Des capacités d'investissement hors normes ont été accordées aux grandes entreprises du numérique, lesquelles donnent la priorité à leur effort d'investissement. Désormais, l'Europe doit, elle aussi, faire des choix politiques forts en matière de numérique. Le *Safe Harbor* est un traité inégal, au sens où les Chinois parlaient de « traités inégaux » au XIXe siècle : en 2000, les Américains pensaient déjà le *big data* de 2015 et, de leur côté, les Européens négociaient en contrepartie un peu plus d'exportations de voitures allemandes et de vin français. Voyez, en parallèle, ce qui reste de notre stratégie de Lisbonne. Doit-on continuer de s'abriter sous le parapluie numérique américain ? Bien sûr, il est plus attractif que le parapluie numérique chinois, mais nous sommes bel et bien dans une nouvelle guerre froide, où le numérique joue un grand rôle et qui a, comme la précédente, l'Europe pour principal terrain : ne soyons pas réduits au rang d'otages technologiques.

Quatrièmement, il est grand temps de se doter d'une véritable politique industrielle. Le plan Juncker allait dans la bonne direction, il était d'assez grande ampleur, mais il ne faisait pour ainsi dire pas de choix stratégiques. On peut tout à fait accepter que la raquette numérique ait des trous - encore faut-il, néanmoins, qu'il y ait une raquette ! Je pense, évidemment, au *cloud*. Il y a une dizaine d'années, les acteurs économiques dominants ont capté les subventions accordées à cette technologie, aux dépens d'OVH, et ils ont échoué : aujourd'hui, il faut faire des choix beaucoup plus fléchés. Je pense également à la 5G. Cette infrastructure-clef ne peut pas être soumise aux aléas d'une nouvelle guerre froide, dans un contexte d'évolutions technologiques que nous ne maîtrisons pas. À cet égard, Nokia, Ericsson et Alcatel auraient un rôle à jouer : tant pis si nous perdons deux ou trois ans. Nous voyons aujourd'hui l'importance géopolitique stratégique de Galileo, qui, malgré des débuts difficiles, a été un succès. Je pense, enfin, à l'*operating system*. Le mois dernier, WhatsApp a dû admettre une grave faille de sécurité. En l'occurrence, c'est bien l'*operating system* qui était en cause : il est indispensable de forger un *operating system* européen. Procéder sans cet outil, cela revient à faire la guerre sans chars ni fusils.

M. Gérard Longuet, rapporteur. - Merci de cette communication passionnante, extrêmement claire et illustrée d'exemples parlants.

Selon la formule consacrée, lorsqu'une innovation apparaît dans le secteur numérique, les Américains en font du business, les Chinois la copient et les Européens la régulent. Mais, pour assurer une régulation à l'échelle de l'Union européenne, il n'est pas facile de dégager une majorité. La question cruciale qui se pose ici est de savoir si les États sont à même de pousser leurs citoyens à adopter tel ou tel comportement, par exemple à ignorer telle ou telle plateforme ?

Mme Catherine Morin-Desailly. - À propos des VTC, vous mettez en évidence ce qu'on nomme le « capitalisme de surveillance ». Mais ne s'agit-il pas d'un nouvel esclavagisme ?

Il faut certes une politique industrielle européenne pour le numérique. Toutefois, une agence serait-elle efficace ? Et les plateformes sont-elles réellement pleines de bonne volonté, voire « embarrassées » par leur pouvoir ? Voyez le lobbying qu'il a fallu vaincre pour mettre en oeuvre le RGPD ou la directive sur les droits d'auteur. Quant à Mark Zuckerberg, il savait dès 2014 que les Russes avaient infiltré Facebook, il n'a rien fait et a même menti sur ce sujet. N'est-il pas temps d'entrer dans une ère nouvelle, en instaurant un véritable statut des plateformes, en reprenant le chantier de la directive sur le commerce électronique et en se gardant de tout angélisme ?

Enfin, pouvez-vous préciser ce que vous suggérez pour la régulation, qu'il s'agisse de la concurrence ou des médias ?

M. Hugues Saury. - Vous faites un parallèle entre le changement climatique et la transformation numérique. Les Européens sont, en grande partie, conscients du premier enjeu. Mais mesurent-ils bien l'importance du second ? Et la révolution numérique peut-elle perdurer longtemps sans l'approbation des citoyens ?

M. Franck Montaugé, président. - Quelles limites apporter à la nécessité de connaître les algorithmes, au regard des droits individuels ?

M. Benoît Thieulin. - Monsieur le rapporteur, je suis persuadé que l'on peut réguler les plateformes à l'échelle européenne. Bien sûr, elles sont adoptées, voire adorées, par nombre d'utilisateurs. En outre, elles ont changé tous les pans de la vie des individus, qu'ils le veuillent ou non. Il ne faut pas tuer cette innovation, mais il est indispensable de contrer ses dérives et, à cette fin, nous disposons d'une force de frappe considérable : les plateformes comptent 500 millions d'utilisateurs en Europe, et ces clients sont parmi les principaux au monde. Si nous leur imposons des règles, elles les appliqueront, et elles les étendront même à d'autres régions du globe. Certes, elles ne sont pas là pour mener une action philanthropique, mais elles sentent le vent tourner. Elles sentent même le vent du boulet.

L'activité de Facebook se concentre sur les réseaux sociaux : c'est un pan assez limité de l'activité numérique, et l'entreprise ne semble pas franchement se diversifier. En outre, les plus jeunes utilisateurs ont déjà

basculé vers d'autres plateformes ; pour l'essentiel, les clients de Facebook ont plus de quarante ans. De surcroît, la personnalité publique, quasi politique, qui incarne l'entreprise, Mark Zuckerberg, peut aujourd'hui apparaître comme un handicap, après avoir été un atout. Voilà pourquoi Facebook traverse une zone de turbulences assez fortes ; voilà pourquoi elle a viré sa cuti en se prononçant en faveur du RGPD. À l'évidence, le rapport de force a changé, à défaut de s'inverser. J'ajoute que le travail en faveur de la protection des données personnelles doit être poursuivi dans le domaine de la vente en ligne.

Madame Morin-Desailly, je ne crois pas tomber dans l'angélisme ; peut-être ai-je même brossé un tableau trop sombre, mais, comme vous l'avez vous-même indiqué dans l'un de vos rapports d'information, il faut à tout prix éviter que l'Union européenne ne devienne une « colonie du monde numérique ». Par leur activisme contre la directive sur le droit d'auteur, les plateformes m'ont profondément choqué : elles ont utilisé leur propre force de frappe à des fins de propagande. Il s'agit là d'un véritable problème démocratique.

Je ne crois pas non plus être naïf face à Uber. Cette entreprise, comme beaucoup d'autres, nous met face à de nombreuses questions sociales auxquelles il faudra répondre.

Pour réguler un secteur, il est indispensable de le connaître. L'Autorité des marchés financiers suit au quotidien les variations suspectes du cours des actions. En cas de soupçon, une enquête est immédiatement déclenchée. Désormais, il faut faire de même dans le secteur numérique. On ne peut plus se contenter de réagir après coup, en attendant de constater des dérives et voire de prononcer des sanctions, notamment politiques. Voilà pourquoi il faut une instance d'évaluation.

Je prendrai un autre exemple concret. EDF dispose, ou du moins disposait, d'un monopole naturel. Imaginez que, du jour au lendemain, cette entreprise décide d'abandonner le 220 volts, pour passer à 400. Dans votre usine, qui fonctionne à 220 volts, toutes les machines brûlent ; EDF vous a prévenu par un mail que vous lisez, trop tard pour éviter de faire « griller » votre usine. Or, de l'autre côté de la rue, vous voyez s'installer une nouvelle société, qui propose les mêmes produits que vous et qui, elle, dispose de machines fonctionnant à 400 volts. Cette situation paraît invraisemblable, mais c'est ce qui se passe en permanence dans le secteur du numérique : les plateformes, qui sont en situation de quasi-monopole naturel, disposent d'un droit de vie et de mort sur tout un ensemble d'acteurs. Il leur suffit de modifier les API.

Il faut revoir la directive sur le commerce électronique. Il faut réfléchir à un nouveau statut pour les plateformes, en leur imposant un cahier des charges contraignant : aujourd'hui, les règles de droit classiques mises à part, elles assument trop peu de responsabilités.

Monsieur Saury, vous avez entièrement raison : face à l'urgence climatique, la prise de conscience est réelle. Mais l'aveuglement persiste face à la révolution numérique. Je peine souvent à faire comprendre à mes interlocuteurs pourquoi la neutralité d'internet est une notion essentielle. Nous ne sommes pas nés avec internet. Nous sommes, d'une certaine manière, des migrants du numérique : mais, grâce à ce décalage, nous disposons d'un autre regard sur la liberté d'expression.

Nous avons un grand travail de pédagogie à mener au sujet des nouveaux médias. Il faut enseigner le codage dans les écoles, ne serait-ce que pour démystifier la technologie. Ma grand-mère et mon arrière-grand-mère connaissaient des rudiments de mécanique et d'électricité. Aujourd'hui, l'effet « boîte noire » asservit nos concitoyens. Il faut leur permettre de décoder le monde numérique pour éviter des entreprises de manipulation.

Enfin, monsieur le président, les changements algorithmiques peuvent avoir des effets considérables sur notre société. Après l'élection de Donald Trump, Facebook a été attaqué pour avoir permis l'essor de la société Cambridge Analytica. Mark Zuckerberg a décidé que les informations seraient à l'avenir diffusées de manière différente, en favorisant les échanges locaux. Au passage, ce dispositif est sans doute l'un des facteurs de l'émergence des gilets jaunes.

À l'évidence, les changements algorithmiques décidés par les plateformes ont, aujourd'hui, de nombreuses conséquences économiques et sociales. Ce serait une folie de les laisser au bon vouloir des entreprises privées : même avec les meilleures intentions du monde, elles n'ont pas la responsabilité démocratique permettant d'exercer de tels pouvoirs.

M. Franck Montaugé, président. - Nous vous remercions de l'éclairage que vous nous avez apporté.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible en ligne sur le site du Sénat.

Audition de M. Bernard Benhamou, secrétaire général de l'institut de la souveraineté numérique,
le 23 mai 2019

M. Franck Montaugé, président. - Notre commission d'enquête poursuit ses travaux avec l'audition de M. Bernard Benhamou.

Cette audition sera diffusée en direct sur le site internet du Sénat et fera l'objet d'un compte rendu publié.

Enfin, je rappelle pour la forme qu'un faux témoignage devant notre commission d'enquête serait passible des peines prévues aux articles 434-13, 434-14 et 434-15 du code pénal. Je vous invite à prêter serment de dire toute la vérité, rien que la vérité. Levez la main droite et dites : « Je le jure. »

Conformément à la procédure applicable aux commissions d'enquête, M. Bernard Benhamou prête serment.

M. Franck Montaugé, président. - Ancien délégué aux usages de l'internet au ministère de l'enseignement supérieur, de la recherche et de l'innovation, vous êtes aujourd'hui secrétaire général de l'institut de la souveraineté numérique, institution que vous avez contribué à créer ; vous comprenez pourquoi nous vous auditionnons aujourd'hui, d'autant que vous êtes familier des travaux que le Sénat consacre au numérique.

Vous avez participé au sommet des Nations unies pour la gouvernance d'internet. Vous y défendiez alors la position française, et européenne, à propos de l'architecture d'internet. Celle-ci se résumait à trois principes fondamentaux : interopérabilité, ouverture et neutralité. Pouvez-vous nous exposer rapidement les enjeux soulevés par la gouvernance d'internet, que vous avez qualifiée de « nouveau théâtre des conflits internationaux » ?

La France ne semble pas être aujourd'hui en position de force sur ce terrain. Elle peine à imposer ses régulations aux grandes plateformes numériques. Les grands acteurs sont américains et, de plus en plus, chinois. Vous ne croyez pas « au déterminisme dans le numérique ». Vous considérez cependant que nous sommes à un moment-clef et, comme notre interlocuteur précédent, M. Benoît Thieulin, qu'au-delà de la France c'est l'Europe qui doit réagir. Sur la forme que doit prendre cette réaction, au niveau national et européen, nous serions heureux d'entendre vos propositions.

M. Bernard Benhamou, secrétaire général de l'institution de la souveraineté économique. - Vous avez cité les travaux que j'ai pu consacrer aux questions numériques quand j'étais sherpa de l'ambassadeur de France aux Nations unies. Depuis lors, nous sommes toujours face à des rapports de force. Dans le même temps, le paysage numérique a changé, mais pas toujours dans le bon sens.

Nos interlocuteurs du département d'État nous disaient : « L'Europe n'a pas de grands acteurs dans ce domaine. Elle ne sait que geindre. » C'était il y a treize ans. De même, pour Barack Obama, alors président des États-Unis, la France était en fait jalouse des géants américains, qui ont façonné internet.

Notre réponse doit être avant tout industrielle. Si important soit-il, le RGPD est largement insuffisant face aux difficultés actuelles. Nous sommes pris en tenaille entre le laisser-faire américain, qui donne lieu aux pires excès - je pense notamment à l'affaire Cambridge Analytica - et la vision totalitaire, orwellienne, défendue par la Chine, avec le système de notation baptisé « crédit social ». En Chine, l'on en vient à imposer aux personnes mal notées une sonnerie téléphonique particulière : le Conseil d'État chinois a vivement approuvé cette mesure, en relevant qu'elle permettrait d'acculer les individus mal notés à la faillite.

Face à ces questions stratégiques, on constate trop souvent une certaine indécision de la classe politique. Le Président de la République a nommé John Chambers, patron de Cisco, ambassadeur mondial de la French Tech. Or ce n'est pas une nomination symbolique. À preuve, M. Chambers a accompagné le chef de l'État lors de son voyage en Inde. On aurait pu faire un meilleur choix....

Il nous faut établir un diagnostic lucide : au-delà des enjeux industriels, nous sommes face à un risque extrême. Désormais, aucun secteur n'est à l'abri de la numérisation, qu'il s'agisse de l'agriculture, de la culture, de la santé, de l'assurance ou du pouvoir de battre monnaie. On ne peut plus se contenter d'une attitude de déploration atterrée. Ce qui se joue, c'est l'avenir européen dans son ensemble. Certes, comme on a pu le rappeler précédemment lors de vos auditions, l'État n'a pas encore été uberisé, mais les plateformes ne demandent pas mieux !

Le déploiement du numérique n'est pas de même nature que l'électrification ou l'essor de la radio au début du siècle dernier : c'est une transformation intégrale de tous les processus de production.

Aujourd'hui, les plateformes sont des intermédiaires incontournables de la vie quotidienne, des éléments essentiels de la structuration du débat public, et partant de l'opinion publique. D'après les pointages, l'élection de Donald Trump s'est jouée à 0,09 % des grands électeurs, soit quelques dizaines de milliers de personnes. À l'échelle d'un tel pays, les plateformes sont tout à fait en mesure d'exercer une influence de cette ampleur.

À côté des GAFAM, on a laissé grandir des monstres inconnus du grand public : les *data brokers*, dont le métier est de rassembler toujours davantage de données. Or, d'après le *Financial Times*, ces acteurs ne peuvent pas être régulés : ce sont « les étoiles de la mort de la vie privée ». Voilà pourquoi il faut penser la régulation du futur. À mon sens, l'activité de ces

data brokers devra à terme être interdite car, du fait de leur modèle économique, ils ne peuvent pour ainsi dire pas être contrôlés. En l'état actuel des choses, ni Facebook ni personne ne peut dire si les élections européennes qui se profilent seront soumises à telle ou telle influence.

M. Gérard Longuet, rapporteur. - Fondamentalement, l'économie numérique semble marquée par une double perversité.

Premièrement, personne ne paye - du moins apparemment - et l'absence de paiement entraîne des addictions extraordinairement fortes, lesquelles contrebattent les volontés politiques nationales ou européennes. La vente de données semble donc, pour l'heure, inévitable.

Deuxièmement, le financement par les marchés est ambigu. Les investisseurs européens veulent avant tout recevoir des dividendes ; mais, dans le monde anglo-saxon et dans les pays de la zone Pacifique, l'on privilégie la montée en puissance de l'entreprise, l'on garde l'oeil rivé sur les parts de marché, et peu importe si, dans un premier temps, l'on perd de l'argent.

Pour un Français, une entreprise comme Amazon est donc doublement curieuse. D'une part, elle a court-circuité toutes les législations nationales relatives à la distribution commerciale, notamment la loi Royer. D'autre part, elle a longtemps accepté de perdre de l'argent pour déployer son modèle économique.

Mme Catherine Morin-Desailly. - Effectivement, rien n'est gratuit : la publicité suscite des clics, donc des revenus, lesquels ne sont pas imposés, et les GAFA sont toujours plus puissants. Mais ce modèle est-il durable ?

Quelques voix s'élèvent pour appeler au démantèlement des plateformes. Or, à une question d'actualité que je lui soumettais hier, M. Cédric O a apporté une réponse édifiante : selon lui, si l'on démantèle les plateformes, les internautes européens devront se rabattre sur des plateformes russes ou chinoises, aux dépens de leurs libertés. S'agit-il d'un risque réel ?

M. Jérôme Bascher. - Est-ce qu'il n'y a pas urgence aujourd'hui à réguler au niveau européen, par de la norme, qu'elle soit technique ou juridique, alors que nous sommes encore aujourd'hui le premier marché pour ces entreprises du numérique ?

M. Bernard Benhamou. - La gratuité telle qu'elle a été conçue par les grandes plateformes qui dominent aujourd'hui l'internet est une gratuité qui s'accompagne d'un travail phénoménal sur le caractère addictif des services. La gratuité a donc été conçue comme la meilleure manière de créer le plus rapidement possible un auditoire qui soit le plus large et le plus captif possible. Les relations que nous entretenons avec les plateformes sont asymétriques, par exemple en droit : personne ne lit les conditions générales d'utilisation. Le législateur devrait trouver une réponse à cette asymétrie et

créer un socle identique de conditions, pour éviter d'en avoir d'infinies variations. Je vous invite à lire *Le capitalisme de surveillance* de Shoshana Zuboff, professeure à Harvard. Cet ouvrage montre le caractère totalement inhabituel de la manière dont ces sociétés sont conçues. Elle cite l'exemple du travail des enfants. On l'a interdit, on ne s'est pas demandé s'il fallait introduire des exceptions. Ce n'est pas le cas pour certaines pratiques extrêmes de profilage.

Je vais vous citer l'exemple d'ERDF et du compteur Linky. Je leur ai demandé s'ils savaient que leur compteur permettait de faire du profilage ethnique et religieux. Ils n'ont pas su me répondre, ils voyaient leur compteur comme un simple outil technique, pour réguler au mieux le réseau et ils ne se rendaient pas compte que la donnée de consommation était infiniment personnelle et révélatrice. Il y a beaucoup d'exemples de données non-sensibles qui le deviennent puisqu'on peut, par l'intelligence artificielle ou par des algorithmes, en tirer des informations sensibles. Avec la loi de 1978, on a considéré qu'il y avait des données sensibles. Or, on peut maintenant deviner des choses sur sa santé rien qu'en regardant sa consommation ou ses informations sur Facebook. On peut faire une cartographie des maladies par le biais des recherches sur Google. La donnée a été conçue comme une perte raisonnable pour l'utilisateur, ce n'est plus le cas aujourd'hui. Nous sommes à l'aube de la génomique de masse. La loi américaine HR1313, qui voulait obliger tous les employés des entreprises américaines à subir des tests génétiques en entreprise, sous peine d'être pénalisé de 4000 à 5000 dollars par an, a failli passer au Congrès.

Sur la logique du « *winner-takes-it-all* » (la première plateforme arrivée gagne tout), c'est ce qui s'est produit avec Amazon puis Uber. Si l'activité de commerce de détail d'Amazon est plus risquée historiquement, ce n'est pas le cas de d'autres services, comme le *cloud,* très largement bénéficiaires. En éteignant toute forme de concurrence, le pari d'Amazon s'est révélé gagnant, au point que nos distributeurs sont obligés de faire alliance avec Amazon ou Google, par exemple pour être présents sur leurs enceintes connectées.

Sur la durabilité du modèle économique des plateformes, elles ne peuvent exister que si elles ont vocation à s'appliquer à tous les autres secteurs. Les secteurs visés par les GAFAM sont aujourd'hui la monnaie et l'assurance et, pour Apple, la santé. Le but est de reconfigurer ces secteurs, d'utiliser leurs technologies pour proposer des instruments de paiement ; proposer des services financiers (avoir les instruments bancaires pour gérer son budget. Apple s'est allié avec Goldman Sachs pour créer une carte de crédit). Les assureurs n'ont jamais bénéficié d'une manne informationnelle aussi grande que celle dont bénéficient les GAFAM aujourd'hui. On disait, il y a quelques années, que Visa pouvait prévoir quand les gens allaient divorcer. Ces plateformes ont aujourd'hui vocation à étendre leur influence. Google a passé un accord avec la ville de Toronto pour gérer l'un de ses

quartiers (capteurs, nouveaux systèmes de transport). C'est un exemple concret d'*ubérisation* de la fonction politique.

Sur l'antitrust, on peut rappeler un exemple historique, celui de l'Union européenne qui a empêché la fusion de deux sociétés américaines, General Electric et de Honeywell, au début des années 2000. On se rend donc compte que l'Europe n'utilise pas aujourd'hui ses propres instruments. Le rapprochement entre Facebook, Instagram et Whatsapp aurait dû faire l'objet de mesures conservatoires pour pouvoir être examiné par l'Europe. Il n'est pas trop tard aujourd'hui, ceux qui réclament qu'on s'intéresse aux conditions réelles du marché ont tout à fait raison. S'il s'agit, certes, moins d'un risque de prix que par le passé, mais le risque de modifier les conditions de l'innovation et les conditions d'existence des autres sociétés est tout aussi justifiable en termes d'action antitrust.

L'argument russe/chinois a été utilisé récemment pour ne pas sanctionner *Huawei*, y compris par la numéro 2 de Facebook, qui craignait que cela ne donne la main aux grandes sociétés chinoises dans ce domaine. Là-dessus, rien n'est moins sûr. Si les sociétés chinoises ont été particulièrement habiles à se développer dans le domaine du hardware et à s'exporter, les réseaux sociaux chinois, eux, ne s'exportent quasiment pas. Un article récent du *New-York Times* montrait que les *start-upers* chinois, contraints par les perspectives de contrôle politique et social, fuyaient la Chine. Il est plus facile de maintenir un haut niveau d'innovation dans le domaine des *hardwares* et des réseaux que dans celui des logiciels : les contraintes politiques qui pèsent sur cette industrie chinoise pourraient devenir un véritable obstacle à son développement.

M. Rachel Mazuir. - Vous avez dit que certains parlementaires américains avaient demandé le démantèlement de Facebook. Pourquoi Facebook plus particulièrement ?

M. Bernard Benhamou. - Facebook est celui qui a posé le plus de problèmes politiques. Google a mieux réussi à passer sous silence son implication dans la radicalisation (par son moteur de recherche mais aussi par les vidéos de *Youtube*). *Cambridge Analytica* s'appuyait sur le *micro-targeting* via Facebook, mais l'antitrust se pose aussi pour les autres géants du numérique : pour Apple et sa plateforme de distribution, pour Amazon et les clauses léonines qu'elle a parsemé dans ses contrats avec les intermédiaires.

Mme Catherine Morin-Desailly. - Nous débattions récemment au Sénat de la taxation des GAFAM. D'aucuns évoquaient alors l'idée de la marchandisation et de la valorisation financière des données. Qu'en pensez-vous ? Ma deuxième question porte sur le rapport de la mission de régulation des réseaux sociaux remis au début du mois de mai 2019 au Président de la République. Quand on le lit, on peut s'étonner de

« l'angélisme » du rapport, qui prône une auto-régulation, voire une corégulation de ces plateformes. Qu'en pensez-vous ?

M. Bernard Benhamou. - Sur la « patrimonialisation » des données, certains défendent l'idée que les utilisateurs pourraient être rémunérés en échange de leurs données. C'est le prototype de la fausse bonne idée, de l'enfermement des utilisateurs sous la coupe des GAFAM. À partir du moment où vous vous êtes dépossédés de vos données, la plateforme est en droit d'en faire ce qu'elle veut, alors même que le contrôle est aujourd'hui déficient. À long terme, on peut imaginer des choses aberrantes, telles que la génomique. Au lieu de s'autoréguler la plateforme, on va essayer d'en obtenir des miettes. Ce n'est pas la bonne stratégie, il faut se demander si le modèle économique de ces sociétés doit être remis en question. Cet aspect était totalement absent du rapport remis au Président de la République. Ce rapport portait sur les propos de haine, or l'un des vecteurs de dissémination de ces propos, c'est le profilage des individus. Si on ne s'attaque pas au coeur, s'attaquer à la périphérie du sujet sera se condamner à l'impuissance. Ce rapport aurait mérité d'avoir une posture plus offensive que la posture de conciliation à laquelle il a abouti.

M. Franck Montaugé, **président. -** Êtes-vous favorable à une relocalisation des données, à l'échelle nationale ou européenne, avec un contrôle de l'utilisation et de la commercialisation des données ?

M. Bernard Benhamou. - Absolument, à l'échelon européen. L'un des éléments clés de la souveraineté est la territorialité. Les Allemands sont allés plus loin en recommandant que les données des Allemands ne quittent pas le territoire européen. L'Inde s'en est aussi inquiétée, tout comme la Chine, pour d'autres raisons. Est-ce que cela sera suffisant au vu de la volonté d'extraterritorialité du droit américain (ex. *Cloud Act*) ? Cela demeure à voir. Après l'affaire Snowden, à laquelle la France a répondu de manière timide à l'époque, contrairement à l'Allemagne, nous n'avons pas fait suffisamment tôt le bilan des événements et de leurs implications. Nous avons été naïfs.

Nous sommes l'une des premières plateformes mondiales de consommation des biens technologiques mais, pourtant, pour l'essentiel, les compagnies qui en retirent le plus de profits ne sont pas européennes. En découlent des problèmes de taxation, des pratiques d'optimisation et d'évasion fiscale. Si on ne développe pas une véritable politique industrielle dans ce domaine, nous n'existerons pas. Là-dessus, les États-Unis ont été d'une extraordinaire opiniâtreté, en jouant un véritable rôle d'entrepreneur. Il faut mettre fin « au mythe du garage ». Les secteurs clés dans ce domaine ont été très largement financés par l'État américain. Palantir, partenaire de Cambridge Analytica, a été fondé sur le fonds d'investissement de la CIA. Palantir a en plus contractualisé avec la DGSI, ce qui n'a pas été sans soulever quelques questions. Après l'ère de la naïveté, l'ère de la lucidité doit rapidement advenir, avec la construction active d'une politique industrielle

européenne et française. Dans les secteurs clés que sont la santé connectée, l'énergie, l'environnement, les transports et les technologies financières, nous nous exposons à de vrais risques si nous ne réagissons pas.

M. Franck Montaugé, président. - Vous avez dit que l'État n'a pas encore été *ubérisé*. L'État a évolué au fil des âges. Le concept d'État-entreprise est aujourd'hui avancé comme un moyen de décrire la situation politique dans laquelle on est. Aujourd'hui, on sent bien qu'à travers ces GAFAM, le rapport de forces s'inverse ; le monde politique se conforme aux techniques et aux stratégies de développement de ces entreprises. Comment voyez-vous les choses ? Considérez-vous que nous vivons un moment d'affaiblissement des États au bénéfice de ces grandes entreprises, qui participent d'un effacement du politique ?

M. Bernard Benhamou. - Je ne suis pas totalement d'accord. Les exemples de la période récente ont montré que les actions menées pour influencer les processus électoraux conduisaient toujours à polariser les opinions pour mener à la prise de pouvoir de partis extrêmes. La reprise en main à laquelle nous assistons en Chine se fait grâce aux entreprises. Internet, dans ses premières décennies d'existence, s'est développé comme une plateforme d'innovation. On a alors vu des géants venir le cartelliser, avec, aujourd'hui, une quasi-concurrence avec les pouvoirs étatiques traditionnels. Est-ce qu'on pourrait assister à une reprise en main par des sociétés qui deviendraient des substituts des États ? Ce n'est pas une perspective impossible. Le premier métier de Palantir, c'est la prédiction en matière de terrorisme. Faire appel à eux revient à déléguer une partie de nos fonctions stratégiques à une entreprise étrangère. Depuis, la France a souhaité se rapprocher de l'Allemagne pour créer une alternative franco-allemande à Palantir, mais ce n'est pas encore fait. Le risque de voir ces entreprises battre monnaie n'est pas non plus nul. Tout n'est pas encore joué, cependant, sur ces liens et ces confrontations entre entreprises technologiques et États. Pour l'instant, il y a une sorte de méfiance réciproque et d'autocontrôle réciproque. Il y avait une grande porosité, sous la présidence Obama, entre l'administration présidentielle et les cadres des grandes entreprises du numérique.

M. Franck Montaugé, président. - Merci.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible *en ligne sur le site du Sénat*.

Audition de M. Thierry Breton, président-directeur général d'ATOS,
le 28 mai 2019

M. Franck Montaugé, président. - Notre commission d'enquête poursuit ses travaux avec l'audition de M. Thierry Breton. Cette audition est diffusée en direct sur le site internet du Sénat. Elle fera également l'objet d'un compte rendu publié. Enfin, je rappelle, pour la forme, qu'un faux témoignage devant notre commission d'enquête serait passible des peines prévues aux articles 434-13, 434-14 et 434-15 du code pénal. Monsieur Breton, je vous invite donc à prêter serment de dire toute la vérité, rien que la vérité, levez la main droite et dites : « Je le jure. ».

Conformément à la procédure applicable aux commissions d'enquête, M. Thierry Breton prête serment.

C'est à un double titre que nous vous recevons aujourd'hui. Vous êtes d'abord un chef d'entreprises. Après avoir dirigé Thomson ou France Télécoms, vous êtes actuellement président-directeur général d'ATOS, l'un des fleurons français des services informatiques. La société que vous dirigez a intégré le CAC 40 en 2017 et sa capitalisation boursière atteint aujourd'hui plus de 7 milliards d'euros.

Mais vous êtes également ancien ministre de l'Économie, des Finances et de l'Industrie. C'est donc également l'homme d'État que nous interrogeons aujourd'hui, car l'objectif de notre commission d'enquête n'est pas seulement de dresser des constats : il est aussi de trouver les voies du renouveau de l'action publique en la matière.

Anticipant la loi « PACTE », vous avez proposé à vos actionnaires une nouvelle « raison d'être » pour ATOS, à savoir contribuer à façonner ce que vous appelez l'espace informationnel. Vous considérez que cet espace, dans lequel les données circulent, sont stockées et sont traitées, vient s'ajouter aux espaces territoriaux, maritimes et aériens. Estimez-vous que la France - ou l'Europe ? - ait les capacités de reconquérir ce nouvel espace, de redevenir pleinement souveraine, alors que la quasi-totalité de la chaîne du numérique, de la technique aux services en ligne, est dépendante des entreprises américaines, et peut-être chinoises demain ? Vous estimez que sans supercalculateurs européens, sans microprocesseurs spécifiques, indispensables à la puissance de calcul considérable que nécessite l'intelligence artificielle, tous les discours légitimes sur notre souveraineté numérique resteront vains. Pouvez-vous étayer ce propos et nous dire quelles sont, selon vous, les briques technologiques nécessaires à la souveraineté numérique de notre pays ?

Enfin, le ministre de l'Économie a annoncé une nouvelle démarche en vue de créer un *cloud* « souverain », à laquelle il a annoncé qu'Atos participerait. Nous savons que les précédentes tentatives en ce sens se sont

soldées par un échec, et que les contours de la notion de *cloud* « souverain » ne sont la plupart du temps, pas clairement définis par ceux qui l'utilisent. Que pensez-vous de cette initiative et comment l'entreprise que vous dirigez pourrait y participer ? Le *cloud* n'est-il pas déjà en voie d'être dépassé par les objets connectés et le *edge computing* ?

M. Thierry Breton. - Merci Monsieur le Président. Je suis très heureux de me retrouver au Sénat pour aborder cette question de la souveraineté numérique.

Vous me demandez si la France dispose des moyens de reconquérir ou plutôt de trouver sa place dans l'espace informationnel, en cours de constitution. Il est un des espaces de structuration de l'activité humaine. Il y a eu d'abord l'espace territorial où, pendant des millénaires, on a créé des valeurs et vécu. Puis a émergé l'espace maritime, qu'il a fallu conquérir et organiser et qui a nécessité la mise en oeuvre de règles communes contre la piraterie. Ensuite est venu l'espace aérien qu'il a fallu, à son tour, conquérir et organiser. La structuration de chacun de ces espaces a généré des richesses et a impliqué des contreparties d'ordre fiscal. Il y a désormais un quatrième espace, l'espace informationnel. L'activité humaine s'organise désormais dans ces quatre espaces interconnectés aux règles de fonctionnement distinctes.

Plutôt que de le reconquérir, il s'agit de bien appréhender et d'organiser cet espace informationnel qui s'est constitué depuis ces vingt-cinq dernières années. Les pouvoirs publics et les représentants des territoires doivent jouer un rôle dans cette organisation dont l'aboutissement réclamera au moins un siècle. En effet, cet espace, plus dense et complexe de jour en jour, est porteur de dérives, faute d'être organisé et totalement régulé. On y voit ainsi des fortunes s'y créer de manière très rapide, des injustices s'y commettre et des crimes s'y perpétrer. L'organisation de cet espace est d'ailleurs un sujet dont votre commission s'est emparé légitimement.

La France, comme beaucoup d'autres pays, dispose des moyens de s'approprier cet espace. Une telle démarche relève de sa responsabilité. C'est un élément de la souveraineté : il y a une souveraineté sur l'espace informationnel comme il y a une souveraineté sur les espaces territorial, maritime et aérien. Avant de préciser les moyens de l'organisation de cet espace, il faut, au préalable, le définir en tant que tel. Cet espace informationnel est constitué par les informations que nous traitons et générons. Il a donc une réalité. En 2018, l'espace informationnel de la planète représentait 33 Zettabytes - soit trente-trois mille milliards de milliards d'informations - et devrait atteindre cette année 40 Zettabytes, soit l'équivalent du nombre de grains de sables sur la planète ou encore de soleils dans les 200 000 milliards de galaxies aujourd'hui observables. La progression de cet espace obéit également à la Loi de Moore, selon laquelle les capacités des microprocesseurs sont multipliées par deux tous les dix-

huit mois, tandis que les coûts en sont divisés par deux. Ainsi, tous les dix-huit mois le nombre d'informations, créées par l'humanité depuis la nuit des temps jusqu'à nos jours, double, soit, chaque année, une augmentation de 60 % des informations que l'activité humaine crée.

Ces informations sont créées autant par les individus dans leurs activités quotidiennes que les entreprises, en relation avec leurs clients ou dans leurs activités industrielles. ATOS, troisième acteur mondial et *leader* européen en cybersécurité, protège les données de ses clients, les traite, les stocke, processe ces informations ; en d'autres termes organise leur patrimoine informationnel, afin de prévenir les pannes et les agressions. Ces informations sont actuellement gérées soit dans des *data centers* ou centres de données mais aussi dans des *clouds*, - véritables « fermes de données » permettant de mutualiser des équipements afin de baisser les coûts production et de stockage -, qui sont localisés. ATOS est d'ailleurs le premier opérateur européen de *clouds*.

Un autre chiffre me semble intéressant pour vos travaux : aujourd'hui, 80 % des données générées sont stockées à travers le *cloud* - qu'il soit public, hydride, c'est-à-dire privé et public, ou encore privé, c'est-à-dire mis en oeuvre par des entreprises exclusivement pour leurs propres opérations multi-sites et de façon fermée - et les centres de données ; les 20 % restant le sont aujourd'hui à l'extérieur, c'est-à-dire par des objets connectés, comme les véhicules équipés de capteurs ou les objets domestiques, comme des *smartphones*. Ces équipements génèrent ainsi des informations avec des capteurs, les traitent localement, et éventuellement les remontent pour faire de la maintenance prédictive. En d'autres termes, ces équipements traitent ces données au plus près du lieu de leur production.

Ces proportions, d'ici 2025, devraient être inversées du fait de l'*Internet of Things* (*IoT*) et de l'*edge computing*, qui correspond à la nécessité d'amener de la puissance de calcul là où sont créées ces données, de façon à pouvoir interagir localement avec des algorithmes d'intelligence artificielle de plus en plus performants et entraînés au préalable grâce aux gigantesques réservoirs de données des *clouds* et des centres de données. Ces nouveaux algorithmes, créés à partir de machines apprenantes (*machine learning*) grâce aux données connectées provenant des centres de données, seront répartis partout, au plus près de la production de ces données, avec 75 milliards d'objets connectés d'ici 2023, soit 10 par habitant de la planète, contre 23 milliards aujourd'hui. Cette accélération sur temps court souligne la pertinence de vos interrogations sur les questions de souveraineté.

Pour les spécialistes, comme ATOS, du traitement et de la valorisation des données, il est possible de créer des algorithmes d'intelligence artificielle ou d'utiliser ceux qui ont été développés par d'autres sociétés. Ainsi, Google a développé Tensorflow qui est le langage de base de l'intelligence artificielle. Au terme de trois années de négociation, ATOS vient d'ailleurs de passer un accord avec Google qui lui permet

d'utiliser, de manière séparée, ses algorithmes dans ses propres centres de données, à la demande de ses clients. Ce procédé permet ainsi d'utiliser ces algorithmes tout en évitant le vol de données et en protégeant la cybersécurité de nos clients. Il nous faut ainsi être ouverts sans être naïfs, afin de répondre aux attentes de nos clients.

Si la sécurité des données est essentielle aux entreprises, elle l'est également pour l'État. Comme ministre en charge de l'Economie, des Finances et de l'Industrie, je m'étais déjà préoccupé de l'économie immatérielle. J'avais, en ce sens, créé l'Agence pour la protection du patrimoine immatériel de l'État, qui existe encore. En effet, les données du patrimoine immatériel sont multiples et doivent être protégées. Sans doute pourriez-vous attirer l'attention du ministère de l'Economie et des Finances sur l'importance des activités de cette agence.

L'État doit ainsi s'interroger sur les données qui relèvent exclusivement de sa souveraineté et distinguer celles qui doivent être partagées pour créer de la valeur notamment. En effet, dans cet espace informationnel, certaines données ne peuvent absolument pas être partagées, tandis que d'autres peuvent être échangées. Contrairement à l'Europe, les États-Unis et la Chine possèdent des réservoirs homogènes de données considérables qui ont permis l'émergence des GAFA. C'est grâce à l'exploitation de ces données, à l'aide de technologies relativement simples, que des géants du numérique ont pu émerger dans ces pays-continents.

La difficulté provient du fait que ces données sont souvent utilisées sans le consentement de leurs utilisateurs. Ce qui pose la question de savoir comment définir la propriété des informations - comment établir un cadastre - au sein de ce nouvel espace informationnel. La spécificité européenne, comme l'illustre le règlement général sur la protection des données personnelles (RGPD), consiste à promouvoir la protection de l'individu. S'il s'agit d'un début de cadastre, encore faudrait-il l'appliquer uniformément au sein des différents pays européens afin d'éviter la création de barrières ! Par ailleurs, la mise en oeuvre de cette réglementation, dont j'ai soutenu l'adoption, est quelque peu détournée par les utilisateurs qui acceptent d'accéder aux services, sans prendre le temps de lire les conditions générales d'utilisation. On se donne certes bonne conscience, mais au final, nos données partent n'importe où et ce, avec notre consentement ! Il faut ainsi réexaminer les dispositifs en vigueur, l'harmonisation européenne ne me paraissant pas, pour l'heure, tangible.

Parallèlement, conformément à l'idée du *Free Flow of Data* promue par la Commission européenne, certaines données, notamment les données industrielles qui ne sont pas stratégiques, doivent pouvoir circuler, de manière à créer - comme aux États-Unis et en Chine - des réservoirs de données et nourrir des algorithmes qui fourniront les applications de l'intelligence artificielle de demain. Ces algorithmes seront ainsi définis avec les spécificités propres à l'Europe, ce qui nous dispenserait d'utiliser des

algorithmes disponibles sur étagère développés par d'autres acteurs et qui pourraient s'avérer porteurs de risques (virus, portes dérobées...).

Que faire pour développer et maintenir cette souveraineté ? En Europe, nous avons la chance d'avoir ATOS, qui est l'un des grands fabricants mondiaux de supercalculateurs qui se répartissent désormais entre la France, la Chine et les États-Unis. Aux États-Unis, Cray a récemment été rachetée par HP. ATOS aurait souhaité pouvoir procéder à cette acquisition mais la « main invisible » en a décidé autrement, comme auparavant sur SGI.

M. Gérard Longuet, rapporteur. - Le Gouvernement des États-Unis, en particulier le *Department of Defense* (DoD) ?

M. Thierry Breton. - J'ai prêté serment, je n'ai pas d'informations sur cet aspect de la transaction, je ne peux donc pas répondre à cette interrogation. Toujours est-il qu'HP est l'un des grands constructeurs. IBM est également présent sur le marché des processeurs ou *Power PCs*, mais ceux-ci sont loin de constituer le standard technologique aujourd'hui. ATOS - qui est l'équivalent européen d'HP - fournit, de son côté, les principales administrations européennes et nationales, dans le domaine de la défense, du renseignement, ainsi que des centres de recherches et des centres académiques. Notre société vient également d'être choisie par le Gouvernement indien. L'Europe est donc dotée de capacités importantes en la matière, et nous les maintenons.

Mais nos concurrents chinois et américains reçoivent des subventions conséquentes pour développer leurs supercalculateurs. Nous ne jouons pas du tout à armes égales avec eux ! Il faut travailler en partenariat avec les pouvoirs publics. Il serait temps que nos ingénieurs de l'armement, qui passent beaucoup de temps avec nos concurrents, regardent ce que nous faisons ! Encore faudrait-il spécialiser nos ingénieurs, notamment issus de l'École polytechnique, dans ce domaine très important, dont le groupe ATOS est un acteur incontournable. En outre, nous fournissons au Commissariat à l'Énergie atomique (CEA) et aux ingénieurs militaires les supercalculateurs nécessaires à la modélisation de l'usage des armes nucléaires. Enfin, le Japon est également présent, avec l'entreprise Fujitsu, sur ce créneau, mais essentiellement dans son marché domestique.

La semaine dernière, nous venons de lancer les applications du *edge computing*, que l'on pourrait traduire par les capacités de calcul à la frontière, en périphérie. C'est l'enjeu d'apporter la puissance de calcul pour le traitement des données là où elles sont produites. On en crée tellement que les bandes passantes seront dans l'incapacité de les remonter ! C'est la raison pour laquelle on parle désormais de « *fog computing* ». Or, il est désormais nécessaire d'interagir en temps réel. Prenons l'exemple d'une voiture connectée qui représente 30 pétaoctets de données par jour, pour qu'elle puisse se mouvoir et interagir en temps réel. La connexion au *cloud* impliquant un temps de réaction trop lent ; la célérité de la réaction requiert

une intervention locale. Le Sequana Edge est notre première réponse à cet enjeu. Il s'agit d'une boîte de 60 cm sur 30 cm pour 8 kilos qui contient jusqu'à 200 pétaflop - soit la capacité de notre plus gros calculateur il y a dix ans -, pour un coût de dix mille euros. Il a vocation à être installé dans une usine - pour connecter et faire interagir des milliers de capteurs - ou même dans un véhicule- même si ce supercalculateur devrait consommer autant d'énergie que le véhicule pour se mouvoir ! On peut encore délocaliser ce type de supercalculateur dans un supermarché pour effectuer du paiement automatique ou dans un grand chef-lieu régional pour assurer la vidéo-surveillance en temps réel. Cela implique évidemment, en aval, le développement d'algorithmes et de programmes pour ces usages, comme la reconnaissance faciale. Ce type de solution a donc vocation à assurer le traitement des informations recueillies au niveau local, car il n'est pas nécessaire de les faire remonter dans un *cloud*.

Pour certaines applications de souveraineté, qui concernent la sécurité des personnes, le suivi ou encore les activités régaliennes de l'État, les infrastructures doivent demeurer critiques. Veillons à ce que des lois d'extraterritorialité ne puissent faire jurisprudence, dans cet espace informationnel, à l'instar du Patriot Act, selon lequel le juge fédéral américain peut se saisir de toute information à partir de son traitement par un acteur de nationalité américaine, ou de la législation chinoise selon laquelle, depuis 2017, les entreprises nationales ont l'obligation de coopérer avec les services de renseignements de Pékin, pour des motifs d'intérêt national. Nous ne pouvons donc être naïfs face aux impératifs de notre souveraineté. Outre les pouvoirs publics, les entreprises sont de plus en plus conscientes que ces données font partie de leur patrimoine informationnel.

Nos solutions seront compatibles avec la 5G, technologie très particulière qui permet, contrairement à la 4G, de travailler à très hautes fréquences, soit entre 2,5 et 3 gigahertz, se traduisant par une pénétration des ondes de 500 à 600 mètres, voire d'un kilomètre. Les ondes de la 5G sont également nanométriques, ce qui entrave leur pénétration des murs, sinon des fenêtres. L'usage de la 5G intervient ainsi au terme de celui de la fibre, lorsqu'il s'agit de désenclaver des déserts numériques. Cependant, si cette technologie ne permet guère de suivre des objets en mouvement, son implantation en zone très dense ou dans une usine assure la connexion directe d'un nombre conséquent de capteurs. Son usage devrait ainsi être plus industriel que celui de la 4G. On déploie déjà des usines virtuelles avec des avatars de machines, par exemple pour anticiper leur usure, sans la 5G. D'ailleurs, son modèle économique n'est pas encore stabilisé à l'heure où le prix de réserve des licences mises aux enchères n'est pas encore connu. La 5G servira, selon moi, avant tout à accompagner les objets connectés.

Pour pouvoir réaliser de telles machines, encore faut-il disposer des processeurs idoines ! C'est l'un des combats que nous menons au niveau européen. Avec le président de SAP, M. Jim Hagemann Snabe, devenu

depuis lors président de Siemens, nous avons promu auprès de la Commission européenne la souveraineté européenne sur les données, c'est-à-dire la création d'un espace homogène de données en Europe, où les données des Européens puissent être stockées, traitées, processées sur le territoire européen et selon nos règles. Prenons garde à ce que les entreprises travaillant sur le sol européen appliquent nos propres règles ! C'est là un message de bon sens et un combat que l'on continue à mener. Cette dimension dépasse le simple cadre national qui intéresse votre commission.

S'agissant des processeurs, aujourd'hui, ceux-ci sont essentiellement américains, taïwanais et sud-coréens. L'industrie européenne, avec STmicroelectronics, existe, mais nous sommes très loin de réaliser les processeurs spécifiques aux supercalculateurs. La Commission a fini par débloquer 250 millions d'euros dans le cadre d'un programme de développement d'un processeur purement européen, dont ATOS est le chef de file. Bien qu'insuffisant, c'est un début. Pour être efficaces et pour faire face à la concurrence internationale, ces financements doivent être plutôt concentrés sur un petit nombre d'acteurs.

La prochaine génération de microprocesseurs devrait toucher aux limites de la matière, en atteignant 7 nanomètres, et démontrer les limites de la Loi de Moore. Dès lors, nous pourrions entrer dans l'ère du quantique, qui aurait de réelles incidences sur la sécurité des systèmes, en particulier sur le chiffrement de l'algorithme RSA fondé sur la quantification en nombres premiers qui ne résistera pas à la puissance de calcul de ces nouveaux dispositifs.

Enfin, s'agissant de la cybersécurité, nous allons passer, dans les cinq ans qui viennent, d'un paradigme de protection relativement localisé, impliquant quotidiennement des *hackers* et des *gangs* parfois soutenus par des États, à une dimension globale, qui va complexifier le travail de nos agences spécialisées et de nos personnels réunis en cyber-brigades, dont je veux ici saluer le travail remarquable et les très grandes compétences. Il nous faut disposer de ressources pour protéger notre patrimoine et savoir être offensifs, comme dans les trois autres espaces. Le problème devient désormais global, c'est-à-dire totalement holistique et planétaire.

M. Gérard Longuet, rapporteur. - C'est une réelle joie, à la fois intellectuelle et personnelle, que d'accueillir M. Thierry Breton dans cette salle qui lui est familière depuis sa collaboration avec M. René Monory et sa contribution à la création du Futuroscope de Poitiers.

M. Thierry Breton. - Alors ministre de l'Industrie, vous m'aviez également conseillé de rejoindre, après le Futuroscope, le Groupe Bull comme directeur de sa stratégie. L'histoire a voulu que plusieurs décennies plus tard, j'ai été très heureux de faire racheter Bull par ATOS.

M. Gérard Longuet, rapporteur. - J'en viens à la Loi de Moore. Celle-ci a-t-elle un avenir ? Le quantique, qui permet un travail de masse avec des

puissances inouïes de calcul et d'analyse, fournit-il une relève vraisemblable ? Dans le *cloud*, comme dans le stockage des données, existe-t-il une fongibilité des stockages de l'un à l'autre ? Le stockage est-il éternel ? En outre, qu'est-ce qu'une donnée et quel est le temps, au final, de son déploiement ? Tout le cinéma-fiction nous montre des comptes bancaires gigantesques pillés instantanément et on imagine également le détournement de données scientifiques au bénéfice d'un État par des intervenants malfaisants. Nous allons passer d'une logique de fermes de données très largement localisées à un système très largement décentralisé et épars.

M. Thierry Breton. - Ce système sera mixte, les deux coexisteront !

M. Gérard Longuet, rapporteur. - Comment l'Autorité de l'État peut-elle appréhender cette réalité ?

Enfin, troisième sujet plus général : votre entreprise sait gagner de l'argent. Nous avons beaucoup travaillé sur les plateformes et les systèmes d'information. En fait, cette économie du net nous surprend, du fait de son apparente gratuité. Celle-ci pourrait d'ailleurs être qualifiée de sournoise, puisque toutes les opérations créant de la valeur ajoutée sont fallacieusement éprouvées comme gratuites. Un internet payant, reposant sur la tarification du service et à la prestation, à l'instar du Minitel, ne permettrait-il pas une indépendance mutuelle du prestataire et du consommateur ? Compte tenu de l'importance des investissements, peut-on concevoir comme durable une économie reposant sur la croyance que l'on va pouvoir vendre tout à n'importe qui, puisqu'on saura l'essentiel de chacun dans le monde entier ?

M. Thierry Breton. - Votre dernière question fait clairement référence à la théorie du marché biface qui a valu le Prix Nobel à M. Jean Tirole. Cette logique repose sur la monétisation implicite des utilisateurs des plateformes dont le service peut être gratuit, tandis que l'exploitation de leurs données en fournit la face payante. Si ce n'est pas la seule, économie envisageable, force est de constater que c'est l'un des aspects du Net qui fonctionne. Mais il y a de nombreuses dérives comme les *fake news*, ou encore la parcellisation et l'individualisation de l'espace informationnel - chaque individu peut ainsi recevoir tout autant qu'émettre, ce qui le place au centre de son propre espace informationnel, mais c'est un territoire mouvant au gré des « *likes* » émis temporairement par d'autres internautes. C'est une réalité aujourd'hui et il nous sera difficile de revenir en arrière.

En revanche, il importe de l'organiser davantage. Dans ce marché biface, un apprentissage devra se faire jour, de manière spontanée ou plus contrainte et régulée. Certaines données personnelles doivent être sanctuarisées et ne pas pouvoir être partagées, telles que les données de santé, tandis que d'autres, moyennant une contrepartie éventuellement financière, impliqueraient l'accord des personnes concernées. La prise de conscience que ces données peuvent avoir une valeur est l'un des combats à conduire pour les années qui viennent. À partir de cette prise de conscience,

le marché biface devrait être mieux organisé. Votre question présuppose d'ailleurs qu'il y a une forme de tromperie, avec d'un côté le vol de nos données et, de l'autre l'amas de fortunes considérables constitué « sur le dos » des personnes connectées. Il convient de mieux organiser ce marché grâce à cette segmentation entre les données les plus intimes qui ne seront monétisées à aucun prix et d'autres qui le seront selon une gradation à définir.

Votre seconde question concernait les localisations des données et leur matérialisation. Cette interrogation, qui évoque en définitive le rapprochement des espaces territorial et informationnel, s'avère complexe. Elle recoupe d'ailleurs les préoccupations de nos clients quant à la migration des données - qui peuvent être définies comme des paquets d'états mis sur des supports sous la forme de 1 et de 0 (les fameux « bits ») et indexés sous forme de métadonnées - au sein du *cloud*. Est-il possible de retrouver ces données une fois disséminées dans le *cloud* ? Cette question, dite de la réversibilité, s'avère difficile - car les données se déplacent dans le *cloud* - et concerne d'ailleurs en premier chef les *clouds* « souverains » : on doit être capable de pouvoir, à tout instant ou dès le moment où les données représentent une valeur, les restituer intégralement aux clients qui le demandent. D'ailleurs, dans certains *clouds* publics, les données migrent en fonction des conditions de remplissage. Il faut ainsi veiller à optimiser constamment le stockage de ces données au sein des centres de données et des *clouds*, qui sont, du reste, plus polluants encore que le transport aérien dans son ensemble ! Notre prestation vise à permettre à tous nos clients de récupérer l'intégralité de leurs données, sans aucune trace s'ils le souhaitent. Ce point est très important car, dans l'espace informationnel, contrairement aux autres espaces, la trace est, en principe, ineffaçable.

Je suis à présent très heureux, en réponse au rapporteur, d'évoquer la révolution quantique qui vient de débuter et concerne les prochaines générations de processeurs. Vous avez aimé la révolution informationnelle ; vous allez adorer la révolution quantique ! On commence à atteindre les limites de la Loi de Moore établie en 1965 de manière empirique. En effet, on double aujourd'hui la capacité de stockage du silicium tous les dix-huit mois. Les lois physiques retrouvant les lois économiques, le doublement du stockage impliquant la division par deux de son coût. Désormais, les capacités de calcul d'un *smartphone* sont plus importantes que celles du superordinateur des années 80, le Cray ! Si la Loi de Moore semble s'être constamment vérifiée, les niveaux de gravure atteignent désormais 10 nanomètres et devraient, dans quelques années, n'être que de 5 nanomètres, soit quelques atomes. Pour pouvoir créer ces puces, il faut être en mesure de les graver avec un laser. Nous sommes donc à la limite de la matière macroscopique pour traiter, tel que nous le faisons actuellement, l'information. Richard Feynman, Prix Nobel de physique, a eu la géniale intuition d'utiliser les capacités de la physique et de la mécanique quantiques - qui abreuvent déjà notre monde, avec l'IRM, le laser, les

horloges nucléaires et les transistors - pour démontrer les propriétés de superposition et d'intrication. Ainsi, le phénomène de superposition permet, comme son nom l'indique, de superposer différents états en définissant un système comme une succession possible dont l'état est figé une fois la mesure faite ; tant que le système n'est pas figé, il est donc porteur de toutes les possibilités. Dès lors, un Qbit ne va plus porter un 1 ou un 0, mais toute la superposition possible des états entre le 0 et le 1, ce qui permet de décupler, de manière exponentielle, les capacités de calcul. Dès qu'on fige, on trouve alors la solution. C'est pourquoi, il est possible de mettre en parallèle ces Qbits, via la technologie des ions piégés, au laboratoire d'Innsbruck, ou celle, mise en oeuvre au CEA, du refroidissement à - 273 degrés des atomes de carbone, afin d'assurer leur supraconductivité. Ainsi, les techniques de superposition sont maîtrisées en France par les partenaires d'ATOS, qu'il s'agisse des laboratoires du CEA, de l'Université de Saclay, de l'Université Pierre et Marie Curie, ou encore d'autres entités situées à Amsterdam et à Innsbruck. La transformation des bits en Qbits permettra d'obtenir la suprématie quantique, c'est-à-dire des capacités de calculs décuplées qui permettront de craquer instantanément, en vertu de l'algorithme de Shor, le chiffrement RSA sur lequel est édifiée toute la sécurité du réseau internet. C'est pourquoi des algorithmes post-quantiques sont déjà à l'étude, à la demande des agences de sécurité. ATOS travaille déjà à la simulation d'un ordinateur quantique - c'est notre *Quantum Learning Machine*, qui simule jusqu'à 41 Qbits - en créant un langage de programmation idoine sur lequel des générations de chercheurs seront formées à travailler.

Personne ne sait lorsque l'ordinateur généraliste, doté d'une puissance de 50 à 100 Qbits, va remplacer l'ordinateur séquentiel ! Cet ordinateur ne doit cependant pas perdre sa cohérence, lors de sa mise en relation avec le monde extérieur. Il faut ainsi trouver les possibilités de le faire évoluer en parallèle. Même si cette démarche s'avère complexe, elle devrait, un jour prochain, aboutir. Nous constatons en laboratoire la possibilité de faire travailler ensemble des ordinateurs dotés d'un nombre plus restreint de Qbits - de 4 à 10 Qbits - pendant une période plus restreinte, allant jusqu'à deux heures, et de les placer dans des accélérateurs sur des algorithmes particuliers, comme celui qui pourrait casser les polynômes que je viens d'évoquer. L'algorithme de Grover va ainsi permettre, précisément, avec un accélérateur et un programmateur quantiques, de trouver, dans une base de milliards de données, une information pertinente en quelques opérations. En chimie, on peut d'ailleurs modéliser, de façon systématique, des réactions chimiques sur les simulateurs quantiques disposant d'accélérateurs. Ainsi, un pétrolier français vient de nous acheter un simulateur quantique pour simuler des opérations géologiques et des réactions chimiques.

Dans les cinq prochaines années, les grosses machines devraient être dotées d'accélérateurs quantiques, alors qu'il faudra attendre plusieurs décennies avant de créer un ordinateur quantique universel ; l'échelle de

temps étant, pour ce dispositif, beaucoup plus longue. En tout cas, nous y travaillons et la Commission européenne a lancé un programme abondé à hauteur de plus d'un milliard d'euros - le « Quantum Manifesto » - qui associera un certain nombre d'entreprises françaises, dont ATOS qui travaillera sur deux programmes. L'Europe commence heureusement à s'y intéresser, emboîtant le pas aux États-Unis et à la Chine.

Enfin, je reviendrai sur l'intrication qui est une autre propriété de la physique quantique : lorsque deux particules sont en interaction, l'évolution de l'une est identique à celle de l'autre, quelle que soit la distance qui les sépare. La découverte de cette propriété des photons intriqués, réalisée par le Professeur Alain Aspect au début des années 1980, peut générer des applications dans le domaine de la protection des communications.

M. André Gattolin. - Vous avez été un homme d'État et vous dirigez une entreprise au capital franco-allemand. Notre commission entend définir les différents niveaux sur lesquels doit s'exercer notre souveraineté. Lorsqu'il s'agit de défendre notre souveraineté nationale, en recourant notamment à la dissuasion nucléaire, nous ne sommes pas dans l'obligation de partager nos technologies ou nos informations. Une souveraineté européenne partagée doit également être reconnue, en raison des échanges avec le reste du monde et de la dimension critique de l'Europe, en matière de capacités technologiques et industrielles, qui garantit à la France l'exercice de sa souveraineté. Comment, selon vous, ces différents niveaux doivent-ils s'articuler dans ce nouvel espace informationnel où l'échange de l'information est la règle ?

M. Thierry Breton. - Sur la souveraineté, lorsque j'étais ministre en charge de l'Economie, des Finances et de l'Industrie, j'avais recensé les technologies clés sur lesquelles le droit de regard, voire plus si nécessaire, de l'État devait s'exercer en cas de rachat d'une entreprise. Depuis, ces listes ont été élargies, y compris par Bruno Le Maire. Des moyens existent et il nous est parfaitement possible d'assumer nos obligations de souveraineté dans le cadre d'un système de régulation transparent et approuvé par la collectivité nationale. L'État peut ainsi faire respecter ce cadre, sans pour autant devoir être actionnaire ! Lorsque nous avons nationalisé, à contre-courant de l'histoire, en 1981 nos entreprises, nous pensions, à tort, que l'État reprenait sa souveraineté en main. C'est faux ! L'actionnariat est fondamentalement distinct de la souveraineté ! Cependant, une régulation et des règles claires, lisibles et pérennes, de manière à favoriser l'investissement des entreprises, sont importantes. C'est donc aux États qu'incombe la définition de ce qui ressort de leur souveraineté, dans un contexte davantage marqué par la parcellisation du monde que par la mondialisation à outrance.

L'Europe doit également se doter de ses propres moyens pour lancer, en contrepartie, une véritable politique industrielle. À l'heure de la désignation du futur président de la Commission européenne, il importe de rappeler l'échec des tentatives européennes de créer des géants européens

pour des motifs juridiques. ATOS, dont 12 % du capital appartiennent à Siemens et les sièges se trouvent à Paris et Munich, représente une réelle coopération franco-allemande. Accueillant 33 000 ingénieurs de Siemens, ATOS s'avère, en quelque sorte, un « petit Airbus des technologies de l'information », avec un nombre d'ailleurs plus important de salariés que celui-ci ! Au nom de principes concurrentiels qui n'ont plus de sens aujourd'hui et qui relèvent d'une politique de marché tournée vers le consommateur, on a interdit la création de champions industriels européens ! L'Europe doit, à l'inverse, favoriser les rapprochements des grands groupes européens afin de mobiliser des investissements dans des secteurs particulièrement voraces en capitaux et garantir l'émergence d'une politique industrielle sur laquelle doit désormais s'aligner la politique de la concurrence. Personne n'a le droit d'être naïf dans cet espace informationnel ! Nous disposons des atouts pour y parvenir. Puisque nous doublons tous les dix-huit mois le nombre de données, il est tout à fait possible de rattraper notre retard. Nous sommes ainsi au début d'une histoire et il appartient aux législateurs que vous êtes de nous accompagner dans l'organisation de cet espace informationnel.

M. Pierre Ouzoulias. - J'ai été très sensible sur la généalogie que vous avez tracée des trois espaces antérieurs à l'espace informationnel. Or, les trois premiers reposent sur la notion de frontière, plus ou moins matérialisée, et sur les modalités claires de l'exercice de la souveraineté, c'est-à-dire étymologiquement du latin médiéval « superanus », c'est-à-dire le pouvoir au-dessus duquel rien ne peut s'exercer. Néanmoins, quelle pourrait être, selon vous, la souveraineté sur ce quatrième espace, privé de frontière matérielle et dont 80 % de l'information seront bientôt détenus par des acteurs individuels et disséminés ? Quelle en sera l'organisation politique ?

M. Gérard Longuet, rapporteur. - En effet, où sera placé le sergent de ville ?

M. Thierry Breton. - J'ai beaucoup réfléchi à ces questions. J'avais écrit en 1984 dans un roman intitulé « La Guerre douce » (« Soft War »), où j'abordais déjà ces trois espaces et la thématique de la guerre cyber, avant, en 1990, de commettre un autre ouvrage, intitulé celui-ci « La dimension invisible », dans lequel j'abordais le défi du temps et de l'information. J'y réfléchissais précisément à la notion de frontière.

La notion de frontière émerge totalement dans des espaces à conquérir. Votre question est pertinente. Aujourd'hui, nos infrastructures gèrent et stockent les données. Il y a donc une corrélation entre les données et ces infrastructures. La matérialité se retrouve dans les lieux de stockage et les éventuels stockages quantiques seront, eux aussi, physiques. C'est pourquoi, face à l'augmentation exponentielle et la délocalisation prochaine de ces données, mes collaborateurs vont devoir évoluer d'un métier de gestionnaire d'infrastructures, porteuses de données, à celui de gestionnaires

« d'infrastructures d'infrastructures ». Cette évolution va marquer le monde qui vient : ces données vont avoir une adresse, afin d'être utilisées et protégées. C'est comme si vous attribuiez une adresse à chacun des grains de sable.

M. Laurent Lafon. - Qui attribue les adresses ?

M. Thierry Breton. - Aujourd'hui, mon groupe attribue des adresses aux données, dans les algorithmes, pour les protéger. On rentre dans un monde qui s'avère antinomique avec ce qu'on attendait de la mondialisation. En effet, comme l'a démontré Louis de Broglie, la physique quantique repose sur la dualité entre l'onde - la continuité - et la particule. Bien que nous n'en avons pas encore évalué toutes les conséquences, force est de constater que l'on passe de la continuité à la discontinuité et à la parcellisation. Nous entrons ainsi dans un monde profondément parcellisé. C'est la logique des choses ! À partir du moment où chaque individu se considère comme le centre de son propre univers et de son propre environnement, il peut désormais vivre sa culture sans avoir à être abrité dans une zone géographique déterminée. Alors qu'auparavant, les hommes portaient l'information dans un périmètre donné, ils vivent désormais leur culture partout où ils se trouvent et sont devenus le centre de leur culture informationnelle. Aussi, la surface informationnelle n'est pas plane, mais sphérique ! En effet, dans toute sphère, chaque point est le centre. Il faut néanmoins que le Politique trouve un sens au vivre ensemble encore localisé avec des individualités qui vivent déjà dans leur propre univers et selon leur propre règle, dans des communautés qui peuvent s'avérer virtuelles, à l'instar de celles que j'avais esquissées en 1985 dans mon livre « Vatican III ». C'est là un défi ! Sans une structure porteuse et transcendant les individualismes, la parcellisation de l'information, que nous voyons à travers le prisme de la technologie dominante, doit être désormais prise en compte dans nos réflexions pour le siècle qui vient.

M. André Gattolin. - C'est une parcellisation sans cadastre !

M. Thierry Breton. - Il faudra l'inventer autrement. Je pense notamment à l'adressage individualisé, comme la physique quantique nous y invite avec le phénomène d'intrication. La notion de frontière, totalement distincte de celle qui prévaut dans les trois autres espaces, est portée par l'individu le plus parcellaire et, ainsi, par l'information la plus élémentaire. Les frontières de cet espace informationnel, défini par l'agrégation de ces informations et l'évolution de leur sens, seront nécessairement fluctuantes.

M. Gérard Longuet, rapporteur. - Pour prolonger l'observation de notre collègue Pierre Ouzoulias, qui est au coeur de notre réflexion sur la souveraineté, la figure de l'individu centre de son monde s'avère compréhensible. Cependant, au gré des vicissitudes du quotidien, chacun de nous se retourne vers la puissance publique. Ainsi, dans notre société où l'individualisme demeure très fort, la vie numérique, qui s'avère réelle,

coexiste avec une vie collective. Existe-t-il un espace national numérique marqué par des règles spécifiques en matière de diffusion de l'information ? Comment intervenir, lorsqu'une plateforme mondialisée se comporte davantage en éditeur qu'en hébergeur de sites aux contenus fortement répréhensibles ? Intervenir est-il possible ou relève-t-il, au contraire, d'un combat perdu d'avance ?

M. Thierry Breton. - C'est une nécessité absolue. Pour preuve, les contenus invraisemblables du *dark web*, espace criminel lieu de tous les trafics sans aucune barrière. Certaines de nos forces de sécurité surveillent de tels espaces, lieux de tous les trafics, qui doivent être régulés. Certains réseaux sociaux, aux contenus antinomiques avec cette appellation, sont aussi surveillés à juste titre. Si des brigades spécialisées dans la surveillance de ce type d'information doivent être constituées et que des algorithmes spécialisés devraient être mis en oeuvre, il est, en revanche, impossible de placer un représentant de l'ordre public derrière chaque internaute ! Dans nos métiers, où nous avons à protéger nos grands clients contre les cyberattaques, nous constatons que deux cent jours s'écoulent en moyenne entre l'implantation d'un virus par un tiers malveillant et sa détection. Les nouveaux algorithmes d'intelligence artificielle permettent de détecter des signaux faibles et de repérer ainsi l'implantation d'un virus en une seule journée ! Cette démarche, gage d'une réelle réactivité, est également utilisée pour détecter des comportements frauduleux sur des réseaux bancaires et peut également être adaptée, en permettant l'analyse sémantique des contenus diffusés, pour la surveillance des réseaux sociaux.

En outre, il m'est apparu que les incivilités commises chaque samedi depuis l'année dernière étaient analogues à celles que l'on trouve sur l'internet, comme si la différence entre les mondes réel et virtuel était abolie ! Certains États et collectivités publiques procèdent également au suivi, notamment *via* la vidéo-surveillance de leurs administrés ; une telle démarche pouvant s'avérer particulièrement utile, comme nous l'indique l'événement survenu, il y a peu, à Lyon. Compte tenu de la multiplicité des informations et des messages, les systèmes de surveillance des réseaux devront être renforcés, et leur impact décuplés, grâce à l'utilisation d'algorithmes d'intelligence artificielle. Nous ne sommes qu'au début de cette évolution. Les grands acteurs de l'internet pourraient, à leur tour, mettre en oeuvre des algorithmes spécifiques pour détecter les *fake news*.

M. Pierre Ouzoulias. - À la Sorbonne, il est possible de scanner les travaux remis par mes étudiants, afin d'en déterminer, le cas échéant, le taux de plagiat !

M. Thierry Breton. - Peut-être serez-vous amenés à imposer ces outils, y compris pour la détection des *fake news*. Je crois ainsi à ces algorithmes spécifiques qui seront encore améliorés. En outre, le droit à l'anonymat, et ainsi à dire n'importe quoi, sur les réseaux va progressivement disparaître, suite à la mise en oeuvre de ces moyens

techniques, qui conduiront, en retour, à responsabiliser les individus. Si la trace informationnelle, à l'instar de ce qu'a illustré l'épisode dramatique de Lyon en conjuguant la vidéosurveillance avec l'historique des données de consultations internet, existe déjà, son exploitation plus poussée sera longue à construire.

M. Jérôme Bignon. - Tout cela va très vite !

M. André Gattolin. - Les capacités accrues de calcul des supercalculateurs, peuvent-elles permettre d'obtenir une forme de rétro-ingénierie et de comprendre les modalités d'élaboration d'algorithmes compliqués ?

M. Thierry Breton. - La réponse à cette importante question est positive. Les algorithmes seront présents partout. Le législateur doit s'emparer de cette question et nous n'avons pas du tout perdu la bataille de l'intelligence artificielle, loin s'en faut. En revanche, que mettra-t-on dans les algorithmes ? La question du contenu éthique des algorithmes doit être abordée, ainsi que celle de la connaissance de leur mode de fonctionnement et des réactions qu'ils provoquent dans un lieu spécifique. On génère une information impliquant une réaction en temps réel ! Nous réfléchissons déjà à ces différents aspects éthiques avec nos clients, en leur offrant la possibilité d'être partie prenante dans la création de ces algorithmes, en fonction de leurs attentes spécifiques et de leurs propres règles internes.

M. Franck Montaugé, président. - Je vous remercie, Monsieur le président, de votre présentation et de vos réponses précises et techniques à nos questions.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible en ligne sur le site du Sénat.

Audition de M. Henri Verdier, ambassadeur du numérique,
le 4 juin 2019

M. Franck Montaugé, président. - Notre commission d'enquête poursuit ses travaux avec l'audition de M. Henri Verdier, ambassadeur du numérique.

Cette audition sera diffusée en direct sur le site internet du Sénat. Elle fera également l'objet d'un compte rendu publié.

Enfin, je rappelle, pour la forme, qu'un faux témoignage devant notre commission d'enquête serait passible des peines prévues aux articles 434-13, 434-14 et 434-15 du code pénal. Je vous invite à prêter serment de dire toute la vérité, rien que la vérité. Levez la main droite et dites : « Je le jure. »

Conformément à la procédure applicable aux commissions d'enquête, M. Henri Verdier prête serment.

M. Franck Montaugé, président. - Vous avez été nommé à un poste presque unique dans le monde. En effet, très peu de pays ont un ambassadeur du numérique. Vous nous préciserez rapidement les contours de votre mission, et vous nous direz comment elle se distingue de celle du « techplomate » nommé par le Danemark comme « ambassadeur » auprès des Gafam.

S'il est normal et nécessaire d'établir des canaux de contact directs et stables, tels que le « cyber-préfet » nommé par la France en 2014 pour la coordination avec les Gafam face aux problèmes de sécurité et de justice, le fait d'élever cette relation au niveau diplomatique me semble avoir un tout autre sens. Au-delà d'un coup de communication probablement efficace, le Danemark n'a-t-il pas reconnu *de facto* à des acteurs privés, intervenant sur son propre territoire, dans la vie de ses propres citoyens, une forme de statut d'État souverain ?

Votre prédécesseur a organisé le très médiatique appel de Paris pour la confiance et la sécurité dans le cyberespace. Ce texte, présenté par le Président de la République au forum sur la gouvernance de l'internet, lors d'un événement chaperonné par l'ONU, a été signé par 359 États, organisations ou entreprises, comme l'ensemble de l'Union européenne, Google, Facebook ou encore l'Association Internet Society. Quelles ont été les répercussions de cet appel ? Favorise-t-il notre souveraineté numérique ? Comment définir cette dernière ? Comment la renforcer ? Quelles actions concrètes menez-vous en ce sens ?

M. Henri Verdier, ambassadeur du numérique. - À proprement parler, je ne suis pas ambassadeur du numérique, mais ambassadeur pour les affaires numériques : je représente, non pas le numérique, mais la France en matière de numérique. Contrairement à nos amis Danois, nous n'avons

pas d'ambassadeur auprès des Gafam ou de la Silicon Valley. Mais il est impératif de travailler avec ces acteurs.

En 1995, quand j'ai créé ma première entreprise, la France comptait 15 000 internautes. Depuis, le numérique a dévoré des secteurs industriels entiers, l'éducation, les médias, la musique, etc. Aujourd'hui, il soulève d'authentiques enjeux géopolitiques. Au demeurant, le prochain conflit majeur commencera très certainement par une cyberattaque, touchant les hôpitaux, le trafic aérien ou encore les banques. À cet égard, la France oeuvre pour faire reconnaître le droit humanitaire et le droit de la guerre dans le cyberespace, afin de protéger les populations civiles ; mais tous les États du monde n'adoptent pas cette position.

Dans ce domaine, un chiffre est extrêmement frappant : en 2018, 86 % des investissements en capital-risque dédiés à l'intelligence artificielle ont été faits en Chine ou aux États-Unis, et plus encore dans le premier pays que dans le second. Nous sommes face à un embryon de nouvelle guerre froide, dans un contexte marqué par un choc technologique radical : la semaine dernière, un décret du président américain a ainsi contraint Google à ne plus livrer Android à Huawei. Or 20 % des citoyens européens ont un téléphone Huawei. En cet instant, on ne sait pas si la décision prise aura des conséquences pour eux.

Des États voyous, des milices, des groupes politiques s'amusent à interférer dans les élections de tel ou tel pays ; des combats sont à l'oeuvre, pour savoir qui créera les infrastructures numériques en Afrique ou en Asie du Sud-Est, si elles seront privées ou publiques, si elles respecteront la neutralité numérique.

De toute évidence, le numérique n'est plus une simple affaire de *geeks* ou de start-ups. Face à ces enjeux géopolitiques, il est naturel que le ministère des affaires étrangères agisse.

Tout d'abord, l'ambassadeur pour les affaires numériques pilote, dans plusieurs instances, diverses négociations relatives au numérique. Cette année, en raison de dissensions entre les Etats-Unis et la Russie, l'ONU examinera deux textes relatifs à la cybersécurité. Il faudra notamment veiller à ce qu'ils ne se neutralisent pas l'un l'autre. À l'OCDE, nous avons convaincu 119 pays d'ouvrir le dossier de la fiscalité du numérique. Au G7, la France, qui assure cette année la présidence, proposera à ses partenaires une réflexion relative aux contenus *harmful*, à savoir les appels à la haine, les fausses informations, les opérations de harcèlement, qu'il est impératif de réguler, mais probablement avec d'autres méthodes que les contenus terroristes.

En outre, le ministre des affaires étrangères m'a confié pour mandat d'unifier une diplomatie numérique cohérente. Ce travail implique d'authentiques enjeux de souveraineté.

La plupart des sujets numériques portent, en eux-mêmes, un certain nombre de contradictions. En défendant la cryptographie, l'on protège notre industrie, mais l'on complique la tâche du ministère de l'intérieur. En défendant la neutralité d'internet, l'on se protège contre certains monopoles, mais l'on entrave aussi certaines stratégies industrielles.

De manière schématique, la diplomatie numérique française répond à quatre principes.

Premièrement, la France défend les droits de l'homme, l'accès à la culture et à l'éducation, la diversité culturelle et linguistique, la neutralité de l'internet, la transparence de l'action publique, bref les principes démocratiques. Je reviens tout juste du sommet mondial de l'*Open Government Partnership*, où, avec les représentants de quelque 70 pays, nous avons évoqué les moyens de réinventer la démocratie à l'heure d'internet.

Deuxièmement, les abus d'internet posent de graves problèmes de défense et de sécurité : c'est un enjeu régalien majeur. Sur le front de la cybersécurité, nous sommes très inquiets. À mon sens, nous sommes plus vulnérables qu'il y a dix ou vingt ans : désormais, on numérise toutes les données, et on le fait moins bien. L'époque héroïque, que j'ai connue, où les informaticiens faisaient l'informatique, est bel et bien passée. Les informaticiens, qui sont soumis à de fortes pressions budgétaires, achètent de l'informatique sur le *cloud* et assemblent des morceaux de code. Beaucoup d'entreprises maîtrisent moins bien, comprennent moins bien ou protègent moins bien leur informatique. En parallèle, les hackers, ou encore les mafias, sont devenus de plus en plus forts. Les rançons obtenues par les *ransomwares* ou rançongiciels atteindraient des milliards d'euros par an ; et, tôt ou tard, il y aura un cyber-Tchernobyl ou un cyber-Pearl Harbor. Voilà pourquoi la France s'efforce de faire reconnaître la légitimité du droit humanitaire dans le cyberespace.

En outre, l'appel de Paris pour la confiance et la sécurité dans le cyberespace a, de manière novatrice, insisté sur la responsabilité des acteurs systémiques : les États ne pourront pas protéger l'économie contre les cyberattaques si l'on ne change pas le niveau de jeu. Par métaphore, les forces de sécurité peuvent vous protéger si vous fermez vos portes et vos fenêtres. Ainsi, en novembre 2018, nous avons lancé un appel à l'industrie mondiale pour la construction de standards de bonnes pratiques permettant d'améliorer la sécurité collective. La réflexion est engagée dans le cadre de l'OCDE. De plus, nous continuons de faire vivre la communauté des 70 États et 350 organisations qui ont signé l'appel de Paris.

Certains contenus font l'objet d'une grande convergence de vues à l'échelle mondiale : il s'agit du terrorisme et de la pédopornographie, dont personne ne veut et qui sont définis à peu près de la même manière partout.

Au sein de l'espace européen, nous avons ardemment poussé à l'adoption d'un règlement, qui a été voté en première lecture à la fin du

mandat de la précédente Commission. En vertu de ce texte, les contenus terroristes détectés par les autorités légitimes des États membres devront être retirés moins d'une heure après leur signalement. Nous avons testé ce dispositif avec les principaux réseaux sociaux : il exige des efforts de leur part, mais il est applicable. En France, c'est la plateforme Pharos qui se charge des signalements, et, à 90 %, les retraits sont effectifs en moins d'une heure.

Face aux contenus haineux, aux polémiques, aux harcèlements, aux accusations, aux fausses nouvelles parfois manipulées par des puissances étrangères, il faut également assurer une régulation. Nous cherchons avant tout à construire un socle de transparence. Les grandes entreprises du numérique doivent nous permettre d'accéder à leurs codes sources, leurs algorithmes, leurs règles de propagation de contenus, de tri et de filtrage, comme le font les acteurs bancaires. C'est sur la base de cette transparence que l'on pourra construire un certain nombre de politiques publiques. Le fait de ne pas transmettre ces données, ou de transmettre de fausses données, est un délit très grave.

Plus largement, il faudra ouvrir une réflexion sur l'économie de l'attention. On ne vit plus vraiment dans internet : on vit dans des réseaux sociaux. Or le modèle économique de ces entreprises privées repose sur une publicité ciblée. Pour maximiser leurs revenus celles-ci s'efforcent de capter l'attention des internautes. Voilà pourquoi, à l'instar des tabloïds, elles poussent au sensationnalisme et à la démagogie. Si vous cherchez, sur Youtube, à quoi ressemble la Terre, vous trouverez 15 % de vidéos affirmant qu'elle est plate.

Le débat doit être ouvert quant à la propagation artificielle de contenus : la liberté d'expression, ce n'est pas nécessairement la liberté d'obtenir le meilleur audimat avec une information ridicule. Comme on le dit en anglais, « *freedom of speech is not freedom of reach*. »

À ce titre, au sein du G7, nous proposons une charte à la suite de l'accord de Christchurch, conclu avec la Nouvelle-Zélande. Mais nous manquons encore de recul, et nous avons besoin de l'engagement volontaire, public, des grandes plateformes. Il faut mener, à leur égard, un travail de démocratie spécifique. On ne négocie pas avec des entreprises comme avec des États, mais nous sommes prêts à dégainer l'arme du « *name and shame* ».

Troisièmement, la gouvernance d'internet elle-même nous place face à des enjeux de souveraineté majeurs.

Au total, une vingtaine d'instances organise la gouvernance d'internet. Je représente la France au sein de l'autorité de régulation des noms de domaine sur internet, l'*Internet corporation for assigned names and numbers* (Icann), ou encore de l'Internet Governance Forum. Néanmoins, je ne peux pas me rendre auprès de chacune d'elles. Parfois, la France est présente, mais trop rarement : beaucoup de choses se jouent dans ces

enceintes, et notre pays aurait intérêt à continuer à défendre la neutralité du numérique, grâce à laquelle internet n'est pas détourné par ceux qui ont accès au marché. C'est sans doute ce principe qui a permis la vague d'innovations que l'on a connue depuis vingt ans. En Europe, une directive le protège, mais, à l'échelle internationale, il est peu à peu grignoté, par les pays qui n'ont pas adopté de normes similaires ou encore par les acteurs qui tentent de prendre le contrôle des téléphones et des ordinateurs par les terminaux.

Au demeurant, internet est largement diffusé par satellite : un État peut très bien décider d'installer un satellite géostationnaire pour développer son propre internet, en filtrant ou en censurant les contenus de son choix. Le risque de désagrégation d'internet, avec un bloc chinois, un bloc russe et un bloc euro-américain est bien réel : nous essayons de l'empêcher, car il infligerait une perte profonde à l'humanité.

Quatrièmement et enfin, avec le ministère de l'économie et des finances, notamment avec la direction générale du Trésor, je concours à une diplomatie économique. Nous travaillons ainsi la question de la fiscalité du numérique. Il ne s'agit pas d'adopter une fiscalité punitive, mais de prendre acte du fait qu'internet a transformé la chaîne de création des valeurs. La valeur ne se crée plus exclusivement dans les bureaux d'études, protégés par la propriété intellectuelle, ou dans les usines. Il y a quelques semaines, le *Sun* titrait en une qu'un grand joueur de football payait, en Angleterre, plus d'impôts que Starbucks et Amazon réunis. Aujourd'hui, il faut partir du principe que la valeur s'apprécie au lieu où l'on consomme. On l'a fait pour la TVA : on peut le faire pour le reste de l'économie. Ce travail imposera beaucoup de négociations multilatérales, mais il ne suppose pas des concepts incroyablement sophistiqués, d'autant que, avec le numérique, l'on sait au centimètre près où se trouve le client.

Nous sommes également attentifs au statut des travailleurs de plateformes. À l'heure actuelle, les chauffeurs Uber, qui sont sous statut d'autoentrepreneur, ne disposent d'aucun droit social. La France pèsera à l'Organisation internationale du travail (OIT) pour que ces travailleurs obtiennent des protections minimales, à défaut d'un statut à part entière.

Dans toutes ces instances, on est de plus en plus préoccupé par la très grande difficulté à caractériser les positions de domination. Avec le numérique, on ne domine pas forcément parce que l'on a davantage de boutiques ou de clients : on peut dominer parce que l'on dispose d'un format propriétaire, parce que l'on est seul à posséder une donnée qui confère de la valeur à toutes les autres, parce que l'on s'est placé à un point très précis du cycle commercial. Les évolutions sont très rapides, et les autorités de la concurrence, où qu'elles soient, sont en grande difficulté pour intervenir à temps.

La souveraineté numérique est une question majeure. Nous vivons dans le monde numérique ; notre vie s'y déroule, qu'il s'agisse des informations, de l'éducation, de la santé ou encore des transports. Bientôt viendra le temps des *smart cities*. Or la question du numérique a été un peu négligée, ou en tout cas mal posée.

De surcroît, nous ne vivons plus dans internet tel qu'il a été conçu à l'origine, par les chercheurs, sur la base d'une culture de transparence et de collaboration, avec un contrôle périphérique ; nos existences se passent chez Facebook, Netflix, Twitter, etc. Ces systèmes n'ont pas les devoirs de neutralité, de légalité et de continuité qui incombent au service public. Ils sont au service de certains intérêts. C'est tout à fait leur droit, à condition que la puissance publique soit en mesure de les réguler. Or, souvent, on nous a fait prendre des vessies pour des lanternes.

Je ne suis ambassadeur chargé du numérique que depuis six mois, mais j'ai été, pendant quatre ans, à la tête de la direction interministérielle du numérique et du système d'information et de communication de l'État (Dinsic). Auparavant, j'ai mené la politique d'*open data* ; encore avant, j'avais créé une *start-up* dans le domaine du numérique.

J'en suis persuadé, le numérique est en somme un élément liquide. Il faut savoir s'en servir : or le grand enjeu du numérique, c'est la capacité stratégique, qui suppose de maîtriser soi-même les compétences dont on a besoin. Il s'agit là du seul moyen de critiquer ce que l'on vous propose, de défier votre fournisseur. À ce titre, l'État s'est peut-être un peu désarmé en entrant dans une logique de sous-traitance maximale. Il m'est arrivé de diviser des factures par dix, car les compétences numériques de mon équipe me permettaient d'évaluer les prestations proposées. Mais encore faut-il disposer de cette expertise.

À l'avenir, l'un des grands rôles des États pourrait être de garantir les « communs », ce qui n'est pas approprié ou privatisé. Dans le secteur numérique, on peut penser à Wikipedia, à certains logiciels libres ou encore à Firefox. Mais ce secteur pourrait inclure une grande partie de l'action publique : l'*open data*, l'identité numérique, que l'État pourrait fournir gratuitement, ou encore les systèmes de paiement neutres, que l'Inde propose d'ores et déjà.

Au sujet de la souveraineté numérique, j'entends beaucoup de propositions de réglementation ; j'entends recommander une intégration verticale de la filière française. Mais cela ne suffit pas, car les filières françaises peuvent être mauvaises ou insuffisantes. La vraie question est la suivante : la situation est-elle réversible ?

La France est tout à fait capable de contester le système dans lequel on tente de l'enfermer. Elle a encore un État, avec son administration, ses ingénieurs et ses *start-ups*. Il n'y a plus tant de pays sur Terre qui disposent

de tant d'atouts. Néanmoins, il faut bien savoir ce que l'on entend par souveraineté.

M. Gérard Longuet, rapporteur. - Le titre d'ambassadeur est prestigieux, et il oblige : on attend d'un ambassadeur qu'il défende la politique française dans différents lieux de décision.

Or toute politique nationale est un compromis entre différentes tensions, différents soucis, différentes préoccupations. Vous avez évoqué ce que devait être la politique française en la matière. Sentez-vous s'exercer des forces contraires, conflictuelles, ou du moins des préoccupations de natures extrêmement différentes, entre les grands acteurs du secteur public français, face à cet « océan du numérique », pour filer la métaphore aquatique ?

De plus, sentez-vous chez nos partenaires européens une ligne de partage entre deux positions tranchées ? Au contraire, assiste-t-on à une dispersion assez grande ?

En matière numérique, pouvez-vous nous préciser les lieux du multilatéralisme ? C'est très bien de signer des chartes, mais il faut également s'intéresser aux instances où l'on produit la norme.

Vous avez évoqué une piste très singulière, celle de l'internet national, par satellite. Pensez-vous qu'un pays puisse être tenté par un tel système, entièrement verrouillé ? Du fait de votre passé professionnel, vous mesurez ce que l'économie numérique a de déconcertant : les utilisateurs ne payent pas, parce qu'ils sont le produit du service, et les employés, considérés de manière flatteuse comme des entrepreneurs, apparaissent parfois comme les exploités d'un nouveau style.

M. Henri Verdier. - Les missions de l'ambassadeur du numérique ont été fixées en conseil des ministres, à la suite d'une réunion interministérielle.

Pour les affaires extérieures, le travail est plus solidaire que dans le fonctionnement usuel de l'État, ne serait-ce que parce que les troupes sont maigres : il est indispensable de se répartir les rôles et de se concerter.

M. Gérard Longuet, rapporteur. - Le Trésor est-il un acteur important dans votre domaine ?

M. Henri Verdier. - Tout à fait, ainsi que le réseau des ambassades, Ubifrance et la French Tech. Bien sûr, des tensions peuvent se faire jour entre les approches ouvertes et sécuritaires, entre un souverainisme à l'ancienne mode et un enthousiasme invitant à embrasser la modernité. Mais, dans l'ensemble, nos positions extérieures font l'objet d'une assez bonne concertation interministérielle.

M. Gérard Longuet, rapporteur. - Quel est le nombre de centres de décision de l'administration centrale impliqués peu ou prou dans ces échanges internationaux ? Une douzaine ?

M. Henri Verdier. - Presque tous les ministères dialoguent avec leurs homologues européens : ces relations impliquent autant d'embryons de diplomatie thématique, et c'est une très bonne chose.

Effectivement, l'on dénombre en tout une douzaine de centres : plusieurs se trouvent à Bercy. S'y ajoutent le secrétariat général de la défense et de la sécurité nationale, le SGDSN, l'Agence nationale de la sécurité et des systèmes d'information, l'Anssi, ou encore le ministère de la culture.

Pour ce qui concerne mes attributions, je peux vous faire parvenir ma lettre de mission.

M. Gérard Longuet, rapporteur. - Volontiers.

M. Henri Verdier. - Pour plusieurs sujets, j'ai la mission de représenter la totalité des ministères. Pour d'autres, je concours à l'élaboration des politiques ; toutes ces dispositions sont assez précisément écrites.

L'espace européen, tel que je le découvre, n'est ni binaire ni tout à fait éclaté. Il est composé de quatre ou cinq espaces, ce qui nous affaiblit un peu. Certains pays sont très atlantistes, très libéraux, défendent le libre-échange et les libertés individuelles à tout prix. De son côté, le sud de l'Europe cherche son chemin. Il faut convaincre ces blocs, un par un, de la pertinence des idées françaises. De grands progrès ont été accomplis lors du mandat de la précédente Commission, mais je ne suis pas certain qu'une souveraineté européenne soit clairement conçue en la matière. En tout cas, elle n'est pas revendiquée de manière suffisamment active.

Aux grandes enceintes multilatérales, l'ONU, l'Unesco, l'OCDE, le G7 et le G20, s'ajoutent de nombreuses instances *multistakeholders* ou multi-parties prenantes : l'Icann, l'IGF (Internet Governance Forum), le W3C (World Wide Web Consortium), etc.

Ce système est indispensable, car il s'agit en l'occurrence d'artefacts fabriqués par un monde industriel : c'est ce dernier qui sait comment tout cela fonctionne. Voilà pourquoi il doit être partie prenante de la décision. De même, sur certains sujets, la société civile refuse que les États et les grandes entreprises du secteur numérique s'entendent dans son dos. Voilà pourquoi elle exige, avec raison, de la transparence et des capacités de contestation.

Si l'État, à travers France Télécom, avait organisé internet à lui seul, nous n'aurions pas connu un tel cycle d'innovation, chamboulant bien des positions acquises : heureusement qu'il y a un *multistakeholderism*. Mais, aujourd'hui, la légitimité de ce système pose question - je pense par exemple à certaines entreprises ou ONG, qui ont du mal à reconnaître que les États ne sont pas des acteurs comme les autres.

M. André Gattolin. - Certains considèrent même que les États sont des acteurs moins importants que les autres.

M. Henri Verdier. - Tout à fait, on le constate par exemple à l'Icann. D'ailleurs, pour l'heure, notre rôle y est strictement consultatif.

Enfin, ce système est-il complet, couvre-t-il bien les bons sujets ? Les pères fondateurs d'internet ont compris l'importance de la neutralité du numérique. Les plateformes ont un devoir de décence, de sincérité et de transparence, mais cette question ne fait pas encore l'objet d'un débat international. Si le péril de la fracture d'internet venait à se concrétiser, je ne sais pas non plus où l'on en débattrait.

L'inconvénient du *multistakeholderism*, c'est que ce sont les standards de fait qui l'emportent, non les mieux conçus mais ceux qui ont attiré le plus d'usagers.

Je souscris à vos propos sur la nouvelle économie, mais je constate que plusieurs modèles de nouvelle économie coexistent. On parle souvent des GAFA ; mais alors qu'Apple vend des objets manufacturés, Facebook vend de la publicité présentée sur la base des conseils de vos amis et Google vend aussi de la publicité, après avoir indexé tous les contenus d'internet. Nos efforts de régulation doivent donc être précisément ciblés en fonction des marchés.

Je rentre d'une mission dans la Silicon Valley : nous avons aussi des alliés là-bas, comme la Mozilla Foundation et l'Electronic Frontier Foundation. Beaucoup de gens, en effet, sont très inquiets face à l'évolution de la culture et du monde numériques.

M. Pierre Ouzoulias. - Merci de votre présentation tout à fait passionnante. Vous avez dit qu'il était nécessaire que l'État puisse maîtriser certains outils et certaines technologies pour garantir l'usage qu'en font les citoyens. C'est fondamental. Pour ma part, j'utilise LibreOffice pour prendre des notes, mais ce logiciel libre a deux défauts : il ne garantit pas la pérennité de mes données, car l'association qui l'anime peut disparaître du jour au lendemain,...

M. Henri Verdier. - Mais Android ne vous la garantit non plus !

M. Pierre Ouzoulias. - ... et il ne m'apporte aucune garantie en matière de sécurité. Comment un État pourrait-il assurer aux utilisateurs la pérennité et la sécurité des données ? Comment les citoyens peuvent-ils vérifier que ces garanties leur sont vraiment apportées ?

M. André Gattolin. - J'ai beaucoup travaillé sur ces questions, et notamment sur la gouvernance mondiale d'internet, avec Catherine Morin-Desailly. J'ai eu l'occasion d'auditionner plusieurs fois le président de l'Icann : on nous promet à chaque fois de grandes réformes pour rendre le *multistakeholerism* plus transparent et satisfaisant pour les Européens. Mais les polémiques se multiplient : en 2016, Donald Trump a menacé de reprendre en main l'Icann ; les conflits d'intérêts sont nombreux. Le système favorise les grandes entreprises, essentiellement américaines, car les soi-

disant représentants de l'internet libre sont, en fait, complètement soumis à ces grands groupes qui les financent en grande partie. Il s'agit donc d'acteurs qui, tout en prétendant ne pas avoir d'idéologie, sauf anti-étatique, sont extrêmement idéologiques. Dans ce cadre, il est très difficile de se faire une place : on est réduit au rôle d'observateur.

Les GAFA font aussi planer la menace d'une fragmentation de l'internet, comme si sa globalisation devait être conservée à tout prix ! Ces organisations, qui se prétendent libres et autonomes, ont en fait un caractère très idéologique et ont finalement imposé leurs règles à l'ensemble des États.

Vous avez aussi envisagé, de manière un peu catastrophiste mais néanmoins vraisemblable, les futurs cyberconflits du XXIe siècle. Le numérique fait bel et bien partie des armes non conventionnelles, qui deviennent de plus en plus importantes. Ainsi la Russie, qui dépense beaucoup moins d'argent dans sa défense que par le passé, s'est-elle concentrée sur les aspects de cyberdéfense.

Outre les attaques visant à détruire ou à paralyser tel ou tel site, il faut mentionner des pratiques plus *soft*, mais plus insidieuses, développées notamment par la Chine, qui consistent à piller des millions de données dans le cyberespace. Ces données alimentent le système d'apprentissage des machines, dans une logique de *deep learning,* ce qui permet d'acquérir une avance en matière d'intelligence artificielle. Ce faisant, une culture ou un État pourrait finir par contrôler toute la planète.

Diplomatiquement, la question est très délicate, car il est difficile de pointer du doigt ces manoeuvres susceptibles de conduire à un conflit généralisé. Nous vivons durablement dans un monde pacifié, où les conflits sont de nature intermédiaire, sans viser à la rupture totale. Ces attaques invisibles sont néanmoins préoccupantes. Plutôt qu'une cyberguerre visant à la destruction de l'adversaire, ne faut-il pas craindre, à terme, une nouvelle forme de colonisation ou de soumission par le biais du contrôle des données ou de l'intelligence artificielle ?

Mme Viviane Artigalas. - Internet a changé le monde. C'est un fait. On ne peut envisager la souveraineté numérique de la même manière que l'on conçoit les autres formes de souveraineté. Il ne suffira pas d'édicter des normes ou d'ériger des murs. Au contraire, notre souveraineté numérique suppose la capacité d'agir, de naviguer, de travailler dans cet univers.

Pour préserver notre souveraineté, peut-on envisager de créer des systèmes publics capables de concurrencer les systèmes privés existants, tout en garantissant la neutralité, la transparence, la gratuité ? Avons-nous les moyens, en France et en Europe, de mettre en place de tels systèmes publics ?

M. Henri Verdier. - Vos questions peuvent être regroupées en deux grandes familles.

La première porte sur la souveraineté par l'action. J'avais dans mon équipe précédente un développeur qui avait une pensée stratégique profonde en matière de souveraineté numérique : il était très vigilant et il anticipait toujours les pièges dans lesquels on risquait de tomber. Dans les années quatre-vingt-dix, il avait créé une start-up qui avait compté jusqu'à 150 salariés et qui produisait des applications pour le *Newton*, l'assistant personnel numérique d'Apple. Puis, un jour, Steve Jobs a décidé de simplifier la ligne des produits et l'a supprimé. Subitement, la start-up a disparu, à cause d'une décision prise à 8 000 kilomètres de la France. Dès lors, il a toujours cherché à savoir où était hébergé le code source, qui le possédait, qui assurait sa maintenance, etc. Il ne voulait plus s'enfermer dans un système nous plaçant sous la dépendance d'un choix technologique ou d'une stratégie marketing. Pourquoi, en effet, placer des services publics sur Google Maps quand il existe OpenStreetMap ? De même, en matière de lutte contre les contenus terroristes, on nous dit qu'il existe déjà une base de données gérée par Google, Apple, Facebook et Twitter. Il suffirait de leur signaler un contenu pour que celui-ci soit retiré dans l'heure. Pourquoi ne peut-on pas avoir accès à cette base, à sa structure ? On ne peut pas vérifier si les contenus que l'on a envoyés ont bien été pris en compte. L'erreur est humaine. Nos ingénieurs pourraient améliorer la base. En la matière, il existe des pistes d'améliorations pour renforcer notre souveraineté.

Pour faire face à ces monopoles gigantesques, on a parfois cru que le meilleur moyen était de créer un monopole concurrent, de faire un Google à l'européenne, un Facebook européen, etc. Mais il est très difficile techniquement de réaliser ce *Consumer Internet*, cet internet de grande consommation. Surtout, ce secteur obéit à la règle du *winner takes all*, selon laquelle le gagnant prend tout le marché : on préfère rester sur Facebook, qui compte trois milliards d'utilisateurs, pour y retrouver ses amis, plutôt que de s'inscrire sur un réseau plus petit où l'on ne connaît personne.

Les effets de réseaux font que le plus gros attire tous les utilisateurs. C'est pourquoi on s'est souvent trompé en la matière ; et finalement les partisans de la souveraineté numérique n'ont plus osé s'exprimer - à tort. Il faut différencier selon les secteurs : par exemple dans les infrastructures, rien n'empêche de faire une 5G européenne. On possède encore les entreprises et le savoir-faire, et le modèle économique est différent. En outre, on n'est pas obligé de construire un contre-monopole pour affaiblir un monopole : quand je dirigeais la Dinsic, j'ai demandé aux administrations de ne plus installer leurs services sur Google Maps, mais d'utiliser OpenStreetMap. On a bien fait : depuis, le coût de Google Maps a explosé. On n'a pas suffisamment cherché à allumer des contre-feux, à posséder des bases arrières, des réserves. Dans une bataille, lorsqu'on ne peut pas gagner, on se replie sur des bases arrière ou dans le maquis pour résister. Avec une bonne compréhension du libre et des « communs », on peut parvenir à créer des points d'indépendance. Sans procéder ainsi de manière systématique, l'État peut au moins veiller à la sécurité juridique, technique, voire financière des

« communs ». Peut-être vaut-il mieux subventionner Firefox pour que son système soit performant plutôt que de se lancer dans des aventures industrielles.

En réponse à vos questions sur ce sujet, la France n'a jamais attribué officiellement une cyberattaque à un pays : je ne peux donc pas le faire ici.

Comme on compte autant de communautés que d'enceintes, le système est lourd et lent. Voilà sept ans qu'Amazon réclame le droit de créer le « .amazon » et que la question reste en suspens.

Au sujet des diverses formes d'emprise, disons-le : il y aura des conflits cyber. On voit les armes prépositionnées, on connaît les budgets ; *WannaCry* était initialement une arme, elle a été volée et utilisée par d'autres. Bien sûr, il existe aussi des formes plus douces de prise de pouvoir. Toutefois, pour reprendre votre exemple, je crois que la Chine a déjà assez largement à faire pour récupérer les données de sa population ; je ne suis pas sûr qu'elle soit déjà en train d'essayer d'aspirer les données des Français, mais nous devons rester très vigilants.

Depuis que je suis ambassadeur, j'ai pu mesurer l'impact mondial du règlement général sur la protection des données, le RGPD : le Japon a négocié et obtenu l'accord d'adéquation avec l'Europe. Ainsi, le RGPD couvre déjà 700 millions de personnes. De même, par le biais de conventions, au titre de l'article 108 du Conseil de l'Europe, une quinzaine de pays se manifestent pour créer un droit similaire : l'Inde, la Tunisie, ou encore la Californie qui s'est dotée d'un régime identique.

À terme, plusieurs milliards d'individus pourront partager le même régime juridique, avec des sécurités comparables et une philosophie identique, selon laquelle c'est le consentement de l'usager qui détermine la licéité de l'usage, et non l'intérêt de l'État ou un contrat extorqué. Nous pouvons en être fiers, même si la mise en oeuvre est complexe.

Vous évoquiez les approches frontales, violentes, et les emprises par des formes de *soft power*, voici un exemple de contre *soft power*. On pourrait aussi mentionner le règlement européen « eIDAS », *Electronic IDentification Authentication and trust Services*, qui permet la reconnaissance mutuelle au sein de l'espace européen des identités numériques respectives. Certains pays demandent à en faire partie. Je crois que dès que les vingt-huit pays européens parviennent à se mettre d'accord sur un texte, l'Europe possède un petit avantage compétitif, car le texte qu'elle adopte est de qualité et peut rassembler. Ce n'est pas un hasard si quinze pays ont d'ores et déjà recopié le RGPD : ce texte avait déjà été largement débattu, décortiqué, mûri.

M. Franck Montaugé, président. - Nous vous remercions de cet éclairage.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible en ligne sur le site du Sénat.

Audition de Mmes Pauline Türk, professeur de droit public à l'université Côte d'Azur et Annie Blandin, professeur à l'IMT Atlantique, membre du Conseil national du numérique,
le 4 juin 2019

M. Franck Montaugé, président. - Notre commission d'enquête poursuit ses travaux avec l'audition commune de Mme Pauline Türk, professeur de droit public à l'université Côte d'Azur, et de Mme Annie Blandin, professeur à l'Institut Mines-Télécom Atlantique et membre du Conseil national du numérique.

Cette audition est diffusée en direct sur le site internet du Sénat. Elle fera également l'objet d'un compte rendu publié. Je rappelle, pour la forme, qu'un faux témoignage devant notre commission d'enquête serait passible des peines prévues aux articles 434-13, 434-14 et 434-15 du code pénal. Je vous invite donc à prêter serment de dire toute la vérité, rien que la vérité. Levez la main droite et dites : « Je le jure. »

Conformément à la procédure applicable aux commissions d'enquête, Mmes Pauline Türk et Annie Blandin prêtent serment.

Madame Pauline Türk, vous apportez à nos réflexions l'approche d'une constitutionnaliste : vous avez coordonné un colloque et un récent ouvrage sur le concept et les enjeux de la souveraineté numérique. Vous y retracez l'histoire relativement récente de cette expression et vous soulignez la grande diversité des définitions qui lui ont été données. Peut-être pourrez-vous nous éclairer, pour commencer, sur les diverses acceptions que reçoit la « souveraineté numérique », selon qu'elle est exercée par les États, revendiquée par les citoyens, voire contestée ou confisquée par certaines multinationales.

Madame Annie Blandin, l'ouvrage que vous avez coordonné, *Droits et souveraineté numérique en Europe*, fait également suite à un colloque. Vos travaux mettent l'accent sur la dimension européenne des enjeux et des réponses à donner. Dans ce livre, vous insistez particulièrement sur le poids de ces géants du numérique - que vous qualifiez même d'« entreprises souveraines » - et vous décrivez les difficultés d'une gouvernance partagée des instances du réseau internet. Vous reviendrez sans doute sur ces défis et sur les moyens dont nous disposons pour y répondre.

Mme Annie Blandin, professeur à l'IMT Atlantique, titulaire d'une chaire européenne Jean-Monnet sur l'Union européenne et la société de l'information, membre du Conseil national du numérique. - L'expression « souveraineté numérique » est désormais entrée dans le vocabulaire courant. Elle nous conduit à repenser notre conception classique de la souveraineté et à l'envisager au pluriel.

Même si l'on accole souvent à la notion de souveraineté des adjectifs multiples - on parle par exemple de « souveraineté alimentaire » -, le sens du mot ne varie pas : la souveraineté incarne la volonté du peuple et permet à la collectivité de déployer toutes ses potentialités. Il ne s'agit pas d'un état qu'il s'agirait de sanctuariser, mais plutôt d'un processus : on parle ainsi de « souveraineté en réseau », compte tenu de la multiplication des lieux de normativité, de « stratégie de souveraineté » et de « souveraineté efficace ».

Cette souveraineté prend tout son sens dans le cadre européen, même si la souveraineté européenne a vocation à interagir avec la souveraineté nationale. La souveraineté est aussi une notion qui se décline. Certaines données sont qualifiées de souveraines, comme les données géographiques, dans le rapport de Mme Valéria Faure-Muntian. En effet, elles servent de support aux décisions de la puissance publique et font autorité ; elles doivent donc être maîtrisées, et l'autorité publique ne doit dépendre de personne pour les élaborer ou les utiliser.

À cet égard, deux idées me semblent essentielles. Premièrement, le numérique conduit à repenser la souveraineté, car ses enjeux se déploient dans toutes les activités humaines et sont d'ores et déjà pris en compte par certaines politiques publiques et dans divers instruments juridiques. Deuxièmement, la souveraineté numérique ne peut pleinement s'exprimer que lorsqu'elle incarne un projet européen.

La souveraineté numérique conduit d'abord à repenser la souveraineté. Il est désormais impossible de parler de souveraineté numérique sans évoquer des formes de concurrence entre souveraineté étatique et pouvoir des entreprises. En effet, le numérique peut concerner tous les champs de l'activité humaine. Avec son livre, *Quand Google défie l'Europe,* Jean-Noël Jeanneney a été l'un des premiers à tirer la sonnette d'alarme dans le domaine de la culture, à propos de la création de Google Books. Désormais, les enjeux se déploient aussi sur le terrain économique, démocratique, social, éducatif, territorial, etc. Il suffit de regarder dans quels domaines investissent les géants du net pour savoir exactement où se situent les enjeux souverains : il s'agit en particulier de la santé, de l'agriculture, ou encore de la mobilité.

Or le numérique est structuré autour de ces grandes entreprises, ces géants du net. On parle aussi d'entreprises systémiques, ou de plateformes, par référence à leur statut d'intermédiation. Je les ai qualifiées de souveraines dans la mesure où elles déploient de véritables attributs de la souveraineté.

Lorsque, à l'instar de Google, l'on entend organiser les informations à l'échelle mondiale afin de les rendre accessible à tous, on proclame une ambition souveraine. Il en va de même lorsque l'on veut « numériser le patrimoine mondial », comme le fait Google Books. Facebook se donne pour but de connecter le monde entier. Ces entreprises possèdent donc certains

attributs de la souveraineté : un territoire transnational, en dépit de différences nationales, où elles édictent elles-mêmes des normes juridiques qui s'appliquent à une population d'internautes. Certes, cette population peut s'exprimer et participer au débat public par le biais des réseaux sociaux, mais elle est aussi surveillée, et son système cognitif est contrôlé jusqu'à la création d'addictions, comme le décrit fort bien la théorie de l'économie de l'attention.

Ces entreprises ont encore d'autres attributs de souveraineté : une langue, l'anglais, à laquelle s'ajoute une série d'innovations linguistiques qui apparaissent sur les réseaux sociaux, une monnaie, virtuelle, le *bitcoin* ; un pouvoir réel d'édiction de normes juridiques et de régulation, à travers les « conditions générales d'utilisation », véritables lois de l'internet, et un pouvoir de modération des contenus.

Ainsi, une nouvelle composante de la souveraineté apparaît, qui consiste à produire ou à utiliser des données, et à maîtriser l'accès à l'information *via* les moteurs de recherche en position dominante, comme Google, ou par le biais des assistants vocaux qui réduisent la liberté de choix des utilisateurs. L'utilisation des donnés est donc centrale. Il n'est pas étonnant qu'une firme comme Alibaba se définisse elle-même comme un groupe de données, et plus seulement comme une plateforme de vente en ligne. À l'image de Monsanto, beaucoup d'autres entreprises, initialement ancrées dans une activité matérielle, se transforment et fondent leur stratégie sur les données et sur l'aide à la décision. Finalement, elles s'insèrent, plus ou moins volontairement, dans un système de surveillance des consommateurs.

Comment ces entreprises se sont-elles développées ? Le cadre politique de certains pays, notamment les États-Unis, a favorisé leur émergence. Elles ont aussi profité des lacunes du droit de la concurrence, peu outillé pour empêcher l'émergence de quasi-monopoles par des entreprises en croissance bénéficiant de l'effet du « *winner takes all* » *(le gagnant remporte tout)*. De même, pour des raisons de seuil, le droit de la concurrence ne peut empêcher les rachats de start-up par ces grandes entreprises. En outre, à l'heure où l'on cherche à responsabiliser davantage les plateformes dans le cadre, notamment, de la lutte contre la haine, on peut se demander si le régime de responsabilité allégée ou aménagée, qui date de la directive relative au e-commerce, ne leur a pas apporté une protection trop grande. Ce sujet est polémique, mais je crois qu'il ne faut s'interdire aucune piste de réflexion.

Ces enjeux sont déjà pris en compte dans certaines politiques publiques. Le RGPD a une dimension d'application extraterritoriale et régule également le transfert des données depuis l'Union européenne vers les États tiers, sous réserve d'une protection adéquate ou équivalente. Autre exemple, la France, qui n'a pas hésité, faute d'accord au niveau européen, à choisir sa propre voie avec la taxe sur les services numériques.

Pour que la souveraineté numérique puisse s'exprimer, certaines conditions doivent être remplies. Il faut commencer par régler la question concurrentielle. Dans le cadre des états généraux des nouvelles régulations numériques, quatre sujets ont été abordés : régulations concurrentielle, sociale, sociétale et moyens de la régulation. Ces sujets sont tous liés. Le constat est simple : il n'est pas possible de lutter, par exemple, contre la surexposition aux écrans ou la haine sur internet si l'on ne s'intéresse pas à la structure du marché, aux modèles d'affaires et aux fonctionnalités techniques.

J'évoquerai quelques pistes d'action. La première est celle de la régulation asymétrique : infliger des obligations plus lourdes aux acteurs systémiques. La deuxième est celle de l'interopérabilité des réseaux sociaux, afin de développer la concurrence et donner davantage de choix à l'utilisateur. La troisième, qui est la plus extrême mais qui n'est plus aujourd'hui un tabou, est celle du démantèlement des géants du numérique. On ne sait pas si cette solution serait efficace, car le principe du « *winner takes all* » laisse à croire que des structures identiques réapparaîtront.

Il faut clarifier les relations entre les États et les géants du net. Quelle part réserver aux droits négociés, à la corégulation, aux différents partenariats public-privé ? Quand doit-on, au contraire, donner de la voix, et recourir à des interdictions ? Même si nous sommes conscients du trop grand pouvoir de ces entreprises, nous sommes paradoxalement en train de leur confier des missions régaliennes, lorsque l'on attend d'elles, par exemple, qu'elles régulent des contenus illicites ou qu'elles déréférencent des sites.

Ce dilemme, il s'exprime actuellement au travers des deux types d'approches envisagées en matière de lutte contre la haine sur Internet et de retrait des contenus. D'un côté la proposition de loi présentée par la députée Laetitia Avia qui, en imposant une action rapide aux entreprises sous la contrainte de très lourdes sanctions, peut amener finalement à leur confier des fonctions quasi judiciaires. De l'autre, les préconisations de la mission sur la régulation des réseaux sociaux, initiée par le secrétaire d'État en charge du numérique et ayant bénéficié d'un accès assez fin aux techniques de modération suivies par Facebook, qui va beaucoup plus dans le sens d'une responsabilisation et d'un rééquilibrage des pouvoirs entre les acteurs privés et l'État.

J'en viens à l'idée selon laquelle la souveraineté numérique devrait reposer sur une voie européenne, fondée sur des acquis et de nouvelles trajectoires.

Les acquis sont essentiellement le niveau élevé de protection des droits et valeurs de l'Union européenne - protection des données personnelles, liberté d'expression, diversité culturelle, etc. -, la volonté de développer une approche éthique, notamment pour le déploiement de l'Intelligence artificielle et l'affirmation de la citoyenneté numérique.

S'agissant des trajectoires, nous avons, en matière de stratégie numérique, une approche trop centrée sur le marché intérieur. Il faut développer une politique industrielle ambitieuse pour faire émerger, si ce n'est des champions, du moins des entreprises ayant un seuil d'activité suffisamment important ou présentant des alternatives crédibles, une politique de concurrence réformée permettant de défendre les intérêts européens, notamment par des investissements dans les infrastructures, et une harmonisation fiscale - nous sommes engagés dans une trajectoire destinée à lutter contre l'optimisation fiscale agressive.

L'Europe a une singularité : elle promeut une vision sociale du numérique. Grâce aux travaux de certains chercheurs, comme Antonio Casilli, nous avons pris conscience du « *digital labor* » *(travail numérique issu des plateformes)*, ces microtâches que l'usager ne voit pas.

Enfin, il ne faut pas oublier la promotion de l'intérêt général. On parle beaucoup des données personnelles, mais on commence seulement à évoquer les données non personnelles. En la matière, l'enjeu est de définir un cadre, incitatif ou obligatoire, pour le partage de ces données d'intérêt général, qui peuvent être une source de valeur, d'innovation et d'activités nouvelles. C'est le cas, en particulier, des données environnementales. Il faut examiner les alternatives, afin de comprendre pourquoi certaines n'ont pas fonctionné - je pense à Europeana. Il est nécessaire de créer des plateformes fondées sur d'autres valeurs, notamment des plateformes collaboratives ou de service public.

Ainsi armée, la souveraineté européenne a vocation à rencontrer d'autres souverainetés dans le monde. L'Union européenne évolue dans un cyberespace qui est, à la fois, un espace de coopération et de conflictualité, notamment parce que certaines règles de droit sont globalisantes. Le sujet est d'actualité, notamment avec la question de l'opportunité de déréférencer les contenus au plan mondial ou seulement au niveau de l'Europe. La CNIL s'est saisie de la question.

Dans ce contexte international tendu, il faut maîtriser les piliers de la souveraineté pour conserver une certaine indépendance.

Il s'agit, d'abord, de contrôler la dimension infrastructurelle du numérique, qui comprend les réseaux de communications électroniques mais aussi les données, lesquelles « font » infrastructure - comme la directive de 2007 établissant une infrastructure d'information géographique dans la Communauté européenne, dite « Inspire », en dresse très bien le constat - , et de développer la cybersécurité, notamment pour tout ce qui concerne les infrastructures critiques.

Il faut également maîtriser les données, en particulier l'accès à l'information, dans les domaines où l'enjeu de souveraineté est fort, comme l'agriculture, l'alimentation et l'environnement. Les professionnels exposés à la mainmise de grandes entreprises doivent conserver leur pouvoir de

décision. Par exemple, dans le domaine de l'agriculture, il s'agit de résister aux grands vendeurs de semences...

Sur cette base, l'Europe a vocation à être ouverte : il s'agit non pas de déployer une souveraineté défensive, mais d'agir sur la scène internationale, en réagissant, en coopérant, en se positionnant sur certains sujets comme modèle, en organisant la convergence des règles. L'exemple du RGPD est éclairant, car il a une véritable ambition internationale : les transferts de données vers les pays tiers sont bien organisés, par exemple. Apple incite ainsi les États-Unis à s'inspirer du RGPD : jouer sur l'aspect de la protection de la vie privée peut aussi constituer un avantage compétitif.

Dans ce contexte, la responsabilité européenne est importante, car, finalement, l'objectif est de faire oeuvre de civilisation. Le numérique est à la source d'une transformation profonde non seulement des processus de production et de consommation, mais aussi des processus démocratiques et des relations sociales. La seule transition d'ampleur comparable est probablement la transition écologique, et il nous faudra sans doute croiser ces deux problématiques pour aller vers un numérique plus sobre, au service de la transition écologique.

Mme Pauline Türk, professeur de droit public à l'université Côte d'Azur. - Je suis également très honorée d'être entendue aujourd'hui par votre commission d'enquête. Je commencerai mon propos en reprenant la fameuse déclaration d'indépendance du cyberespace de John Perry Barlow, l'un des pères du mouvement libertarien qui a grandement influencé la construction du réseau internet, lequel s'adressait ainsi aux gouvernements : « Vous n'avez pas de souveraineté où nous nous rassemblons ». Cela révèle un hiatus entre l'État, qui exerce une autorité verticale, hiérarchique et unilatérale sur un territoire formé par des frontières physiques, et le réseau, dont les principes fondateurs valorisent une conception horizontale, dématérialisée, transnationale et non hiérarchisée, fondée sur le principe de liberté contre les régulations et la censure.

Je voudrais également citer une autre formule célèbre, celle de Lawrence Lessig, professeur de droit constitutionnel à Harvard, lequel constatait voilà déjà vingt ans : « *Code is law* » : sur les réseaux, le code informatique fait loi. La régulation des comportements dépend ainsi davantage des normes techniques définies par des ingénieurs informaticiens que des normes juridiques édictées par les États.

En 2017, le Danemark a nommé un ambassadeur auprès des géants de la Silicon Valley, considérant les GAFA comme des partenaires dans les relations diplomatiques.

La souveraineté numérique, ce sont d'abord des enjeux. Les réseaux sociaux transnationaux dématérialisés ne sont plus un monde virtuel : les applications se sont multipliées, les plateformes se sont développées, les techniques algorithmiques ont progressé, avec des effets majeurs dans le

monde réel. L'évolution ne va pas s'arrêter, avec les perspectives de la 5G et de l'intelligence artificielle.

Tous les secteurs sont concernés : l'économie, le politique, le commerce - eBay et Amazon -, les transports - Uber, BlaBlaCar -, la culture - Amazon, Netflix, Spotify -, l'information et les télécommunications - Twitter, Facebook -, le secteur médical - Google, Truven Health Analytics -, le secteur militaire et de défense, la justice, l'enseignement...

La souveraineté en droit, historiquement, c'est l'indépendance des États, le pouvoir de commandement suprême sur un territoire et une population. Or on constate que les sociétés humaines et les États qui les organisent sont dans une situation de dépendance croissante vis-à-vis des technologies du numérique et des entreprises américaines qui les contrôlent. L'État est affaibli, concurrencé dans toute une série de compétences par des opérateurs privés qui redessinent les politiques publiques. Certains responsables de multinationales revendiquent même le fait de pouvoir, dans quelques années, rendre des services équivalents, voire supérieurs, à ceux des États. Traditionnellement, les services rendus par l'État sont la contrepartie de l'obéissance à la loi et des impôts payés par les citoyens : il existe donc un risque de déséquilibre du modèle classique. Qui cherche encore aujourd'hui un emploi à Pôle emploi ? On recourt davantage à Viadeo, Linkedin, Monster, qui sont des applications américaines.

La concurrence touche les fonctions régaliennes : la monnaie, avec le bitcoin et les autres monnaies virtuelles ; la fiscalité, qui est inadaptée au monde numérique - je ne reviens pas sur la taxe GAFA - ; le système politique et institutionnel, avec des ingérences extérieures dans des processus électoraux ou les processus de transition démocratique. Les États ont des difficultés à faire respecter le droit - droit commercial, droit de propriété, droit d'auteur, droit à la protection de la vie privée ou des données personnelles -, la loi - celle sur l'interdiction de diffuser des sondages le jour des élections est contournée, puisque les résultats sont publiés sur des sites étrangers, en Belgique ou en Suisse -, les décisions de justice - le livre du docteur Gubler sur la maladie de François Mitterrand a été interdit, mais était pourtant disponible en ligne -, le secret défense - en 2013, la direction centrale du renseignement intérieur-DCRI- a eu du mal à obtenir de Wikipédia la disparition d'informations portant sur un site militaire classé secret défense. Je n'évoque pas les fuites de documents confidentiels et les difficultés de l'État à assurer la sécurité au regard du développement de la cybercriminalité. On se souvient du rançongiciel Wannacry en 2017 : 150 pays attaqués, 200 000 victimes, 30 000 institutions ou entreprises, dont Renault et la société des chemins de fer allemands, le ministère de l'intérieur russe et des dizaines d'hôpitaux britanniques touchés.

La souveraineté numérique, c'est ensuite un terme, qui revêt plusieurs acceptions. La notion est critiquée parce qu'elle est floue, ambiguë,

protéiforme, polysémique. Chacun met ce qu'il veut derrière ce mot, qui recouvre une réflexion sur le pouvoir de commandement dans le monde numérique : qui fixe les règles ? Sur quel fondement et avec quelle légitimité ? À qui obéit-on, et avec quelles garanties ? Répondre à ces questions, c'est comprendre qui est souverain sur les réseaux et comment s'exprime cette souveraineté.

Certains conçoivent la souveraineté numérique sous l'angle juridique et politique, d'autres sous l'angle économique, et d'autres encore sous l'angle technique. La souveraineté est collective pour les uns, individuelle pour les autres. Elle peut se concevoir au niveau national, au niveau européen - pour la protection des données -, et même au niveau international - pour la gouvernance des réseaux. La souveraineté numérique est souvent revendiquée par les États, mais elle est aussi parfois reconnue aux GAFA ; elle est quelquefois réclamée pour les communautés d'utilisateurs, voire pour les individus.

Pour mettre de l'ordre dans ces acceptions, on pourrait retenir trois approches du concept de souveraineté numérique.

La première est juridique : c'est celle des États au sens classique. Depuis une dizaine d'années, les États revendiquent la souveraineté numérique au sens de pouvoir de commandement et de se faire obéir sur les réseaux. À l'origine, il s'agit surtout d'une revendication de la Chine ou de la Russie, qui étaient inquiètes de l'américanisation d'internet. Rapidement, cette préoccupation devient générale : je pense au Brésil, qui a organisé un sommet NETMundial spécifiquement sur cette question, à l'Allemagne ou à la France à la suite des révélations sur l'affaire Snowden.

La souveraineté des États, c'est l'égalité des États, mais, en réalité, tel n'est pas le cas, car certains sont plus ou moins souverains sur les réseaux : les États-Unis le sont plus que les autres, et la Russie ou la Chine travaillent à le devenir davantage. Tous les États ne retiennent pas la même conception de la souveraineté numérique : pour certains, elle est autoritaire, voire offensive - c'est le droit pour l'État de reprendre le contrôle des espaces numériques, d'y appliquer sa loi, d'y promouvoir ses intérêts - ; pour d'autres, dont l'Europe fait partie, elle est plus libérale et défensive - c'est le droit pour l'État de protéger ses citoyens contre les entités malveillantes ou mues par des intérêts purement commerciaux.

La deuxième approche de la souveraineté numérique est politique et économique : c'est celle des Gafam. Les multinationales américaines ont bâti des réseaux, qu'elles gèrent très largement : elles disposent *de facto* du pouvoir d'imposer des règles. Elles bénéficient d'une suprématie grâce à leur position dominante sur le marché, et sont les véritables pouvoirs souverains dans le cyberespace. Qui fixe les conditions générales d'utilisation ? Qui est en situation de monopole pour la fourniture de services devenus indispensables ? Qui a le pouvoir de se faire obéir ? Qui peut décider de

supprimer des contenus, de censurer un tableau, de fermer le profil d'un utilisateur - cela équivaut à une mort sociale, notamment pour la jeune génération -, de vendre des données personnelles, de ne pas rendre des données stockées sur un *cloud* ? Ce sont toujours les mêmes : Google, Amazon, Facebook , Apple, etc..

La troisième approche est plus libérale et individualiste : c'est celle des utilisateurs. On se rapproche de la notion de souveraineté populaire. Le pouvoir de commandement est pour soi-même : c'est le droit à l'autodétermination, le droit de maîtriser son destin - nous n'en sommes pas encore là. Cette souveraineté peut être individuelle : l'individu doit rester maître de son destin sur les réseaux. Cela se traduit concrètement par des garanties qui sont en cours de consécration : le droit à la portabilité des données, le droit à l'oubli, le droit au déréférencement, le concept d'autodétermination informationnelle que certains voudraient d'ailleurs voir inscrit dans la Constitution.

Malgré des conceptions assez variées, la souveraineté numérique renvoie à une préoccupation : le refus que les peuples, les communautés d'utilisateurs, les États, les individus perdent le contrôle de leur destin au profit d'entités mal identifiées, non légitimes et ne poursuivant pas l'intérêt général.

J'en viens aux solutions et aux perspectives.

Il faut, d'abord, poursuivre la prise de conscience. Elle est à l'oeuvre dans le monde politique, votre commission d'enquête en témoigne. Depuis 2012, elle se fait à l'échelon international, avant de prendre de l'ampleur en Europe. Je rappellerai les rapports parlementaires sur le sujet, la loi de 2016 pour une République numérique et les travaux sur le *cloud* souverain - un décret récent est venu imposer un stockage des données des archives nationales sur le territoire. Une réflexion a été menée sur un commissariat à la souveraineté numérique, et des débats ont eu lieu sur la constitutionnalisation d'une charte du numérique pendant l'été 2018.

Dans le grand public, la problématique reste, en revanche, très largement méconnue, je le constate moi-même à l'université. Il faut réfléchir à la meilleure façon de former les jeunes générations, en leur expliquant le rôle de certains acteurs de la gouvernance de l'internet comme l'*Internet corporation for assigned names and numbers* (Icann), en les sensibilisant à la protection de leurs données sur les réseaux, en les incitant à utiliser certains moteurs de recherche comme Qwant et en leur enseignant les rudiments du code informatique, au moins en option.

Cette sensibilisation leur permettra peut-être de se laisser moins dominer par les machines que notre génération : ils seront plus concernés, moins fatalistes, et prendront conscience des leviers d'action dont ils disposent à titre individuel.

Il faut, ensuite, développer notre potentiel technologique. Nous ne pouvons pas continuer à rester spectateurs de la guerre que se livrent les puissants. Il est nécessaire de développer un système d'exploitation et un moteur de recherche européens - la Chine a Baidu, la Russie Yandex - pour casser les monopoles, et menacer les États-Unis de façon crédible sur le plan technologique.

Il faut, par ailleurs, faire progresser la régulation dans le sens de nos valeurs et de l'intérêt général. Il s'agit de continuer à négocier des aménagements en matière de protection des données personnelles, comme le RGPD qui est un beau succès - acquis de haute lutte ! -, et nos principes fondateurs : la liberté d'expression, la neutralité, la diversité linguistique, le respect de la vie privée.

Il faut, enfin, réfléchir à la gouvernance, et y prendre notre part. Le mouvement est à l'oeuvre et il permettra de mieux partager les responsabilités de la gestion des réseaux et d'y promouvoir nos valeurs européennes. L'évolution des statuts de l'Icann, société californienne qui s'est progressivement ouverte, le montre bien : c'est une lutte diplomatique de tous les instants. Songeons à la fameuse formule prononcée en 2015 par Barack Obama, qui assumait : « Internet est à nous »... La bataille n'est pas gagnée. L'Icann et les autres organismes de gestion des ressources critiques, les sommets mondiaux, les forums annuels sur la gouvernance d''internet, les instances de gouvernance technique sont autant de lieux de négociations méconnus où nous devons être présents. À terme, certains revendiquent même l'élaboration d'une charte internationale de l'internet, dans laquelle seraient consacrés les principes essentiels qui devraient régir le développement du réseau. Cette solution est sans doute très idéaliste, mais la perspective a été tracée.

En attendant, faute de partage des responsabilités, les États les plus préoccupés n'ont pas attendu : ils en ont tiré des conséquences en faisant internet à part - c'est la balkanisation du web -, ce qui n'est pas souhaitable. En termes de rapport de forces, nous avons des atouts : les utilisateurs européens sont le premier marché économique pour les GAFA. Nous avons aussi des possibilités d'alliance entre pays européens, mais également au-delà : notre préoccupation est largement partagée sur tous les continents.

Rappelons que, sur le plan des valeurs, nous avons une grande proximité avec les États-Unis, avec lesquels la collaboration l'emportera toujours - espérons-le ! - sur la confrontation.

Depuis deux cents ans, nous avons essayé d'organiser le pouvoir politique pour qu'il soit conciliable avec le respect des libertés des citoyens. Pour obtenir cette démocratie, on a fait des révolutions, guillotiné, voté, construit des régimes démocratiques dans lesquels les gouvernants sont élus par les gouvernés, sont responsables, transparents, tenus d'agir dans l'intérêt général et de rendre des comptes. C'est à ces conditions qu'ils peuvent

exercer le pouvoir qui est le leur. Aujourd'hui, nous nous soumettons à de nouveaux pouvoirs qui commandent sur les réseaux et ne sont soumis à aucune de ces contraintes et exigences démocratiques. Jusqu'à récemment, cela ne dérangeait personne. Il est temps d'en prendre conscience et de reprendre la main.

M. Gérard Longuet, rapporteur. - Je vous remercie de la qualité de vos interventions et de la passion qui vous anime.

Madame Blandin, la solution est, pour vous, européenne. Mais sur cette question tous les pays n'ont pas la même approche. Faut-il catégoriser les États européens par grands groupes de comportement ? Nous sommes convaincus, et c'est la raison pour laquelle le Sénat a accepté cette commission d'enquête, que le numérique est une question éminemment politique et totalement universelle, non seulement par son étendue mondiale, mais par l'universalité de ses sujets.

Madame Türk, vous avez insisté sur l'émergence difficile de la démocratie, qui est une forme d'organisation politique tardive et fragile et vous avez eu raison de rappeler l'approche libertarienne qui est à l'origine de la création d'internet. L'autorité de l'État qui s'est progressivement constituée repose sur un contrat de sécurité : les impôts sont la désagréable contrepartie de la protection que l'État nous garantit. La sécurité a changé de forme et de modalités, et la démocratie a introduit une idée plus nouvelle, celle de la participation à la construction permanente de ce contrat, à sa vérification, à son contrôle.

Une personne que nous avons entendue a évoqué la démocratisation interne des GAFA. Vous avez, pour votre part, mentionné le démantèlement, qui a déjà touché les sociétés pétrolières américaines et les sociétés de télécommunications. On peut imaginer que la grande structure a une volonté de démiurge, mais aussi qu'elle est opportuniste : elle veut des utilisateurs. Si ceux-ci souhaitent qu'un certain nombre de comportements soient adoptés à leur endroit, elle peut en tenir compte, dans un intérêt purement commercial. La démocratisation est-elle impensable dans un système qui se veut, d'origine et de construction, libertarien ?

Mme Annie Blandin. - Pour tout ce qui intéresse le numérique, l'Europe agit, et avec succès. On a évoqué la libéralisation des télécommunications...

M. Gérard Longuet, rapporteur. - C'était il y a vingt-cinq ans !

Mme Annie Blandin. - ...plus récemment, il y a eu le RGPD.

M. Gérard Longuet, rapporteur. - Il s'agit d'une véritable réalisation, mais le RGPD ne mobilise pas le client final. Peut-être contribue-t-il à inciter les grandes entreprises et les grands clients des GAFA à adopter des comportements différents afin d'éviter, s'ils ne respectaient pas cette

réglementation, l'effet négatif des sanctions? Pour ma part, je clique toujours de bon coeur pour donner mon consentement, persuadé d'être protégé.

Mme Annie Blandin. - Le RGPD n'est pas sans faille. Mais la règlementation sur la protection des données personnelles ne sort pas de nulle part : En effet, elle remplace une directive qui avait déjà posé le principe du consentement - même si l'on peut discuter du caractère éclairé ou non de ce consentement. Les entreprises s'y conforment-elles par seule crainte des sanctions ? Je crois plutôt qu'elles le font parce que c'est dans leur intérêt concurrentiel pour gagner des utilisateurs.

Au niveau européen, en ce qui concerne la régulation juridique du numérique, on constate que les directives laissent la place à des règlements, , car les régimes s'uniformisent entre États membres - je pense notamment, outre le RGPD, aux règles de connectivité dans les télécoms ou aux relations entre les plateformes et les entreprises.

Un projet européen fondé sur des valeurs communes, mais avec des actions nationales diversifiées est tout à fait possible. Même si la fiscalité des Gafam et la taxe sur le numérique sont des sujets qui divisent, chaque État entreprend des actions nationales, dans une perspective européenne. Le débat fait rage sur la proposition de loi pour lutter contre la haine sur Internet. L'action de l'Allemagne, résolument fondée sur une sanction lourde à l'encontre des entreprises qui ne modèrent pas les contenus, crée un effet d'entraînement. La France choisira sans doute une voie médiane, en responsabilisant les entreprises concernées. Je reste convaincue que le niveau européen est pertinent pour agir.

M. Gérard Longuet, rapporteur. - Ne faut-il pas faire une distinction entre les pays libertaires, ceux qui sont alignés sur des standards atlantiques, et ceux qui privilégient des standards nationaux ?

Mme Annie Blandin. - Des tendances diverses se dessinent au sein de chaque pays. Notre président de la République reçoit Mark Zuckerberg, mais mène une politique volontariste en matière de lutte contre la haine sur Internet. Aucune fracture n'est insurmontable. Regardez l'industrie des télécoms - que vous connaissez bien, monsieur le rapporteur -, la France s'était opposée à leur libéralisation, soutenue par les pays du sud de l'Europe, alors que l'Allemagne y était favorable. À force de temps, de jurisprudence, et de garanties données en termes de service public ou de couverture, le processus s'est concrétisé.

M. Gérard Longuet, rapporteur. - Qu'en est-il de la démocratisation interne des structures et de la gouvernance ?

Mme Pauline Türk. - La gouvernance s'appuie sur des acteurs divers qui débattent des principes à défendre dans le cadre d'ONG ou de forums d'utilisateurs. On pourrait effectivement y insuffler des principes démocratiques.

Les Gafam défendent naturellement avant tout des intérêts particuliers, privés et commerciaux. Les démocratiser reviendrait à leur donner le statut de pouvoirs souverains au niveau politique. Cela s'inscrirait dans la perspective d'un droit constitutionnel global, qui considère que pour préserver les principes démocratiques des États, il faut les transposer à l'échelle supra-nationale. Cela ne va pas encore de soi...

M. Gérard Longuet, rapporteur. - Selon vous, le droit de la concurrence n'est pas la solution absolue. Dans les domaines de l'énergie ou des télécoms, force est de reconnaître que la liberté du citoyen s'exprime dans la liberté d'achat. Dans des systèmes monopolistiques, une autre forme de régulation existe, qui passe par le comportement des utilisateurs.

Mme Pauline Türk. - Ces opérateurs n'ont pas pour objectif de défendre l'intérêt général. Le nerf de la guerre, c'est leurs intérêts commerciaux. Ils se démocratiseront si les utilisateurs les obligent à faire évoluer leur régulation, en choisissant telle ou telle plateforme plutôt qu'une autre en fonction, par exemple, de la rédaction de leurs conditions générales d'utilisation. La confiance est au coeur de la relation commerciale. Pour conserver leurs clients et en gagner de nouveaux, les Gafam doivent répondre aux souhaits des utilisateurs et anticiper les risques pour leur réputation.

M. Gérard Longuet, rapporteur. - Vous avez mentionné le rachat des start-ups. Le droit de la concurrence tel qu'il s'exerce en Europe reste archaïque. La logique de ces acquisitions est diabolique, car celui qui dispose de moyens financiers peut absorber une entreprise dont le développement n'est pas encore abouti, en la privant de la possibilité d'exister indépendamment. C'est une forme d'étouffement de la concurrence par un *round-up* sur toutes les nouvelles plantes. Certaines pousseront, d'autres pas. Les clients perdent la possibilité d'avoir accès à certains fournisseurs nouveaux.

M. Rachel Mazuir. - Le droit a du mal à s'imposer, mais il existe aussi un levier industriel. Vous nous suggérez une sorte d'Airbus européen de la technologie. Il reste à trouver le partenaire. Dans un monde soumis à la finance, seule une puissance industrielle à l'échelle de l'Europe peut faire contrepoids.

Certaines plateformes ont investi dans le champ de la santé. Doctissimo, initiée par notre collègue Claude Malhuret, est une poule aux oeufs d'or qu'aucune plateforme ne peut concurrencer.

Enfin, le Président de la République a reçu Mark Zuckerberg en lui réservant des honneurs dignes d'un chef d'État. N'est-ce pas faire peu de cas de notre souveraineté ?

M. Hugues Saury. - La localisation des données est un enjeu majeur. Certains considèrent que les données devraient être territorialisées en France ou en Europe. D'autres estiment qu'elles ont vocation à être diffuses. Il existe

des obligations de désignation de représentants en France. Tout cela peut-il suffire pour garantir l'application de nos lois ?

M. Jérôme Bignon. - Quand j'étudiais le droit européen, sous l'autorité du professeur Teitgen, il avait utilisé le syndrome du nénuphar sur l'étang pour qualifier le processus de construction de ce qui allait devenir l'Union européenne. On découvre un jour que le nénuphar a recouvert toute la surface de l'étang, grâce au déploiement des rhizomes sous la surface de l'eau. Les Gafam vont encore au-delà, grâce au principe d'extraterritorialité qui les caractérise. Comment contrôler leur action à l'échelon européen ? Peut-on envisager une souveraineté européenne qui les forcerait à respecter les valeurs des 28 États membres ?

Dans nos discussions avec les Gafam, il faudrait que nous puissions faire valoir notre souveraineté sur tous les sujets. Comment le pourrions-nous dès lors que notre président reçoit M. Zuckerberg comme un chef d'État ?

Mme Türk a mentionné le droit constitutionnel global, en précisant que les Gafam n'étaient pas les partenaires des États. Parmi les acteurs de ce droit, il faut aussi prendre en compte les organisations non gouvernementales, comme l'Union internationale pour la conservation de la nature (UICN), ou bien la Fédération internationale de football association (FIFA) qui joue un rôle quasi-étatique dans les négociations très politiques où l'on décide du lieu où sera organisée la Coupe du monde. Les Gafam ne pourraient-ils pas entrer dans un cadre de ce type ?

Le débat autour de la propriété des données personnelles a été abordé à plusieurs reprises au cours de nos auditions. Peut-on imaginer que l'Europe ou la France la consacrent ? On nous a laissé entendre, lors de notre première audition, qu'il était possible de rétablir ou d'imposer une forme de territorialité pour ces données. Le champ d'action extraterritorial des Gafam ne rend-il pas ce processus compliqué ? Sans doute vaut-il mieux continuer d'avancer pas-à-pas plutôt que d'entrer dans des conflits qui favoriseraient les blocages.

M. Franck Montaugé, président. - À propos, justement, d'extraterritorialité, le *Cloud Act* qui date du début de 2018 permet aux autorités américaines d'aller chercher des données sur simple mandat, hors mécanismes de coopération judiciaire internationale. Alors que les Européens se croient protégés par le RGPD, les États-Unis peuvent en réalité récupérer leurs données. N'est-ce pas là une source de conflit entre juridictions ? Comment faire primer nos valeurs européennes ?

Une branche des études juridiques porte sur l'économie constitutionnelle. Ne peut-on pas considérer que le développement des Gafam rebat les rapports de souveraineté entre les États et contribue au développement de cette économie, selon laquelle l'intérêt général n'est plus

exclusivement défini par les États, mais aussi par les grands prescripteurs que sont devenus les Gafam ?

Mme Pauline Türk. - À partir du moment où des acteurs privés exercent un pouvoir politique sur une communauté, souvent transnationale, ils entrent dans le champ du pouvoir constitutionnel.

Les lieux de stockage des données ont été diversifiés et un certain nombre d'entre eux sont désormais situés en Europe. Faut-il continuer à nous battre en ce sens ? Je n'en suis pas certaine, car en matière de données, toute l'architecture est précisément pensée pour échapper aux frontières.

La patrimonialisation des données est une idée récurrente : Doit-on faire de chaque individu le propriétaire de ses données, à charge pour lui d'en faire ce qu'il souhaite ? L'Europe ne se résout pas à cette approche très individualiste, par crainte d'un désinvestissement de la puissance publique, à qui il revient d'assurer la protection de ces données.

La logique des rhizomes me rappelle celle de la grenouille que l'on plonge dans une marmite d'eau froide dont on porte la température à ébullition et qui ne se rend pas compte qu'elle est en train de bouillir. Deux approches sont possibles, celle des Russes qui souhaitent imposer par le haut un traité international qui fixera des règles ; et celle, plus pragmatique, qui consisterait à mettre en place des ramifications pour dessiner un paysage de règles, en opérant par le bas, dans une logique multi-acteurs déjà propre à certaines de ces organisations, associant les ONG, les techniciens informatiques et les Gafam.

Mme Annie Blandin. - Faut-il prendre le risque d'un conflit avec les Gafam ? ou considérer plutôt que l'équilibre des pouvoirs finira forcément par se créer au fil des années ? La particularité des plateformes tient à leur emprise remarquable sur le système cognitif des individus, au-delà des services de mise en relation qu'elles fournissent. Le Conseil national du numérique ne pourra pas lutter contre la surexposition aux écrans, sans mettre en cause les entreprises au sujet de leur objectif caché de créer de l'addiction chez leurs utilisateurs.

M. Gérard Longuet, rapporteur. - En 1947, la diffusion des films à la télévision avait suscité une inquiétude en France. Le cinéma français existe toujours...

Mme Annie Blandin. - L'asymétrie de l'information et l'opacité entretenues par les entreprises sont un obstacle qu'il nous faut lever, si nous voulons que les utilisateurs puissent choisir l'acteur le plus fiable. On cite en modèle la « régulation par la donnée » de l'Arcep - qui favorise le changement d'opérateur via l'obligation d'informations claires sur les différentes offres en présence -, et la loi pour une République numérique a joué un rôle précurseur en la matière, en introduisant les principes de loyauté et de transparence entre les plateformes. Cela va de pair avec l'application optimale des règles de concurrence, alors que le règlement sur

les concentrations n'a pas de prise sur le rachat des start-ups, pour des questions de seuils, il faudrait remédier à cet angle mort.

M. Gérard Longuet, rapporteur. - Le faut-il vraiment ? Les start-ups répondent à des enjeux de profit. Ceux qui les lancent, conscients qu'ils n'auront pas forcément le succès d'un Steve Jobs, souhaitent surtout revendre au meilleur prix compte tenu de l'investissement réalisé. Si une start-up est prometteuse au point de devenir autonome, son fondateur pourra légitimement prétendre à une subvention.

Mme Annie Blandin. - C'est vrai, si l'on considère que ce sont toujours les plus riches qui rachètent les jeunes pousses.

Quand on parle de données, il faut toujours préciser s'il s'agit de données personnelles ou pas. L'obligation de localisation des données entre dans un statut général que l'on est en train de définir. Un État membre ne peut pas exiger la localisation des données non personnelles sur son territoire, et la libre circulation est la norme. Mais se pose le problème du transfert des données vers un État tiers et de leur circulation globale.

Si la propriété ne s'applique pas - et ne devrait pas, selon moi, s'appliquer - sur les données personnelles, d'autres formes de protection existent : je pense au droit spécifique qui régit les bases de données. Les questions d'accès et de partage se posent sur toutes les données non-personnelles, avec des gisements de création de valeur, notamment dans le domaine de l'environnement, qu'il ne s'agit évidemment pas de brider.

Mme Pauline Türk. - M. Mazuir regrettait avec justesse l'absence de promotion de l'équivalent d'un Airbus européen sur les questions technologiques. Manque de volonté politique, erreur stratégique, insuffisance des moyens ou manque de partenaires ? Mauvais choix de candidats, peut-être ? Il y a eu des échecs retentissants dans le cloud souverain et des acteurs à côté desquels on est sûrement passé en misant sur le mauvais champion... Nous avons les compétences technologiques, n'est-ce pas la volonté politique qui manque encore ?

M. Franck Montaugé, président. - Je vous remercie.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible en ligne sur le site du Sénat.

Audition de représentants de la commission d'éthique sur la recherche en sciences et technologies du numérique d'Allistene, l'alliance des sciences et technologies du numérique : MM. Jean-Gabriel Ganascia, Eric Germain et Claude Kirchner,
le 4 juin 2019

M. Franck Montaugé, président. - Nous entendons à présent MM. Jean-Gabriel Ganascia, président du comité d'éthique du CNRS, Éric Germain, chargé de mission « éthique des nouvelles technologies, fait religieux et question sociétale » à la direction générale des relations internationales et de la stratégie du ministère des armées, et Claude Kirchner, directeur de recherche émérite à l'Institut national de recherche dédié aux sciences du numérique.

Cette audition sera diffusée en direct sur le site internet du Sénat et fera l'objet d'un compte rendu publié. Un faux témoignage devant notre commission d'enquête serait passible des peines prévues aux articles 434-13, 434-14 et 434-15 du code pénal.

Selon la procédure applicable aux commissions d'enquête, MM. Jean-Gabriel Ganascia, Éric Germain et Claude Kirchner prêtent serment.

Vous êtes tous trois membres de la Cerna, la commission de réflexion sur l'éthique de la recherche en sciences et technologies du numérique. C'est dans ce cadre que vous avez publié en octobre 2018 un rapport sur la souveraineté à l'ère du numérique. La Cerna a étudié cette problématique sous un angle que nous n'avons que peu abordé jusqu'ici, celui des questionnements éthiques soulevés par la révolution numérique. Vous pourrez sans doute nous en dire davantage sur ces enjeux. C'est une approche d'autant plus pertinente que la ministre des Armées, Mme Florence Parly, a annoncé le 5 avril 2019 que son ministère allait se doter d'un comité de réflexion sur les implications éthiques des nouvelles technologies dans le domaine de la défense.

Dans votre rapport, vous expliquez également que la révolution numérique a bouleversé notre conception classique de la souveraineté nationale, les entreprises privées concurrençant de plus en plus les États dans l'exercice de leurs fonctions régaliennes. Vous reviendrez sans doute sur ces bouleversements et sur les moyens dont nous disposons pour y répondre. Vous invitez dans votre rapport à ne pas parler de la souveraineté numérique mais des souverainetés numériques. Il est toutefois difficile de concilier souveraineté nationale, entrepreneuriale et individuelle.

M. Claude Kirchner, directeur de recherche émérite à l'Institut national de recherche dédié aux sciences du numérique. - Je préside la Cerna depuis le 1er janvier dernier et je suis également membre du CCNE, le comité consultatif national d'éthique, pour les sciences de la vie et de la

santé. La Cerna est la commission de réflexion sur l'éthique de la recherche en sciences et technologies du numérique de l'alliance Allistene (Alliance des Sciences et Technologies du Numérique), qui regroupe l'ensemble des institutions de recherche en numérique des universités et des grandes écoles. Cette commission a été créée en 2013, à la suite de rapports du CNRS et de l'Institut national de recherche dédié aux sciences du numérique (Inria), pour aider les institutions françaises de recherche en numérique et les scientifiques qui y exercent à réfléchir aux enjeux éthiques soulevés par les recherches en sciences et technologies du numérique, tout particulièrement dans les sciences informatiques, mathématiques, électroniques et robotiques. Nous travaillons sous la responsabilité du comité de coordination d'Allistene. Nous sommes saisis, mais nous pouvons aussi nous autosaisir. Nous avons travaillé en particulier sur des questions d'éthique de la recherche en robotique ou dans l'apprentissage-machine, mais également sur les questions liées à la notion de souveraineté, en particulier à l'ère du numérique.

La réflexion éthique s'est développée depuis au moins 3 000 ans, et n'est pas neuve. Comme le disait Michel Serres, le numérique bouleverse complètement nos sociétés. Il leur procure des apports considérables, et les systèmes de traitement de l'information que nous avons créés complètent et interagissent avec les systèmes biologiques de traitement de l'information que nous sommes. Il en résulte des conflits inédits entre hiérarchies de valeurs.

Historiquement, la souveraineté désigne la capacité du souverain à maîtriser un certain nombre d'attributs dont il revendique le contrôle : frontières, armée, police, monnaie, langage, etc. Cette autonomie stratégique, ce pouvoir de pouvoir, se trouve, grâce au numérique, à la disposition d'entités nouvelles. Ainsi, la reconnaissance faciale contribue à la sécurité, mais les entreprises qui maîtrisent les algorithmes de reconnaissance et les données qui sont nécessaires à leur mise au point ont souvent une base multinationale, et échappent aux entités souveraines nationales - et leurs stratégies ne coïncident pas nécessairement avec celle d'un pays.

Les crypto-monnaies ne dépendent pas d'un État. Le contrôle aérien n'est plus nécessairement local, puisque la tour de contrôle n'est pas nécessairement sur l'aéroport et peut très bien être déportée de plusieurs dizaines, voire de plusieurs centaines de kilomètres. Le numérique impacte donc une activité de souveraineté comme la gestion du trafic aérien. Les données de santé et leur traitement ne sont plus nécessairement sous la responsabilité d'un État, ni de sa politique de santé. Les scientifiques, dans leur activité d'élaboration de connaissances et de publication, doivent être autonomes dans leur capacité à accéder aux informations qui leur permettent de faire avancer leurs réflexions et leurs travaux. Mais en fait, nombre de maisons d'édition scientifique ne permettent plus cet accès souverain aux scientifiques.

Bref, souveraineté et éthique s'articulent de manière fondamentale, car sans souveraineté, il est difficile d'élaborer une réflexion éthique qui nécessite liberté de penser, d'action et d'accès à la connaissance ; et il est impossible de mettre en oeuvre de manière claire et responsable les choix découlant de cette réflexion éthique si l'on n'a pas accès à la souveraineté.

L'*Insitute of Electrical Electronic Engineers* (IEEE) est une organisation professionnelle dont le siège est à New-York et qui regroupe environ 460 000 scientifiques et ingénieurs issus de 160 pays. Elle a plusieurs rôles, dont celui de maison d'édition. Or, dans le processus de l'élaboration de la connaissance scientifique, tout article doit être relu par des pairs. Vendredi dernier, sous prétexte des mesures protectionnistes mises en oeuvre aux États-Unis, l'IEEE a déclaré que le personnel de Huawei ne pourra plus servir d'évaluateur des contributions soumises à publication. Or, ces personnes sont membres de l'IEEE à titre personnel, en tant que scientifiques. Cette décision revenait à modifier la manière d'accepter ou non des articles sous prétexte qu'on appartient à une entreprise. Elle a provoqué un tel tollé pendant le week-end qu'elle a été retirée lundi. C'est un cas typique de manque de souveraineté scientifique : la décision est prise sans aucune concertation avec la communauté scientifique, probablement sous l'effet de certaines pressions, alors même qu'elle va à l'encontre des pratiques scientifiques usuelles.

Nous devons réinventer les notions de souveraineté et comprendre comment elles s'articulent entre elles. Le numérique dans l'agriculture pose des questions fondamentales de souveraineté, puisque les données permettent de savoir quand récolter, mais ne sont pas toujours à la disposition de tous. Nous devons aussi nous donner la capacité de penser l'éthique des sciences, technologies, usages et innovations du numérique et de l'intelligence artificielle, en allant vers la création d'un CCNE du numérique et de l'intelligence artificielle. En dehors de la Cerna, dont l'objectif est de réfléchir à l'éthique de la recherche en sciences et technologies numériques et, de façon plus large, sur l'ensemble des questionnements éthiques en termes scientifiques et technologiques, il n'y a pas d'entité en France pour réfléchir sur les usages et les innovations. Le CCNE, créé par la loi sur la bioéthique, a un objectif limité aux sciences de la vie et de la santé. L'idée est de travailler en collaboration avec lui pour voir comment faire émerger un CCNE du numérique et de l'intelligence artificielle, dont Cédric Villani a traité dans son rapport l'an dernier.

Nous devons nous donner la capacité de sensibiliser, éduquer et responsabiliser les individus, les entreprises, les institutions et les États au numérique et à ses impacts. L'éducation numérique commence à imprégner l'école, depuis le primaire jusqu'à l'Université. Ce n'est qu'un début. La capacité à maîtriser l'ensemble des systèmes numériques qui nous entourent doit être effective pour tous.

M. Jean-Gabriel Ganascia, président du comité d'éthique du CNRS. - La notion de souveraineté est toujours pertinente mais a subi des bouleversements. Le comité d'éthique sur le numérique s'est senti obligé d'aborder cette question après la loi sur la République numérique qui, en octobre 2016, envisageait la création d'un commissariat à la souveraineté numérique qui aurait été rattaché au Premier ministre, et dont les missions auraient consisté à garantir l'exercice, dans le cyberespace, de la souveraineté nationale et des droits et libertés individuels et collectifs que la République protège.

La notion de souveraineté numérique est ambiguë, comme l'a expliqué Pierre Bellanger. Il y a deux idées antagonistes derrière l'idée de souveraineté numérique. C'est pourquoi nous parlons de souveraineté à l'ère du numérique. D'une part, en effet, la souveraineté nationale connaît de nouveaux enjeux à l'ère du numérique. Pour rester souverain, un État devrait s'assurer de son indépendance en déployant des solutions informatiques à cet effet, comme par exemple un système d'exploitation souverain. D'autre part, la souveraineté elle-même se transforme à l'ère du numérique, et le numérique défie les États.

Je suis professeur d'informatique, spécialiste de l'intelligence artificielle et l'idée d'un système d'exploitation souverain me paraît contreproductive. Un tel système serait peu utilisé - et comment interdire d'utiliser des ordinateurs de la marque Apple ? De plus, du point de vue technique, le système d'exploitation n'est pas tout ! De nombreux programmes, à l'intérieur des ordinateurs, peuvent fournir de l'information. Pour éclairer le débat national, nous soulignons les difficultés qu'il y aurait à revendiquer ces solutions techniques comme étant la solution au problème posé par la souveraineté numérique. Toutefois, un effort national et européen sur la question des données serait bienvenu.

Le numérique a fait évoluer la notion classique de souveraineté nationale. Au fil de l'histoire, à partir des travaux de Bodin, Locke et Rousseau, la souveraineté a désigné la supériorité et le pouvoir sur un territoire. L'idée de souveraineté nationale est liée à celle d'autonomie de la nation, à la capacité de la nation à se doter de ses propres lois. Le numérique défie la souveraineté nationale car les réseaux traversent les frontières et permettent à des acteurs étrangers d'imposer leur loi. La co- extension du territoire et de l'État se trouve mise en défaut, et les territoires sont traversés d'influences diverses, dont l'État n'a plus la maîtrise.

Si l'on considère que la souveraineté nationale est mise en cause par les acteurs étrangers, qui défendraient leur propre souveraineté sur le territoire national, nous avons affaire à un conflit relativement classique de souveraineté, avec des armes nouvelles. Comme la France et l'Europe sont incapables d'avoir une politique claire en matière du numérique, elles se mettent sous la dépendance de grands États comme les États-Unis ou la

Chine, et sont vulnérables aux actions d'autres États, comme la Russie, qui interfèrent avec les procédures démocratiques.

On peut aussi se dire que c'est l'idée même de souveraineté nationale qui est mise en cause par le numérique. En effet, les grands acteurs de la toile que sont les moteurs de recherche ou les réseaux sociaux ont des programmes politiques. Ils ont accumulé des capitaux considérables, et souhaitent désormais promouvoir leurs aspirations libertariennes, c'est-à-dire ni libertaires ni libérales, mais prônant un désengagement total de la tutelle des États pour donner à la propriété un pouvoir absolu.

Ces grands acteurs souhaitent assumer à la place des États un certain nombre de prérogatives qui relevaient de la souveraineté, comme le privilège de battre monnaie, celui d'établir des cartes et donc un cadastre, nécessaire pour lever l'impôt, ou celui d'assurer la sécurité intérieure. La vérification d'identité se fait par la reconnaissance faciale, directement liée à la possession d'un très grand nombre de photos. Or l'État français possède des photos d'identité, mais d'assez mauvaise qualité et en nombre extrêmement limité. Et nous donnons aux grands acteurs du numérique toutes nos images... Ils peuvent aussi se développer dans le domaine de la justice, avec l'idée de justice prédictive. On pensait que la défense était un domaine réservé à l'État, mais, désormais, elle concerne aussi le cyberespace.

Si nous sommes effectivement confrontés à une nouvelle forme de souveraineté, cela signifie que nous entrerions dans une forme de féodalisme, où de multiples acteurs se partageraient le pouvoir sur des régions virtuelles, et où les États démocratiques n'auraient plus qu'une part mineure, et ancillaire, à jouer.

M. Éric Germain, chargé de mission « éthique des nouvelles technologies, fait religieux et question sociétale » à la direction générale des relations internationales et de la stratégie. - J'ai été universitaire, mais je travaille aujourd'hui pour le ministère des Armées. Je m'exprime devant vous à titre strictement personnel. Depuis dix ans, je conduis au sein de ce ministère une réflexion sur les questions religieuses et les questions de laïcité. Chez nos alliés, les aumôniers militaires sont souvent les premiers acteurs sollicités pour mener, en interne, une réflexion éthique. C'est ce qui m'a conduit, à partir de 2010, à m'intéresser aux problématiques éthiques posés par les nouvelles technologies. J'ai rejoint la Cerna en janvier 2016 à titre privé.

L'éthique, c'est le bien agir. C'est un arbitrage entre valeurs morales, un choix, contingent à un contexte particulier. L'éthique peut inspirer le droit et la loi, mais elle est elle-même difficilement codifiable car elle relève d'une appréciation dynamique, qui évolue en permanence. C'est un bien agir qui n'est pas nécessairement reproductible. L'éthique, ce n'est pas la simple conformité à un corpus de valeurs morales universelles. Elle représente aussi des cultures, avec des particularités nationales qu'il ne faut ni surestimer ni

sous-évaluer. Léopold Sédar Senghor disait qu'une culture était une manière particulière de se poser des questions, et d'y répondre.

Pour un Français, pour un Européen, l'éthique est aussi une certaine manière de se poser des questions et d'y répondre. C'est pourquoi il est si important d'être souverain en matière de réflexion éthique. C'est d'ailleurs cette prise de conscience qui est à l'origine de la création cette année par la ministre des armées, Mme Florence Parly, d'un comité d'éthique ministériel. La France est la première grande puissance militaire à s'être dotée d'une structure de réflexion permanente sur les enjeux éthiques des nouvelles technologies dans le domaine de la défense. La création de ce comité est un acte de souveraineté significatif, qui inspire dès à présent d'autres pays, et ce comité échangera nécessairement avec les autres comités qui existent déjà.

La plupart des personnes que votre commission d'enquête a auditionnées parlent d'une seule souveraineté, la souveraineté nationale, française, parfois élargie à un niveau régional comme l'Europe. Quand Pierre Bellanger parle de souveraineté numérique, il discute de l'application de la seule souveraineté nationale au domaine du numérique, et se demande comment assurer une souveraineté française sur les algorithmes ou leur paramétrage, sur l'exploitation et l'hébergement des données, etc.

Le rapport de la Cerna ne parle pas directement de souveraineté numérique mais bien de souveraineté à l'ère du numérique, en partant du constat que les technologies bouleversent le sens même du mot « souveraineté », et la nature des acteurs, qui ne se limitent plus aux États mais s'élargissent aux entreprises, aux communautés professionnelles, scientifiques, voire à une échelle individuelle.

Le pas de côté que nous avons fait en rédigeant ce rapport nous a montré que les Gafami (Google, Apple, Facebook, Amazon, Microsoft et IBM), par exemple, ne sont pas simplement un nouveau genre d'auxiliaire de la souveraineté nationale américaine. Ces sociétés revendiquent une souveraineté propre, distincte de celle des États. L'enjeu est de comprendre les interactions nouvelles qui sont nouées et de voir comment on peut les concilier avec les valeurs de notre République.

Le chapitre 3.2 parle de l'immixtion, ou de l'ingérence, de sociétés commerciales du numérique dans notre vie démocratique. C'est le domaine assez préoccupant de l'influence sociale et de l'initiative citoyenne. Autre enjeu : la souveraineté scientifique. Nous l'abordons dans le chapitre 4.3. La liberté de formuler des questions, y compris des questions éthiques, naît d'un principe de science ouverte qui est aujourd'hui contesté par la privatisation croissante des données scientifiques. Nous avons parlé de souveraineté individuelle, là où les puristes parleraient plutôt d'autonomie du sujet ou de libre arbitre. L'expression « être souverain à soi-même » a déjà été employée il y a près de deux siècles par l'immense esprit français que fut votre collègue, représentant de la Nation, Félicité Robert de Lamennais. Il

traduisait l'expression utilisée par Dante dans *La Divine Comédie.* Cet attachement très individualisé à la liberté de penser est peut-être le trait essentiel de notre identité européenne - une singularité dont le numérique nous rappelle aujourd'hui toute l'importance.

La conclusion du chapitre 3.3, comme plusieurs recommandations du rapport de la Cerna, évoque cette souveraineté numérique nationale que l'on peut reconquérir par le bas, au niveau de chaque individu, qu'il faudrait davantage éduquer et sensibiliser.

M. Gérard Longuet, rapporteur. - Merci de la qualité de vos interventions, qui apportent un éclairage éthique passionnant, surtout au sein d'une assemblée de parlementaires élus au suffrage universel, qui ont à rendre compte de leurs réflexions et de leurs travaux à nos compatriotes. Ceux-ci se tournent vers le pouvoir politique en se demandant si ce dernier a encore les moyens de ses ambitions - s'il a encore la capacité d'agir. Nos réflexions sur la souveraineté numérique nous conduisent à nous demander quels choix politiques le Parlement pourrait imaginer, pour chaque groupe, dans le débat législatif.

Il me semble que tout ce qui est numérisé a vocation à être connu, par les uns ou par les autres, sans qu'on sache exactement selon quelles règles. Les lois de bioéthique ont été récemment soumises à l'Office parlementaire d'évaluation des choix scientifiques et technologiques (OPECST), que je préside. Elles rendent le séquençage du génome accessible. Or qui dit diffusion de masse dit utilisation de masse. Nous sommes là au coeur de la souveraineté politique : l'analyse génétique est prescrite, alors qu'elle risque d'être, *proprio motu* en quelque sorte, diffusée, notamment par des hypocondriaques, dupés par n'importe quel marchand de facéties.

Je trouve passionnant de rencontrer quelqu'un qui s'occupe de l'éthique à l'armée. J'ai toujours pensé que l'armée pouvait faire son métier parce qu'elle avait une culture ancienne, solide et mâtinée d'expérience - frottée à l'épreuve des faits. Cela lui confère la résignation nécessaire pour accepter ce que l'opinion, émotive et immédiate, n'accepterait pas, par exemple, le fait que le feu tue, célèbre expression de la Première guerre mondiale, que nos compatriotes oublient lorsqu'ils demandent des interventions militaires et s'étonnent que celles-ci soient coûteuses, pour nous ou pour les autres.

Un sujet qui mériterait d'être approfondi est celui des diversités culturelles, et des particularités sociologiques ou nationales qui doivent nous faire regarder la souveraineté à l'époque du numérique comme étant d'une nature différente. Prenez par exemple la sécession des classes dirigeantes, thème bien connu de Jérôme Fourquet. Une fraction de nos compatriotes a considéré que l'accès à une pleine liberté numérique est un droit personnel absolu, ce qui n'en fait pas pour autant des libertariens ou des libéraux à l'américaine. On en voit des exemples pittoresques en Californie : certains

n'accepteront pas d'être censurés ou encadrés dans leur accès à la connaissance et aux données. Cela ne les empêchera pas de se retourner vers l'État en lui reprochant de ne pas assurer la sécurité. La légitimité de l'État, qui nous impose de respecter la loi et qui nous fait payer beaucoup d'argent pour financer son fonctionnement, est en effet d'abord d'assurer la sécurité.

En France, si l'on excepte le cas très particulier du terrorisme, la probabilité d'être envahi par un ennemi agressif est à peu près nulle. La sécurité, on veut bien la payer, à condition qu'elle soit totale. Or elle touche justement ces secteurs. Il y a donc des catégories qui, s'estimant dispensées de respecter une éthique du numérique, n'hésiteront pas à solliciter l'aide de l'État pour les sécuriser et les protéger contre toute offensive.

Quels ont été les effets de votre rapport ? Vous évoquez la création d'un commissariat à la souveraineté numérique. Comment définiriez-vous votre rôle par rapport à d'autres institutions existantes ? Nous avons reçu notre ambassadeur du numérique, vous avez évoqué M. Bellanger, un autodidacte du numérique passionné et très convaincant - et parfois inquiétant par les solutions qu'il préconise, qui conduisent à un cryptage généralisé. Quant à vous, défendez-vous une ligne - le souhaitez-vous ? Comment la Cerna envisage-t-elle son rôle dans un système français plus marqué par l'organisation de colloques que par l'investissement résolu dans les projets ? Vous êtes des scientifiques : existe-t-il selon vous une communauté européenne, les échanges sont-ils courants en Europe, une ligne directrice se dégage-t-elle ?

M. Hugues Saury. - Quel réconfort d'entendre parler d'éthique dans un secteur, le numérique, qui évoque plutôt le far-west ! L'intelligence artificielle est présentée comme une technologie clé pour l'avenir économique et social, elle pourrait nous permettre de restaurer une forme d'indépendance - l'Union européenne a adopté une stratégie, des lignes directrices, pour la recherche comme pour la vie des entreprises. Avez-vous travaillé sur ces propositions éthiques ? L'Europe, avec ses valeurs fortes, en décalage par rapport au far-west, peut-elle être néanmoins concurrentielle ?

M. Franck Montaugé, président. - Vous avez évoqué dans le rapport l'enjeu de la privatisation des données scientifiques. Le développement du *big data* et des méthodes d'analyse pour les exploiter ne remet-il pas en cause la méthode scientifique que l'on a connue jusqu'à présent, et qui a fait de l'homme ce qu'il est ?

Entrevoyez-vous dans le développement de l'intelligence artificielle - au sens où vous l'étudiez, dans une acception plus large que l'exploitation des données de masse - la possibilité de créer une autre pensée métaphysique ? Je pense, à la suite de certains auteurs, que la métaphysique est le propre de la pensée humaine. Une intelligence artificielle pourrait-elle remettre en cause la spécificité de l'être humain sur terre ?

M. Claude Kirchner. - Premier effet du rapport : lorsqu'a émergé la notion de souveraineté numérique, elle a suscité un questionnement chez les scientifiques. Le rapport a été une manière de coucher sur le papier l'ensemble de nos réflexions. C'est à ce jour le seul document, en français et en anglais, de ce genre. Il a été repris par le Comité consultatif national d'éthique lorsqu'il s'est intéressé aux données massives. C'est un document qui nous aide à progresser dans la compréhension d'une notion fondamentale, déclinée à présent à tous les niveaux, individuel, économique, environnementale, etc. La Cerna a émis des recommandations scientifiques - disponibilité des données, concept de souveraineté scientifique, maîtrise des données de travail comme condition d'une recherche au meilleur niveau international... Notre rôle concernait seulement la recherche, mais dès lors que nous avons exploré bien d'autres domaines, nous avons formulé sur ces derniers non des recommandations mais des suggestions d'évolution, reprises par diverses instances.

La maîtrise des données, des algorithmes, des systèmes d'information exige de mettre en place une cyber-sécurité au profit de l'entité qui a besoin de maîtriser ces données. Cela commence au niveau individuel : où sont conservées les photos de famille, qui y a accès, combien de temps, et pour quoi faire ? Nous avons des capacités robustes pour développer une cyber-sécurité. Il n'y a certes pas de sûreté absolue. Les informations chiffrées sont aujourd'hui difficiles à déchiffrer en quelques secondes. Mais, dans cent ans, on saura le faire instantanément. Il importe de prendre en compte la durée pendant laquelle on peut assurer la sécurité des données.

On met en oeuvre aujourd'hui des techniques de chiffrage homomorphe. Une fois les données chiffrées, les calculs ne portent pas directement sur, par exemple, l'âge et le taux de cholestérol, mais sur A et B - si l'on possède les clés de déchiffrement, on peut lire les résultats ; mais une entité peut être chargée de faire tous les calculs souhaités sans disposer de ces clés ; le coût en calculs est élevé, mais on sait le faire, du moins lorsqu'il s'agit d'opérations simples, multiplication, soustraction. Pour calculer un sinus, un cosinus, il en va autrement... C'est en tout cas une piste intéressante, que la recherche pourrait explorer : au lieu de machines souveraines, on pourrait recourir à des machines travaillant sur des objets chiffrés, dont seul le commanditaire aurait la clé.

M. Franck Montaugé, président. - Celui qui travaille sur les données ne les connaît pas.

M. Claude Kirchner. - C'est cela. Il effectue des opérations sur des chiffres. Le propre du chiffrage homomorphe, c'est que des opérations standard sont applicables aux données une fois chiffrées.

M. Gérard Longuet, rapporteur. - On pourrait alors employer des systèmes mondiaux tout en conservant la maîtrise des données ?

M. Claude Kirchner. - Oui, mais ces algorithmes sont difficiles à déchiffrer aujourd'hui, il faudrait y consacrer beaucoup de capacités. Il faudrait aussi approfondir les recherches afin que les processus de chiffrage puissent s'appliquer à des fonctions plus nombreuses. La France travaille sur ces sujets, ses équipes sont remarquables.

Concernant l'accès aux données ou la protection de celles-ci, une éducation s'impose. Qui sait qu'utiliser une adresse numérique gratuite non chiffrée, gmail par exemple, mais également répondre à un gmail, revient à confier au facteur une carte postale sans enveloppe ? Le facteur ne lit pas toutes les cartes, mais Google a, lui, la capacité de lire tous les mails et d'en tirer toutes les informations.

Toute personne peut prétendre : « mon génome m'appartient ». En réalité, celui-ci est hérité et appartient aussi aux ascendants et aux descendants. En envoyant 200 dollars et un peu de salive aux États-Unis, à *23andMe*, cette personne connaîtra une grosse partie de son génome. Elle le conserve pour elle, ou accepte de le publier en ligne - alors, elle expose les données de toute sa famille

M. Gérard Longuet, rapporteur. - Et surtout de ses descendants. C'est le plus grave !

M. Claude Kirchner. - Vous nous interrogez sur la communauté scientifique numérique européenne. Elle est en train de se constituer, avec des associations professionnelles comme le *European research consortium for informatics and mathematics* (Ercim), qui regroupe 16 ou 17 entités de recherche, ou *Informatics Europe*.

M. Gérard Longuet, rapporteur. - Les scientifiques ont-ils envie de travailler ensemble en Europe ?

M. Claude Kirchner. - Oui, et ils le font depuis trente ans !

Quelques mots de la privatisation des données scientifiques. Le numérique est un outil exceptionnel. On peut aujourd'hui, par la simulation, faire exploser des galaxies en laboratoire ! On analyse un nombre immense de données. Cela ne détruit pas la méthode scientifique ancienne : la recherche demeure fondée sur l'observation, le modèle, les tests et les conclusions. La nouvelle capacité de calcul, de simulation, d'exploration vient en complément, non en substitut, du raisonnement inductif ou déductif. Elle l'enrichit. Comment en faire un bien commun ? Telle est la question. Comment faire pour que les données, les algorithmes, les résultats scientifiques ne soient pas captés, par des éditeurs par exemple ? Le ministère de l'enseignement supérieur et de la recherche, ou le Comité pour la science ouverte, qui coordonne en France les instituts et universités, s'y emploient.

M. Jean-Gabriel Ganascia. - Imaginer une pensée métaphysique produite par l'intelligence artificielle, c'est envisager que la machine prenne

son autonomie et nous échappe. C'est une question très populaire, sur laquelle je me suis penché. J'ai écrit un petit livre pour répondre à la théorie de la singularité technologique, qui laisse imaginer que l'on pourra télécharger son esprit pour devenir immortel, ou que la machine deviendra à terme plus puissante que l'homme. Les arguments avancés par les tenants de cette thèse n'ont pas de valeur scientifique. Ils reposent sur la loi de Moore et l'accélération du pouvoir des machines. Mais que celles-ci soient de plus en plus rapides ne signifie pas qu'elles soient conscientes. Elles ingurgitent plus de connaissances que l'homme n'est capable d'en apprendre tout au long de sa vie ; elles n'en deviennent pas autonomes. L'apprentissage est supervisé par l'homme. La machine condense un savoir humain, rendant ainsi des services considérables, mais elle ne peut tout faire toute seule. La rupture épistémologique au sens de Bachelard signifie que les concepts évoluent : pas la machine.

Quant à savoir si l'intelligence artificielle est dangereuse comme le prétendent de grands acteurs de l'internet...

M. Gérard Longuet, rapporteur. - Cela renvoie au transhumanisme.

M. Jean-Gabriel Ganascia. - Si des fabricants de cigarettes affirment que le tabac est nocif, il faut s'interroger sur les motivations d'un tel discours ! Susciter une grande peur peut servir à masquer la réalité. Des groupes d'activistes ont ainsi persuadé les députés européens de voter une résolution sur les systèmes d'armes létales autonomes, autrement dit les robots tueurs. Cela a conduit certains des parlementaires européens à recommander à la Commission européenne de ne pas financer des programmes tendant à inclure de l'intelligence artificielle dans les systèmes de défense - ce qui pose un problème dramatique à la fois pour l'industrie de l'Europe et pour sa sécurité ! Le masque de l'éthique peut dissimuler les agissements, en l'occurrence de grands acteurs européens ou israéliens, ou de tout autre concurrent au plan mondial...

Sur la privatisation des données, l'enjeu est considérable du point de vue de la souveraineté. Sur le problème d'épistémologie que vous avez soulevé, je ne suis pas complètement d'accord avec mon collègue. Je dirai pour ma part que les techniques d'apprentissage détectent des corrélations, pas des causalités. On nous dit qu'il n'y a plus de modèle, plus de théorie, plus de langage : c'est faux, et Google nuance son discours quand on le pousse dans ses retranchements.

Je suis sensible à la question des peurs et de l'éthique. Les grandes transformations provoquées par l'intelligence artificielle ne sont pas métaphysiques mais politiques, car le numérique transforme tout. On peut parler de « réontologisation » : l'amitié se transforme avec les réseaux sociaux, la réputation avec les *reputation score* comme en Chine, la confiance avec la *block chain*... C'est la même chose pour la souveraineté. Il convient de prendre en compte ces transformations qui induisent des vulnérabilités.

Aucun de nous trois n'a pas fait partie du groupe des experts de haut niveau chargé de définir des lignes directrices au niveau européen, mais un de nos collègues de la Cerna y siégeait. En novembre dernier, nous étions perplexes devant la première rédaction, marquée par une éthique reposant sur les principes anciens de la communauté européenne. Adopter une démarche éthique, n'est-ce pas plutôt se poser des questions ? Quant à « adopter une approche centrée sur l'homme », je suis étonné, et même gêné, car y en a-t-il une autre ? Les machines sont des systèmes sociaux-techniques pensés à l'intérieur de la société dans laquelle ils naissent.

J'en viens à la sécurité. On ne peut plus parler de dilemme, désormais, mais de trilemme : aux deux exigences également légitimes qui entrent traditionnellement en conflit, protection de la vie privée et sécurité, vient s'ajouter une troisième notion, la transparence, qui entre en conflit avec chacune des deux premières. Transparence pour les puissants, protection pour les pauvres : c'est une fable ! On peut être aux deux places. Je songe à un instituteur, dont on veut connaître les moeurs privées, pour vérifier qu'elles sont compatibles avec l'éducation des enfants... Il y a donc des tensions entre des exigences contraires, et il faudra bien convaincre la société que des choix sont inévitables - il faut les faire collectivement.

M. Eric Germain. - Créer une nouvelle pensée métaphysique ? C'est bien plutôt l'ancienne que l'on retrouve à l'occasion des nouvelles interrogations, je songe, par exemple, à la dignité de l'être humain, notion profondément ancrée en chacun de nous, propre à notre culture européenne.

Premier effet du rapport : nous avons pris le temps de travailler comme rarement, en partant de la notion de souveraineté, en remettant en question toutes nos idées sur la souveraineté, dans tous ses aspects. Ce n'est pas un hasard si en France on parle beaucoup d'éducation : celle-ci recèle un enjeu majeur de responsabilité collective, un devoir à l'égard de l'ensemble des citoyens ; elle recouvre bien un domaine de souveraineté. Outre-Manche, la notion suscite un moindre attachement.

Parler de far-west au sujet de l'Europe est judicieux. Le groupe européen d'experts était lui-même très influencé par une approche far-west de l'éthique, opposant bien et mal, bons et méchants, de manière très manichéenne, alors que les valeurs en présence sont en conflit les unes avec les autres, et même avec elles-mêmes : la transparence est à la fois bonne et mauvaise ! La réflexion éthique doit porter sur ces tensions. Tel le raisonnement militaire, qui définit une cible et des moyens de l'atteindre, il faut aller vers ce que l'on a défini comme un avenir commun désirable.

Un groupe essentiellement au service d'intérêts privés crée un label éthique en noir et blanc, comportant des cases à cocher : trop simple ! L'éthique, c'est autre chose : un effort constant, politique, pour aller vers un futur commun désirable. Nous posons la question : la souveraineté pour

faire quoi ? Être souverain, c'est avoir la possibilité d'être libre. Ce n'est pas rien !

M. Franck Montaugé, président. - Vous avez aujourd'hui fait la démonstration que la science, lorsqu'elle rime avec conscience, enrichit l'âme. Nous vous en remercions.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible *en ligne sur le site du Sénat*.

Audition de MM. Thomas Courbe, directeur général des entreprises et commissaire à l'information stratégique et à la sécurité économique, et Mathieu Weill, chef du service de l'économie numérique à la direction générale des entreprises (DGE),
le 12 juin 2019

M. Franck Montaugé, président. - Notre commission d'enquête poursuit ses travaux avec l'audition de MM. Thomas Courbe et Mathieu Weill. Cette audition sera diffusée en direct sur le site Internet du Sénat et fera l'objet d'un compte rendu publié. Je rappelle, pour la forme, qu'un faux témoignage devant notre commission d'enquête serait passible des peines prévues aux articles 434-13, 434-14 et 434-15 du code pénal.

Conformément à la procédure applicable aux commissions d'enquête, MM. Thomas Courbe et Mathieu Weill prêtent serment.

En vos qualités respectives de directeur général des entreprises et chef du service de l'économie numérique de cette direction, au sein du ministère de l'économie et des finances, vos services sont chargés de la réglementation du numérique et de la conception et de la mise en oeuvre des politiques industrielle et d'innovation. Ils produisent donc de la norme, mais ils mettent également en oeuvre des politiques publiques.

De plus, monsieur Courbe, en tant que commissaire à l'information stratégique et à la sécurité économique (« Cissé »), vous êtes chargé de la politique de sécurité économique. Comme le rappelle le décret du 20 mars 2019 relatif à la gouvernance de la politique de sécurité économique, votre mission à ce titre « inclut la défense de la souveraineté numérique ».

Je commencerai donc par vous demander comment vous appréhendez cette notion de souveraineté numérique et, en tant que Cissé, quel est votre plan de bataille sur ce sujet.

S'agissant de la conduite de la politique économique et industrielle, il semble que la notion de souveraineté suppose qu'un État soit souverain sur les technologies clés de l'ensemble de la chaîne du numérique. Le Président de la République a lancé une stratégie nationale au printemps 2018 sur l'une d'entre elles : l'intelligence artificielle. À ce jour, quelle est la feuille de route de la direction générale des entreprises (DGE)sur le sujet ? Où en est la réflexion relative à la création de « communs des données » par secteur économique ?

Le Gouvernement essaie aujourd'hui de créer, avec l'Allemagne, un géant européen des batteries. Menez-vous également des réflexions sur de potentiels géants à faire émerger sur l'ensemble des couches numériques ?

M. Thomas Courbe, directeur général des entreprises, commissaire à l'information stratégique et à la sécurité économique. - Merci de votre invitation. Avec la numérisation de l'économie, la souveraineté numérique

est devenue une part importante de la souveraineté économique. Elle se définit par la capacité d'un pays à maintenir son indépendance dans le monde numérique grâce à deux leviers principaux.

Le premier consiste à définir des règles répondant à un objectif de souveraineté économique en matière de sécurité, de valeurs et de partage de la valeur dans l'économie. Le second consiste à maîtriser les technologies.

La production de règles s'applique d'abord à la sécurité. La DGE a ainsi pris des mesures pour les interceptions légales dans le cadre des objectifs de sécurité et pour la sécurité des infrastructures de télécommunications. C'est un sujet d'actualité au niveau mondial, en particulier avec l'arrivée de la 5G qui va rendre les réseaux beaucoup plus critiques qu'auparavant. En imposant un régime d'autorisation des équipements déployés par les opérateurs, la proposition de loi en cours de discussion sur la sécurité de ces réseaux, sera, si elle est adoptée, une contribution essentielle à notre souveraineté numérique.

La DGE contribue également à la réflexion sur un enjeu relatif aux valeurs fondamentales de notre société appliquées au domaine numérique. Le Président de la République a missionné une équipe pour travailler avec Facebook à des recommandations de régulation des plateformes en ligne. Ses conclusions nous semblent pertinentes et applicables à d'autres champs, en particulier au champ économique.

En effet, la régulation doit permettre d'assurer un partage équitable de la valeur, car le numérique se caractérise par une concentration de celle-ci dans les mains d'un petit nombre d'acteurs qui, à la faveur des effets de réseau, acquièrent une dimension systémique. Le débat sur la régulation a lieu à la fois aux niveaux français, européen et mondial. La présidence française du G7 a ainsi porté certaines propositions dans ce domaine.

Quant à la maîtrise des technologies, second volet de la souveraineté numérique, elle repose en premier lieu sur une politique industrielle du numérique consistant à soutenir les acteurs susceptibles de les développer. La France a un écosystème de l'innovation très riche ; nous nous efforçons de le stimuler en aidant les entreprises à grossir. Le nombre de licornes, ces *start ups* dont la valorisation est supérieure à un milliard d'euros, a augmenté significativement, mais il reste insuffisant. Nous travaillons à l'accompagnement des entreprises les plus prometteuses, à leur financement pour les aider à atteindre une taille critique et à l'attraction des talents.

En second lieu, l'objectif de maîtrise des technologies repose sur une politique industrielle ciblée sur les technologies identifiées comme essentielles. Première de ces technologies, les semi-conducteurs, secteur dans lequel le maintien d'acteurs de dimension internationale est essentiel. C'est un point traité dans le plan Nano 2022. Deuxième secteur identifié, le super-calcul, élément important de la souveraineté numérique, dont Atos est l'un des leaders et participe au programme européen EuroHPC. Le troisième

secteur est l'intelligence artificielle. Le volet économique de la stratégie nationale sera présenté le 3 juillet par le ministère de l'économie et des finances et le secrétariat d'État au numérique.

Dans le cadre du Pacte productif 2025, nous cherchons à compléter l'identification des technologies clés au-delà des domaines cités, en nous assurant que nous aurons des entreprises capables de porter ces technologies. Nous avons d'ores et déjà identifié le *cloud* de confiance. Dans le domaine du *cloud*, il est difficile d'envisager une offre française ou européenne susceptible de rivaliser avec ses homologues américains. En revanche, il nous semble possible, comme dans différents autres secteurs, de développer une offre française qui se différencierait par les valeurs qu'elle porte et la sécurité qu'elle garantit en matière de protection des données - c'est le cas du *cloud* de confiance -, en particulier des données personnelles - c'est le cas des moteurs de recherche intégrant le *privacy by design.* . Les solutions d'intelligence artificielle pourraient également se différencier dans un certain nombre d'applications par des éléments d'auditabilité et de redevabilité. L'algorithme d'un véhicule autonome devrait ainsi faire l'objet d'une certification pour assurer la confiance des utilisateurs. Sur certains segments, il sera donc possible de rivaliser avec des concurrents plus avancés grâce à cette différenciation de l'offre.

En revanche, il est certains domaines où la France ou l'Europe ne pourront pas rivaliser, en particulier sur les fonderies de microprocesseurs. Dans ce cas, la souveraineté sera garantie par la diversification des sources et la sécurité des approvisionnements.

Cette politique industrielle se complète d'un volet plus défensif consistant à identifier notre patrimoine et nos actifs économiques stratégiques, notamment à travers les technologies maîtrisées. C'est le travail mené par le Service de l'information stratégique et de la sécurité économiques (Sissé), qui anticipe les menaces sur ce patrimoine, à commencer par les projets d'acquisition par des acteurs étrangers, et met en oeuvre des outils de protection. Ceux-ci ont été renforcés, notamment par la loi Pacte grâce à l'élargissement du dispositif de contrôle des investissements étrangers aux domaines de la cybersécurité et du stockage de données. Il faut également faire évoluer nos outils face à l'évolution des menaces. Dans le cadre d'un rapport prochainement présenté sur le *Cloud Act* américain qui donne aux agences américaines un accès excessivement large aux données hébergées dans le *cloud*, le député Raphaël Gauvain recommandera une adaptation de la loi de blocage de 1968.

C'est une problématique qui a profondément évolué, dans le sens d'une interpénétration entre des problématiques régaliennes, économiques et sociétales. La place des États est désormais bien acceptée par les acteurs dans ce domaine, comme le montrent les récentes déclarations de Mark Zuckerberg. Enfin, l'*executive order* pris le 15 mai par le président Trump et les décisions contre Huawei montrent le caractère mondial de ces enjeux.

M. Gérard Longuet, rapporteur. - Vous avez mentionné parmi vos missions la production de règles, notamment pour la sécurité des informations dans les réseaux de télécommunications. En quoi la 5G est-elle différente des générations précédentes ? L'hostilité des États-Unis envers Huawei relève-t-elle à vos yeux du principe de précaution ou s'inscrit-elle dans le cadre de leur relation bilatérale, parfois conflictuelle, avec la Chine ?

Vous avez également évoqué la mission Facebook. La réception de Mark Zuckerberg par le Président de la République a été très médiatisée, à juste titre sans doute mais certaines des personnes que nous avons entendues ne perçoivent pas l'intérêt d'une régulation conjointe entre les États et les plateformes elles-mêmes. Le ministère de l'intérieur négocie-t-il des accords avec les trafiquants de drogue pour une distribution raisonnable de leurs produits ? Ne faudrait-il pas une régulation plus autoritaire ?

Concernant le partage de la valeur, avec la vision transversale de la DGE, que pensez-vous de cette économie insolite du numérique où tout est gratuit en apparence ? En réalité, l'argent rentre, et dans des conditions qui favorisent la concentration de la marge sur un petit nombre de très grands acteurs au détriment des plus petits, notamment à cause d'une politique d'acquisition des *start ups* au détriment de la concurrence.

Pouvez-vous préciser les propositions de la présidence française du G7 dans le domaine numérique ? De même, pouvez-vous détailler les lignes de force du plan Nano 2022 ?

Concernant le *Cloud* de confiance, nous ne savons pas bien où nous allons. Le président d'Atos a estimé, lorsque nous l'avons entendu, qu'il représenterait au maximum 20 % du stockage de données ; en revanche, il a évoqué l'*edge computing*. Pouvez-vous nous éclairer sur cette notion ?

Enfin, quels sont les goulots d'étranglement et les positions de monopole qui pourraient menacer la sécurité des approvisionnements ? Comment les contourner ? La presse se fait abondamment l'écho du contrôle par la Chine de la production de terres rares. Autre exemple, les câbles sous-marins sont-ils considérés comme stratégiques, et les problèmes de sécurité, d'atterrage et de connexion sont-ils assez maîtrisés pour que nous ne dépendions pas des acteurs américains ?

M. Thomas Courbe. - Les réseaux 4G avaient pour vocation de transporter de la voix et des données ; la 5G permettra, grâce à des temps de latence très faibles dans la transmission, la connexion directe d'objets entre eux. Ce temps de latence sera par exemple compatible avec le temps de réaction d'un véhicule autonome en situation de risque. Mais l'intégration de la 5G donnera à de nombreux sites industriels une dimension critique : avec des usines, des hôpitaux connectés, nous ne pourrons nous permettre aucune défaillance de réseau.

Concernant Huawei, je ne pourrai donner qu'une réponse partielle. La France a choisi une option différente de celle des États-Unis, prévue par la

proposition de loi que j'ai évoquée. Il s'agit d'un régime d'examen au cas par cas des équipements de 5 G, au regard de nos objectifs de sécurité. Les autorités américaines ont souhaité intégrer ce sujet dans les négociations commerciales, ce qui confirme bien la dimension commerciale du sujet.

La *smart regulation* ou régulation agile nous semble adaptée aux acteurs systémiques. D'abord, l'expérience montre que la prévention est plus efficace que la répression, qui arrive généralement longtemps après le dommage, sous forme d'amendes peu dissuasives. Il est préférable de fixer des règles, des objectifs, par exemple en matière de mise à disposition des données et de non-discrimination entre les acteurs, avec un régulateur qui s'assure que ces objectifs sont atteints. C'est une régulation par le résultat, et non par les moyens, qui pourrait s'articuler avec un renforcement du droit de la concurrence : une régulation conjointe plutôt qu'autoritaire, dans un contexte de grande asymétrie d'information au bénéfice du régulé.

M. Gérard Longuet, rapporteur. - En l'espèce, le régulé a une dimension mondiale, et nous aurons des accords de régulation nationaux...

M. Thomas Courbe. - Il serait souhaitable de mettre en oeuvre, *a minima*, une régulation européenne. Le projet de règlement *Platform to Business*, qui vient d'entrer en vigueur, est un premier pas dans cette voie. Cela n'empêche pas les États membres de mettre en oeuvre de premiers étages de régulation, comme la proposition de loi Avia en France. Nous sommes en discussion avec les plateformes de commerce électronique : une régulation d'équité au plan national dans ce domaine, garantissant à nos PME une absence de discrimination et une transparence satisfaisantes, aurait du sens. Il est également utile d'avancer au niveau national pour convaincre nos partenaires européens de la nécessité d'une régulation.

Deux risques principaux pèsent sur le partage de la valeur. Le premier est celui des acquisitions prédatrices, c'est-à-dire la pratique consistant, pour les grandes plateformes systémiques, à acheter des concurrents pour les fermer quelques mois plus tard. Le second est la publicité en ligne, marquée par un pouvoir de marché croissant des grandes plateformes au détriment d'acteurs plus classiques de l'économie, notamment des médias. Ces enjeux peuvent être systémiques. Chaque champ et chaque modèle économique du numérique appellent une régulation adaptée pour lutter contre les effets de réseau et les positions dominantes. Nous réfléchissons, avec les acteurs de la publicité en ligne et les places de marché, à une régulation de ces deux secteurs. Contre les acquisitions prédatrices, il convient de rendre plus efficaces les règles de la concurrence. Sur ce point, nous sommes en ligne avec la Commission européenne.

La présidence française du G7 a proposé une charte sur les contenus pour obtenir des plateformes un filtrage ou un retrait rapide des contenus haineux par exemple. Elle a également avancé, conjointement avec le

Canada, la proposition d'un GIEC (Groupe international des experts sur le climat) de l'intelligence artificielle : un panel d'experts indépendants et reconnus de ce domaine susceptibles de guider les États dans leur réflexion, notamment au plan éthique.

M. Gérard Longuet, rapporteur. - Est-ce une bonne idée ? Ces organismes internationaux finissent par acquérir une autonomie telle que l'on peut s'interroger sur leur responsabilité. Le GIEC mobilise des milliers d'experts, mais leurs conclusions sont filtrées par les représentants des États, qui sont des visions politiques ; cela aboutit à des recommandations où chacun trouve son compte. Un organisme international réfléchissant en autonomie finit par ne rendre compte qu'à lui-même, entretenant une dynamique qui peut tendre vers un discours apocalyptique. Dans le domaine de l'intelligence artificielle, la tentation est de diffuser, *via* ces experts en totale autonomie, une vulgate obligatoire mondiale.

M. André Gattolin. - Ces propos n'engagent que le rapporteur !

M. Gérard Longuet, rapporteur. - J'en conviens sans difficulté.

M. Mathieu Weill, chef du service de l'économie numérique, direction générale des entreprises. - Ce concept de GIEC de l'intelligence artificielle a été mis en avant pour marquer les esprits. Certains pays sont réservés. Il n'est pas acquis qu'un dispositif de ce type sera adopté, mais nous avons besoin d'un organisme doté d'une assise scientifique forte, susceptible d'anticiper les problématiques économiques et sociales qui émergeront avec le développement de l'intelligence artificielle. Cette réflexion se poursuivra jusqu'au sommet de Biarritz.

M. Thomas Courbe. - Troisième action de la présidence française du G7, un échange sur la sécurisation des réseaux de télécommunications, domaine dans lequel nous voyons les grands pays prendre des options différentes.

L'objectif du plan Nano 2022 consiste, pour conserver la maîtrise de certaines technologies clé, à maintenir en Europe et en France des acteurs stratégiques, comme STMicroelectronics et Soitec pour les semi-conducteurs, en particulier en vue de certaines applications comme l'intelligence artificielle embarquée. Dans ce domaine, qui combine étroitement le logiciel et le physique - au point que l'on parle de systèmes cyberphysiques, nous pensons être en mesure de faire émerger des champions sur ce marché naissant, notamment sur la partie matérielle de cette industrie, alors que nous aurons des difficultés à rivaliser en matière d'intelligence artificielle pure.

L'ordinateur quantique est un enjeu identifié à moyen terme. Une stratégie nationale sera prochainement présentée dans ce domaine où il est important d'investir, à travers le soutien à la recherche et la préparation de l'émergence d'acteurs nationaux.

De plus en plus d'acteurs, particuliers et entreprises, sont sensibles au risque lié à la protection de leurs données sur le *cloud*. Ces inquiétudes sont aggravées par le *Cloud Act* qui, en s'appliquant à toute donnée gérée par une entreprise américaine, quelle que soit la localisation du serveur, crée une grande incertitude sur la maîtrise de la donnée. Il y a là un marché qui pourrait répondre aux besoins des entreprises, mais aussi de l'État et des collectivités, et nous avons en France des acteurs susceptibles de développer des offres en ce sens.

Enfin, nous avons pris des mesures fiscales pour rendre plus compétitive la création de *data centers* en France. Nous travaillons sur ce sujet avec la filière des industries de sécurité, pour développer des solutions répondant à ces enjeux et nous assurer que les investissements des entreprises seront justifiés par l'émergence d'un marché. En l'espèce, nous pensons être dans cette configuration, contrairement à de précédentes initiatives.

M. Hugues Saury. - La décision du président américain contre Huawei a-t-elle un impact sur notre industrie, en particulier le secteur des semi-conducteurs ? A-t-elle mis en évidence des faiblesses au niveau européen ? L'Europe ne sera-t-elle pas un spectateur de cette guerre économique ? Enfin, je souhaiterais des précisions sur l'idée que l'offre française se distinguera par les valeurs qu'elle porte.

M. André Gattolin. - Il faut aussi que le traitement des données soit territorialisé, et que des portes dérobées ne soient pas introduites dans nos machines : le cas s'est produit avec certains microprocesseurs. Voici quelques années, je m'étais étonné de voir que Bpifrance stockait ses données dans un *cloud* Microsoft ; on m'avait répondu qu'il était trop cher d'aller ailleurs. Peut-on garantir que nos grandes institutions, qui travaillent à la réception, à l'analyse, à l'accompagnement de projets stratégiques, sont protégées ?

M. Thomas Courbe. - L'impact de la décision américaine semble limité, pour les fournisseurs comme les clients français de Huawei. Nous sommes en train d'envisager, avec les entreprises concernées, les moyens de le réduire.

Les valeurs que pourrait porter l'offre française sont la sécurisation des données pour le *cloud*, le caractère auditable et certifiable et le respect des droits fondamentaux. Pour l'intelligence artificielle ces valeurs seraient intégrées *ab initio* dans la conception des algorithmes. Nous avons lancé un grand défi d'innovation de rupture sur cette question.

La protection des institutions dans le cadre du *cloud* sécurisé se décline en plusieurs phases : d'abord la stratégie *cloud* de l'État, ensuite la définition des données sensibles, avant d'envisager, en concertation avec les acteurs et sous réserve d'une offre française compétitive, d'imposer des obligations en matière de stockage de ces données sensibles - à des acteurs publics ou, éventuellement, privés.

M. Franck Montaugé, président. - Je vous remercie.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible en ligne sur le site du Sénat.

Audition de Mme Claire Mathieu, directrice de recherche au CNRS,
spécialiste des algorithmes,
le 12 juin 2019

M. Franck Montaugé, président. - Mes chers collègues, notre commission d'enquête poursuit ses travaux avec l'audition de Mme Claire Mathieu. Cette audition sera diffusée en direct sur le site Internet du Sénat et fera l'objet d'un compte rendu publié. Je rappelle, pour la forme, qu'un faux témoignage devant notre commission d'enquête serait passible des peines prévues aux articles 434-13, 434-14 et 434-15 du code pénal.

Conformément à la procédure applicable aux commissions d'enquête, Mme Mathieu prête serment.

Madame Mathieu, vous êtes informaticienne et directrice de recherche au CNRS, spécialisée dans la recherche sur l'algorithmique et, en particulier, sur la conception d'algorithmes destinés à trouver des solutions quasi optimales à des problèmes difficiles à résoudre exactement.

Vous vous êtes notamment intéressée à la modélisation du phénomène dit du « plafond de verre » dans les milieux sociaux.

Notre commission d'enquête s'interroge, à propos de la question de la souveraineté numérique, sur les moyens dont disposent la France et l'Europe en la matière. À cet égard, et dans la perspective de la réaffirmation de notre souveraineté numérique, qui concerne directement l'État, les citoyens ou les acteurs de la société - je pense en particulier aux entreprises -, en quoi la science des algorithmes peut-elle apporter des solutions de progrès ?

À la faveur de la réémergence de l'intelligence artificielle, dont on parle depuis très longtemps, et grâce aux capacités de calcul décuplées et aux gigantesques bases de données désormais disponibles, les algorithmes font l'objet de beaucoup de fantasmes.

C'est notamment la souveraineté des individus qui serait au premier chef, selon certains, menacée par les algorithmes. L'exemple qui vient naturellement à l'esprit, c'est celui du réseau social Facebook, dont l'algorithme risquerait de contraindre notre liberté de penser et d'être informé.

La question de la transparence des algorithmes est aussi l'objet de nombreuses interrogations. Le phénomène de la « boîte noire » est-il inéluctable ? Est-on condamné à ne plus connaître le contenu des algorithmes et leurs calculs ? Serons-nous un jour incapables de comprendre les décisions prises pour nous par des machines ?

Enfin, estimez-vous que la recherche française, publique comme privée, dispose de suffisamment de moyens en la matière pour faire le poids face aux géants du numérique ?

Mme Claire Mathieu, directrice de recherche au CNRS, spécialiste des algorithmes. - Merci de votre invitation. Cela fait plus de trente ans que je fais de la recherche sur les algorithmes. Après un parcours universitaire classique, j'ai travaillé dans l'enseignement supérieur et la recherche, essentiellement en France, dans des lieux très divers, mais aussi à l'étranger, aux États-Unis. J'ai en particulier passé huit années à temps plein comme professeur d'informatique à l'université Brown, aux États-Unis, l'une des universités de la Ivy League. Cela m'a permis de me familiariser de l'intérieur avec le système américain.

J'ai également été consultante pour quelques entreprises - NEC, AT&T, Microsoft Research - et, récemment, pour le compte du ministère de l'enseignement supérieur et de la recherche, au sujet de Parcoursup. J'ai rempli un rôle de consultant pour les laboratoires de recherche de ces entreprises, où j'ai effectué le même type de recherche que celles que je mène ordinairement, avec des collègues chercheurs travaillant pour Microsoft, AT&T, etc.

Quelques exemples des travaux de recherche que j'ai pu mener : J'ai conçu avec des collaborateurs un algorithme quasi optimal pour placer des rectangles dans une bande, de façon à utiliser le moins de longueur possible. Il s'agissait de réfléchir à la découpe de vêtements. Ceci est resté au niveau théorique. Avec d'autres collaborateurs, j'ai travaillé sur l'analyse d'une heuristique très populaire pour la classification de données en petite dimension. J'ai démontré qu'une variante était quasi optimale. Enfin, toujours avec des collaborateurs, j'ai proposé un modèle pour la croissance des réseaux sociaux et l'émergence d'un plafond de verre pour les minorités.

Tout mon travail s'articule autour de la conception, l'analyse d'algorithmes et parfois leur modélisation. Ma tâche est de concevoir des algorithmes et de démontrer des théorèmes.

Vous avez parlé de transparence. C'est un sujet auquel je me suis particulièrement intéressée dans le cadre de Parcoursup, la plateforme d'affectation des candidats bacheliers aux formations de l'enseignement supérieur. Cet exemple d'algorithme comporte des impacts sociétaux. Ce qu'on gère ce ne sont plus des rectangles, mais des êtres humains. Ceci change la donne : un algorithme, même s'il est totalement optimisé, ne pourra en effet être accepté que s'il a la confiance de ses utilisateurs.

Pour acquérir cette confiance, l'équipe de Parcoursup a essayé d'être très transparente. Comment y parvenir concrètement ? Nous avons publié l'algorithme et le code du coeur de Parcoursup. Ce n'est pas forcément une lecture très digeste pour tout un chacun, mais nos collègues informaticiens peuvent lire ces publications, les critiquer, voir s'il existe des erreurs et

évaluer la qualité du travail réalisé. Cela contribue à la transparence, même si le citoyen moyen a du mal à comprendre ce qui se trouve dans ces publications.

Nous avons également essayé d'être simples. Lorsqu'une formation reçoit des candidats, elle réalise un classement. Celui-ci est ensuite modifié pour tenir compte d'un taux de boursiers, déterminé selon la loi par le recteur. Nous avons donc conçu un algorithme que nous avons essayé de rendre aussi simple que possible pour modifier le classement, de façon à respecter le taux du recteur.

Un candidat doit aussi pouvoir comprendre ce qui se passe, et pourquoi il est pris ou non. Pour cela, Parcoursup fournit chaque jour au candidat son rang sur la liste d'appel de la formation, ainsi que le rang du dernier appelé. Par exemple, s'il est 300e et que le dernier est 297e, l'intéressé sait qu'il n'y a plus qu'à attendre trois renoncements avant de recevoir une offre. Cela lui permet de suivre l'évolution et d'avoir une perspective.

Un travail supplémentaire est indispensable en matière de critères d'examen des voeux. Les formations doivent fournir des renseignements suffisamment précis sur leurs attendus et sur les critères pour que les futurs candidats sachent quels cours suivre pour être acceptés et sur quels sujets se concentrer durant leurs années de lycée. Il est, pour ce faire, indispensable que les informations soient suffisantes.

De plus, chaque candidat qui n'est pas retenu peut demander communication des motifs de la décision. C'est un sujet de débat juridique. Une piste de réflexion pour l'avenir : on pourrait synthétiser l'avis des jurys en présentant une liste de matières avec des coefficients, ainsi qu'une partie laissée à la libre appréciation du jury. Malheureusement, avec 14 000 formations et 900 000 candidats, une même formule peut difficilement s'appliquer à tous. La question n'est donc pas encore résolue.

Quelques suggestions en matière de transparence...

Ma première suggestion concerne Affelnet - qui signifie « Affectation des élèves par le Net ». Il s'agit d'orienter les élèves de 3e vers les lycées selon un système de points attribués en fonction de leurs résultats scolaires, du temps de trajet entre le domicile et le lycée, de leur situation sociale. Cet algorithme existe depuis de nombreuses années, mais souffre d'une opacité encore plus grande que Parcoursup. Comment améliorer la transparence de cet algorithme afin que les familles puissent en comprendre le résultat ?

Une possibilité serait de fournir à l'élève, avant candidature, une estimation de son barème en lui montrant combien de points il aurait eu s'il avait été candidat l'an dernier, et de publier les seuils d'admission passés de chaque lycée. Il serait fait de même, chaque année, en fin de campagne. Ceci pourrait permettre à chaque élève de vérifier que la décision qui a été prise répond à une certaine légitimité. Vous le voyez ; cette proposition

améliorerait la transparence, sans qu'il soit besoin pour autant d'expliquer les détails de l'algorithme.

Mon deuxième souhait concerne le calcul de l'impôt sur le revenu. Actuellement, lorsqu'on a fait sa déclaration, on obtient seulement un chiffre correspondant au montant de l'impôt sur le revenu. J'aimerais, comme autrefois, que l'on indique également comment on est parvenu à ce résultat, et que l'on connaisse la formule de calcul. C'est tout à fait faisable, me semble-t-il, et l'explication donnerait plus confiance qu'un simple chiffre.

L'actualité récente nous apprend que la majorité des membres du Gouvernement n'ont pas été capables de remplir correctement leur feuille d'impôts : c'est bien qu'il existe un problème !

Je propose donc de simplifier les choses.. C'est une question en partie algorithmique, puisqu'il s'agit de trouver un graphe plus simple qui calcule la même chose. Cela me semble important pour l'intégrité du système.

Mon troisième souhait porte sur la transparence de la synthèse du grand débat national. En effet, la Société informatique de France s'est inquiétée de savoir si cette synthèse serait compréhensible et digne de confiance. Les contributions en ligne des participants sont accessibles à tous. C'est un élément important, n'importe quelle équipe scientifique pouvant s'en saisir pour essayer de faire sa propre analyse. Par ailleurs, les contributions ont été regroupées en catégories et sous-catégories. Ces catégories sont publiques. C'est également un élément de transparence. Ainsi, à la question : « *Que pensez-vous de l'organisation de l'État et des administrations en France ? De quelle manière cette organisation devrait-elle évoluer ?* », 2,9 % de la population a répondu spontanément en proposant la suppression du Sénat. En réponse ouverte, ce n'est pas négligeable. Reste qu'on ne sait pas comment les personnes ayant réalisé cette synthèse en sont arrivées à choisir comme catégorie la suppression du Sénat...

Il serait également bon de rendre transparentes les correspondances : pour chaque contribution, connaître les « étiquettes » qui lui sont attribuées par catégorie et sous-catégorie. Cela permettrait à chaque participant de vérifier la bonne correspondance et donc l'intégrité de la synthèse qui en a été faite. De plus, ceci aiderait à reproduire les résultats obtenus et à en vérifier la validité. Ce n'est pas ce qui est actuellement proposé.

L'algorithme n'est pas public... mais est-ce nécessaire pour la transparence ? Ce n'est pas indispensable, car même sans en connaître les détails, détenir suffisamment d'éléments sur les données, les résultats et les correspondances permet de vérifier la validité du résultat. Rendre l'algorithme public - ce qui poserait des problèmes de propriété intellectuelle - n'est donc pas forcément essentiel pour l'intégrité de la synthèse du grand débat national.

Enfin, on parle beaucoup d'algorithmes d'apprentissage profond s'agissant de l'intelligence artificielle. Comment le calcul est-il réalisé ? Chaque noeud regarde les noeuds de la couche précédente et établit une moyenne pondérée des entrées, en y appliquant certains coefficients. Par exemple, si la moyenne est supérieure à 10, on estime que le résultat est de 1, si elle est inférieure à 10, le résultat sera de 0. Les noeuds de la deuxième couche vont utiliser à leur tour ces résultats pour réaliser leurs propres calculs, et ainsi de suite. Au bout de quelques couches, on obtient une sortie.

Ces coefficients sont essentiels pour le fonctionnement de l'algorithme. Ils sont retenus grâce à une méthode d'apprentissage. C'est le cas de la météorologie, par exemple : on observe les données dont on dispose, et on ajuste les coefficients grâce à diverses méthodes d'optimisation, de façon à ce que les données produites par le réseau soient le plus exactes possibles, comparées aux données passées.

Les coefficients sont ainsi établis pour « coller » au mieux aux données du passé et sont jugés corrects par rapport aux éléments dont on dispose déjà. Une fois qu'on est parvenu à produire un résultat suffisamment proche de ces éléments connus, on estime avoir réussi à établir des coefficients satisfaisants pour que l'algorithme réalise des prédictions.

On peut donc, certes, réclamer la publication de l'algorithme, mais dans le cas de ce type d'algorithmes, à quoi cela servirait-il ? À supposer même que l'entreprise, oubliant les questions de propriété intellectuelle, publie généreusement la totalité de son algorithme avec tous ses coefficients, cela ne nous dira rien sur ce qui se passe vraiment.

C'est publier le principe et les méthodes de constitution de l'algorithme qui est utile, car cela peut aider les chercheurs à estimer si ce type d'algorithme souffre ou non de certains problèmes potentiels et à comprendre ce qui a été fait pour y remédier.

La qualité du réseau qui résulte de ces opérations dépend essentiellement des données sur lesquelles l'apprentissage a été réalisé. La qualité du résultat dépend de la qualité des données.Publier ces données serait donc idéal, car si les données étaient publiques, n'importe qui pourrait proposer ses propres prédictions et critiquer l'ensemble des données.

Cette méthode algorithmique prédit que le comportement futur de ce qu'on essaie d'estimer est similaire au comportement passé des données qu'on possède. Cela signifie que si les données ont un biais, l'algorithme reproduira ce biais. La qualité des données est essentielle. Il serait bon, *a minima*, que tous les algorithmes qui utilisent des données publient les caractéristiques de celles-ci et qu'on puisse expliquer ce qui a été fait pour obtenir des garanties sur leur qualité.

C'est ce qui se fait d'ailleurs de façon assez classique dans la recherche médicale : dans ce domaine, les résultats sont basés sur une étude en précisant un certain nombre de patients, d'hôpitaux, de cohortes, etc.,

avec des données statistiques. C'est fondamental pour avoir confiance dans la méthode utilisée.

Dans quels cas l'intelligence artificielle ainsi décrite fonctionne-t-elle bien ? J'ai demandé à un collègue spécialiste de l'apprentissage de me fournir des exemples et des contre-exemples. Selon lui, un des succès de l'intelligence artificielle réside actuellement dans la traduction et un autre dans la prédiction de tumeurs. En général, cela fonctionne si le contexte est très cadré, s'il existe peu d'incertitudes, que les données sont précises et que l'on sait exactement ce que l'on veut prédire. Plus le problème est précisément défini, mieux les méthodes fonctionnent.

Les problèmes qui présentent encore des défis pour l'intelligence artificielle se rencontrent lorsque les données sont floues, comportent beaucoup d'incertitudes et qu'on ne peut envisager toutes les configurations possibles.

Par exemple, la voiture autonome : elle peut fonctionner sur un circuit fermé, mais à partir du moment où on est sur la route, l'interaction avec les autres véhicules constitue un défi que l'intelligence artificielle ne peut actuellement pas surmonter de façon fiable.

Imaginez que l'algorithme commette une erreur sur un million... mais qu'on ait un million de voitures sur les routes : on aura tous les jours un accident imputable à une erreur de l'algorithme ! Ce n'est pas acceptable. Actuellement, l'intelligence artificielle ne peut produire des voitures autonomes capables de se débrouiller seules en milieu réel.

Un autre exemple est celui du diagnostic médical complet. Là aussi, il y a actuellement trop de paramètres, trop d'inconnues, trop de flou. On ne peut y parvenir.

Comment, dès lors, contrôler les algorithmes en matière d'intelligence artificielle ? Dans son livre *À quoi rêvent les algorithmes ?*, Dominique Cardon écrit: « *Le futur de l'internaute est prédit par le passé de ceux qui lui ressemblent* ». C'est une formulation qui décrit bien la façon dont fonctionnent ces algorithmes.

Que faire pour éviter une discrimination liée au genre ? On pourrait, dans les données, effacer l'information « hommes », « femmes » ou autres. Et pourtant, ce n'est pas efficace, car il est généralement facile de reconstruire le genre à partir des autres informations collectées. Par exemple, dans le cas de candidats à des formations d'enseignement supérieur, même si on ne sait s'il s'agit de garçons ou de filles, l'information selon laquelle ils font de la boxe, par exemple, permet de penser avec une bonne probabilité qu'il s'agit de garçons. En fait, l'information du genre est contenue implicitement dans ces données.

Il vaudrait mieux tenter de savoir si les données servant à l'apprentissage sont biaisées et, surtout, tester la discrimination *a posteriori*.

Ainsi, il devrait être possible de demander aux entreprises utilisant des méthodes d'intelligence artificielle de préciser les outils qu'elles emploient pour corriger les biais des données et mettre en place des tests de discrimination avec des résultats *a posteriori*.

On a récemment entendu parler de propositions d'emploi faites à des femmes à qui un algorithme proposait des salaires moins élevés que ceux des hommes. Il faudrait donc que la loi impose des tests *a posteriori* pour signaler un biais. Les objectifs fixés par le législateur devraient pouvoir être traduits en conditions mathématiques servant à tester les résultats des algorithmes et à signaler un problème.

Pour conclure, que peut-on faire en matière de transparence des données ? On a vu qu'un bon résultat s'obtient en appliquant un bon algorithme sur des bonnes données. Les entreprises dominantes peuvent acquérir plus de données que les autres, ce qui leur permet d'améliorer leurs résultats et de passer à une situation d'hégémonie. C'est le cas, en France, pour le moteur de recherche Google. Ceci explique partiellement la position de force des GAFA.

Les risques sont nombreux. Le livre de Cathy O'Neal, *Weapons of Math Destruction*, aujourd'hui traduit en français, en décrit tout le panorama pour le grand public. Il présente ce dont il faut se méfier.

Que faire pour éviter les dérives ? Il conviendrait d'éviter de confier des marchés publics aux GAFA. Actuellement, par exemple, les données médicales françaises sont l'objet de la convoitise de toutes sortes d'entreprises. Celle qui remportera le marché, si elle n'est pas française, aura tout de suite un gros avantage par rapport aux entreprises nationales en bénéficiant de ces données.

Il existe beaucoup d'autres risques. Ainsi, lorsque le débat se déplace sur Twitter, il est conduit selon les règles de Twitter, qui décide qui a le droit de parler ou non, ce qu'on a le droit de dire ou de ne pas dire. C'est une des difficultés de l'extension du numérique dans notre société.

Vous m'avez demandé si la recherche française pouvait faire entendre sa voix, sachant que la société du XXIe siècle sera numérique. Je me placerai au niveau de l'Europe plutôt qu'au niveau de la France. La France est en effet un petit pays, et l'Europe dispose d'un plus grand poids.

En Europe, certaines tentatives ont avorté. L'une des difficultés vient du fait que le numérique a besoin de chercheurs. Or, en raison de l'importance de la demande de compétences par rapport au vivier, il existe actuellement une tension sur les salaires dans ce domaine. Quand la différence devient trop importante, les jeunes ont du mal à résister aux offres des entreprises étrangères.

Je pense aussi que les start-up ont du potentiel, pourvu que le Gouvernement ne contribue pas à faire pencher la balance du côté des

GAFA. La situation hégémonique est là, et on ne peut guère que tenter de la contrôler, mais il reste dans le numérique beaucoup de domaines où les algorithmes ne sont pas encore au point. Des possibilités s'offrent donc à de nouveaux acteurs et l'Europe a toutes ses chances dans ce domaine.

M. Franck Montaugé, président. - Merci beaucoup, je donne la parole aux commissaires qui le souhaitent.

M. Pierre Ouzoulias. - Merci pour la clarté de votre exposé, madame et chère collègue.

Vous avez dit fort justement que le danger vient de ce que des sociétés monopolistiques accaparent une masse de données qui confortent leur position dominante sur un marché. La meilleure façon de protéger ces données n'est-elle pas finalement de les rendre publiques ? Un open data général, organisé par l'État, n'est-il pas une solution pour éviter toute position monopolistique ?

Mme Claire Mathieu. - Un open data général ? Je n'ai pas envie que vous sachiez ce que j'ai commandé sur Amazon, par exemple.

M. Pierre Ouzoulias. - De façon anonymisée...

Mme Claire Mathieu. - L'open data anonymisé général serait-il envisageable, et les recherches que je fais sur Internet pourraient-elles être publiques ? Est-ce que ce serait acceptable ? Pourrait-on le mettre en place ? Avec quelles conséquences ?

Et si une application sur mon ordinateur pouvait me permettre de l'accepter, toutes les informations pourraient être données au Gouvernement, un peu comme en Chine... Je ne pense pas que ce soit votre suggestion, et j'y vois quelques dangers...

M. Pierre Ouzoulias. - L'ambassadeur pour les affaires numériques nous a dit que les préfectures travaillaient avec Google Maps jusqu'au jour où le prix des licences est devenu exorbitant. Elles ont compris que fournir des données publiques à OpenStreetMap permettait de continuer à utiliser le service. Elles donnent aujourd'hui une large publicité à leurs données, permettant ainsi à des logiciels libres de s'en emparer pour offrir des solutions là où des opérateurs privés imposent des coûts prohibitifs.

Mme Claire Mathieu. - C'est le même esprit qui a présidé à la publication de toutes les participations au grand débat national. Il est vrai que cela permet à tous les scientifiques d'utiliser les données comme ils le souhaitent.

M. Franck Montaugé, président. - On nous a également dit qu'il était fondamental que les données scientifiques restent publiques et accessibles à tout le monde.

Mme Claire Mathieu. - Absolument !

M. Franck Montaugé, président. - C'est là un enjeu politique majeur. C'est un point qui me paraît fondamental pour l'avenir de la science si on souhaite que celle-ci ne soit pas privatisée au bénéfice de certains et au détriment du plus grand nombre.

Mme Claire Mathieu. - Il est nécessaire, pour améliorer la transparence, de disposer de plus de données publiques de façon proactive. D'un autre côté, pour améliorer la transparence des moteurs de recherche, on pourrait imaginer que l'utilisateur reçoive tous les matins un message l'informant que telle et telle information le concernant a été collectée la veille et divulguée à tel et tel destinataire. Cela permettrait à chacun d'être conscient de ce qu'il partage...

M. André Gattolin. - Regardez LinkedIn qui adresse régulièrement à ses membres un rapport sur les personnes qui ont consulté leur profil ! J'arrive ainsi à savoir, en fonction de mes interventions, s'il s'agit de scientifiques ou d'une administration, étrangère ou non. C'est instructif.

En matière d'algorithmes, la question des biais est particulièrement intéressante. En informatique, on procède à de la rétro-ingénierie, remontant au code source pour comprendre les failles Ceci a-t-il un sens s'agissant des algorithmes d'apprentissage profond ?

Je fais d'ailleurs le lien avec le développement des super-calculateurs : si un algorithme devenait tout-puissant dans un domaine sensible, comme la santé, sous une influence étrangère ou dans un but commercial, ne pourrait-on parvenir techniquement, avec l'aide de puissants moyens de calcul, à comprendre sa construction sans même disposer des données de base ? Et cela présenterait-il un intérêt ?

Mme Claire Mathieu. - Je ne suis pas spécialiste des algorithmes d'apprentissage automatique mais, en la matière, disposer des coefficients ne nous aide pas à comprendre le problème.

On peut toutefois, en réduisant les coefficients, essayer d'observer si le résultat demeure assez bon. On pourrait ainsi estimer que le résultat s'explique à 20 % par tel ou tel facteur et à 15 % par la combinaison de tel et tel autre. Quand le problème est simple, on peut, trouver les coefficients dominants pour expliquer une partie du résultat, ce qui est plus satisfaisant.

Malheureusement, on ne peut pratiquer de la sorte pour tout : pour prédire la météorologie à dix jours, trop de facteurs entrent en ligne de compte. Il est donc impossible de fournir une explication simple, le problème étant par nature complexe.

Mme Viviane Artigalas. - Le traitement des données et ce qui peut en être tiré m'apparaissent également importants. On imagine bien comment, à un moment donné, des algorithmes de traitement des données, s'ils tombent dans de mauvaises mains, peuvent volontairement déboucher sur de la manipulation ou de la discrimination, positive ou négative.

Comment faire pour prévenir les difficultés qui peuvent survenir dans le traitement des données ? Grâce aux évolutions technologiques, celles-ci vont être traitées dans un nombre sans cesse croissant de lieux. C'est l'absence de droit de regard sur leur traitement qui pose question.

Mme Claire Mathieu. - Je n'ai hélas pas de réponse directe à votre question, mais un des dangers qui existe est fort bien expliqué dans le livre de Cathy O'Neal déjà cité : les algorithmes destinés à prédire l'apparition d'une tumeur peuvent être optimisés au fil du temps car les maladies se comporteront toujours de la même manière.

Mais avec des algorithmes ayant pour objet des êtres humains, on est confronté au fait que, les personnes peuvent justement adapter leur comportement à cet algorithme. Prenez l'exemple du classement de Shanghai, censé présenter les meilleures universités au monde. Les universités ont pris cela suffisamment au sérieux et changé la façon dont elles fonctionnent non pour s'améliorer de façon générale mais bien spécifiquement pour satisfaire aux critères dudit classement.

Le comportement se modifie... et la formule n'est plus bonne ! Ceci est vrai pour tous les algorithmes qui agissent sur le comportement humain. Toutes sortes de déviations deviennent ainsi possibles.

M. Franck Montaugé, président. - C'est une réponse à une forme de contrainte, une réduction des libertés...

Mme Claire Mathieu. - En effet.

M. Franck Montaugé, président. - Merci beaucoup.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible en ligne sur le site du Sénat.

Audition de M. Éric Léandri, président et cofondateur de Qwant,
le 12 juin 2019

M. Franck Montaugé, président. - Nous poursuivons nos travaux avec l'audition de M. Éric Leandri.

Conformément à la procédure applicable aux commissions d'enquête, M. Léandri prête serment.

Monsieur Léandri, vous êtes le fondateur et l'actuel président de Qwant, entreprise à capitaux franco-allemands que vous avez créée en 2013. Son activité principale consiste à fournir un moteur de recherche qui se distingue de Google par la protection de la vie privée de ses utilisateurs. Il se rapproche sur ce segment du méta-moteur de recherche américain Duck-Duck-Go.

Votre entreprise a réalisé un chiffre d'affaires de 5 millions d'euros en 2018 et compte 160 salariés. Son activité est en croissance. En avril 2019, votre moteur de recherche aurait traité 100 millions de requêtes contre 18 millions en avril 2018. Les chiffres grimpent de mois en mois. Mais le chemin reste long comparativement à Google, par exemple, qui dispose de 95 % des parts de marché si mes informations sont bonnes.

Vous avez fait le pari ambitieux de concurrencer l'un des principaux géants du numérique américain. Cela intéresse notre commission d'enquête, car nous devons nous interroger sur les voies et moyens de faire émerger les fameux géants européens du numérique que certains attendent parfois comme une sorte de Messie.

Vous bénéficiez du soutien financier de la Caisse des dépôts, qui détient 20 % de votre capital, soit autant que le groupe allemand Axel Springer. Estimez-vous que les écosystèmes français et européen sont suffisamment favorables à l'émergence de tels champions ?

Aujourd'hui, les critiques et les amendes pleuvent sur certains géants américains du numérique en raison de leurs pratiques anticoncurrentielles. En avez-vous été victime vous-même ?

Enfin, comment appréhendez-vous la notion de souveraineté numérique, qui est au coeur de l'objet de notre commission d'enquête ? Estimez-vous que votre entreprise peut aider la France et l'Europe à conquérir cette souveraineté dans le cyberespace ?

M. Éric Léandri, président de Qwant. - Mesdames les sénatrices, messieurs les sénateurs, je souhaite vous remercier tout d'abord d'avoir créé cette commission d'enquête parlementaire sur la souveraineté numérique et de nous donner la possibilité de partager la vision de Qwant. C'est un sujet structurant pour notre pays, qui doit tous nous réunir.

Nous avons créé Qwant en 2011 et avons enregistré environ 18 milliards de requêtes l'année dernière.

C'est précisément le souci de contribuer à une certaine vision de la souveraineté numérique des Français et des Européens qui nous a poussés, il y a déjà huit ans, à créer le moteur de recherche Qwant. Je vous expliquerai, dans la suite de mon propos, pourquoi un moteur de recherche est indispensable dans une stratégie de souveraineté numérique.

Lorsque nous avons lancé Qwant, Google avait déjà plus de 95 % de parts de marché en Europe. Il générait 40 milliards de dollars de chiffre d'affaires à travers le monde, 30 % de ce chiffre d'affaires étant réalisé en Europe.

De toute évidence, il n'y avait que très peu de gens à cette époque pour croire en une alternative européenne. Tous nous disaient que la bataille était perdue d'avance, qu'il était déjà trop tard pour créer un moteur de recherche européen. Avec mes associés, nous avons pris le contre-pied et fait fi de ces réticences. Nous avons réussi à convaincre suffisamment de partenaires privés pour démarrer et accompagner notre croissance. Ils avaient compris l'importance vitale de la souveraineté numérique pour notre pays.

Après huit ans de travail acharné, j'en vois toujours ici ou là qui semblent espérer notre échec ou tentent de ralentir la construction d'une alternative durable, mais je suis fier de constater que Qwant est aujourd'hui le moteur de recherche choisi par un nombre grandissant de secteurs économiques - PME, mais aussi grandes références comme Safran, Thalès, BNP Paribas, la Caisse d'Épargne, Audiens, le Groupe Nice Matin, le Groupe France Télévisions, la SNCF Transilien, la MAIF, le CNES, le CEA et bien d'autres.

Massivement, dans les territoires, les collectivités font le choix d'une alternative souveraine et éthique. Nous avons été choisis par de grandes métropoles comme Paris, Nice, Rennes, par exemple, des villes petites et moyennes, mais aussi des départements et des régions, comme les Hauts-de-Seine, les Yvelines, l'Ille-et-Vilaine, la Bretagne ou l'Ile de France. Nombreux sont les ministères à avoir adopté Qwant, notamment l'intérieur, l'éducation nationale ou la culture, mais aussi les armées et, prochainement, toute l'administration française, sous l'impulsion du secrétaire d'État au numérique.

Tous ces choix, privés et publics, s'ajoutent aux millions d'internautes qui nous font confiance. Tous nous permettent d'accélérer notre développement, avec un effet très concret : le mois dernier, ce sont 240 millions de visites que nous avons reçues sur Qwant.

Nous avons encore beaucoup de travail à réaliser. Qwant ne serait pas là - et je ne serai pas aujourd'hui devant vous - s'il n'y avait pas eu, en France et en Europe, une véritable prise de conscience des enjeux de

souveraineté numérique. Le plus grand nombre a la volonté de retrouver une certaine forme de libre choix et d'indépendance.

La souveraineté, c'est la capacité que nous avons tous, en tant qu'individus, collectivités, entreprises, à prendre librement des décisions. Qwant essaye d'apporter des réponses à deux niveaux de souveraineté numérique.

Le premier, c'est celui de la souveraineté numérique collective, au sens de la capacité de l'État et plus généralement de notre société à rester maître de ses systèmes d'information, dont dépendent des pans entiers de l'activité du pays et de nos actions à l'extérieur. Le second niveau, c'est celui de la souveraineté numérique individuelle, au sens de la capacité de chaque individu à conserver son autonomie quotidienne, sans dépendre d'outils numériques sur lesquels il n'a plus aucun contrôle.

En matière de souveraineté numérique, le rôle du moteur de recherche est fondamental pour garantir une liberté suffisante aux pouvoirs publics, à la société et à l'individu. Il est primordial de comprendre ce qu'est un moteur de recherche, et comment il fonctionne, car nous utilisons tous un moteur de recherche, tous les jours, sans forcément le savoir.

Un moteur de recherche, c'est par définition un outil qui permet de savoir où se trouve l'information recherchée. Au préalable, il faut donc qu'il connaisse le maximum d'informations pour pouvoir répondre à la question qui lui est posée. C'est le rôle de l'index. L'index, en simplifiant à l'extrême, est en quelque sorte la bibliothèque d'Alexandrie.

Pour constituer son index, Qwant envoie des logiciels appelés *crawlers*, ou indexeurs, qui, simulant l'activité d'un internaute *lambda*, se promène sur internet, regarde le contenu de la page et en note les changements. Aujourd'hui, l'index de Qwant compte 20 milliards de pages, dont 2 milliards sont visités chaque jour.

Une fois qu'on dispose de l'index, il faut pouvoir effectuer un tri à l'intérieur de cette masse d'informations, afin de faire remonter les résultats les plus pertinents. Ceux-ci viendront fournir les réponses à la question que pose l'internaute. C'est le rôle joué par les algorithmes de tri des résultats. C'est ce qu'on appelle le *ranking*, ou classement. Chez Qwant, nous avons mis au point nos propres algorithmes de tri. Nous sommes parmi les seuls à détenir des brevets dans ce domaine. Ils prennent en compte des dizaines et des dizaines de facteurs différents, pour déterminer quelle page afficher en premier dans nos résultats, puis en second, etc.

Avec ces deux éléments clés, l'index et les algorithmes de tri, le moteur de recherche utilisé a une influence très importante sur l'information à laquelle on peut accéder et qu'on peut partager. En fonction des contenus qu'il choisit d'indexer ou non, vous n'aurez peut-être pas accès à certaines informations ou, au contraire, verrez des contenus impossibles à trouver chez d'autres, sur lesquels cliquent la très grande majorité des utilisateurs.

Or dans le monde, il n'existe que huit vrais moteurs de recherche grand public qui disposent à la fois de leur propre index du web et de leurs propres algorithmes : Google et Bing aux États-Unis, Naver en Corée du Sud, Yandex en Russie, Baidu en Chine, Seznam en République Tchèque, Yahoo au Japon, et Qwant en France.

Tous les autres sont des méta-moteurs qui utilisent exclusivement les résultats fournis par d'autres moteurs de recherche - la plupart du temps Google ou Bing. Ce sont des interfaces de recherche. La plupart du temps, ils sont installés sur une des infrastructures d'un géant comme Amazon.

Cette différence est décisive. C'est en cela que Qwant est stratégique. Sur le plan de la souveraineté collective, c'est essentiel. Qwant est né du constat du manque total d'indépendance de l'Europe en matière d'accès à l'information à travers les moteurs de recherche. Dans 95 % des cas, quand un Français ou un Européen fait une recherche sur un sujet quelconque, c'est un moteur de recherche étranger qui lui dit où se trouve l'information la plus pertinente de son point de vue. Il est donc intéressant d'avoir un moteur européen et français.

Il s'agit d'un pouvoir d'influence énorme à l'échelle d'un continent. Cela peut avoir de nombreuses répercussions, y compris sur les élections. C'est du jamais vu ! C'est donc un risque majeur pour la souveraineté de la France et de l'Europe.

C'est évidemment la même chose sur les réseaux sociaux ou les plateformes de vidéos. Une très grande partie de notre accès à l'information et au savoir et notre capacité à partager cette information dépend aujourd'hui d'acteurs étrangers, lesquels peuvent avoir les meilleures intentions du monde, mais aussi des intérêts différents des nôtres.

Que se passera-t-il si les États-Unis, demain, décident que Google ne doit plus fournir de résultats en France, filtrent tel ou tel résultat, et coupent le service de messagerie électronique qu'utilisent des millions de Français et d'entreprises ? Cela paraît invraisemblable, mais c'est un peu ce qui s'est passé pour un géant chinois. Du jour au lendemain, les États-Unis ont demandé à Google de rompre son partenariat avec le deuxième constructeur mondial de *smartphone*, privant ainsi le marché de plus de 200 millions d'appareils par an.

Toutes les informations qu'ils indexent sont très utiles par ailleurs pour d'autres développements fondamentaux. Je pense en particulier à l'intelligence artificielle. On commence à la voir un peu partout. Demain, elle sera omniprésente, aussi bien chez les individus que dans les industries, les administrations, l'armée...

Si nous ne disposons pas d'une capacité à fournir notre propre intelligence artificielle alors qu'elle fait tourner une grande partie de l'économie et contribue au fonctionnement de la société, nous ne maîtriserons plus rien. C'est un risque qui me paraît tout à fait inacceptable.

Pourrons-nous toujours nous offrir le luxe de nous fâcher, même provisoirement, avec un allié avec lequel nous ne sommes pas d'accord, alors que c'est lui qui nous fournit nos moyens de communication, nos informations et notre intelligence artificielle ? Si nous devons craindre que les services numériques dont dépend toute notre économie soient coupés ou bridés, serons-nous vraiment libres de ne pas suivre ce qu'on nous demande de faire ? C'est cela, la souveraineté ! Je pourrais aussi vous parler de la santé connectée, des bases de données médicales et des objets de santé intelligents, ou encore des cryptomonnaies, qui échappent de plus en plus au contrôle régalien.

Je voudrais aussi évoquer le risque que représente un moteur de recherche qui sait ce que nous recherchons et ce que nous consultons. Cela touche la souveraineté individuelle. Ce volet rejoint les préoccupations sur la souveraineté collective.

Comme vous le savez, Qwant a séduit les internautes avec une promesse forte, qui précédait largement le Règlement général de protection des données (RGPD), celle de ne pas collecter les données personnelles des utilisateurs et de donner une vision neutre et panoramique de l'internet. Nous l'avons fait parce que nous avons la conviction que, chaque fois que nous confions nos données personnelles à quelqu'un qui peut les utiliser, nous prenons le risque de perdre un peu plus de liberté.

De même, nous sommes convaincus que notre moteur doit rester neutre et ne pas faire de discrimination selon les sites ou les contenus, ni modifier les réponses selon l'utilisateur.

Sur un moteur de recherche, chaque fois que vous dites ce que vous recherchez, vous révélez ce qui vous intéresse. Vous le dites tout au long de la journée, sur votre ordinateur, votre *smartphone*, ou même chez vous, le soir, si vous avez acheté une de ces nouvelles enceintes connectées. Si je me souviens de tout ce que vous demandez, au bout de quelques semaines j'ai une idée très précise de qui vous êtes - régime alimentaire, religion, sexualité, santé, opinions politiques. C'est sans fin.

Tout cela, ce sont des informations que Qwant a choisi de ne pas collecter et de ne pas revendre. Nous croyons fondamental de préserver la vie privée et la liberté de l'individu, donc sa souveraineté.

Qwant a été conçu autour du droit à la vie privée, tel qu'il est énoncé dans l'article 12 de la Déclaration universelle des droits de l'homme. Je refuse que mon entreprise puisse exploiter des données qui lui permettraient de trier les résultats de recherche afin d'influencer et de biaiser les informations que reçoit telle ou telle catégorie de la population, ou de permettre à des annonceurs de cibler des personnes selon leur profil.

C'est ce qui s'est passé avec Cambridge Analytica, et c'est le risque que nous courons avec d'autres acteurs. En Europe, avant d'être des consommateurs, les internautes sont avant tout des citoyens. Or les citoyens

ont des droits. Il n'a jamais été aussi facile de manipuler une élection en utilisant les biais psychologiques de chacun et en personnalisant l'information affichée, grâce aux données personnelles collectées. Ce n'est pas seulement l'apanage des Russes.

Si un moteur de recherche a accès aux recherches d'une administration, une PME ou une grande entreprise française, il est facile de faire de l'intelligence économique et diplomatique. Il n'y a plus qu'à personnaliser les résultats pour influencer les décisions. Ce sera encore beaucoup plus facile avec le développement des assistants personnels, avec qui on a un rapport de confiance parce qu'ils ont une voix humaine et qui nous parlent comme si nous étions leur ami.

C'est pour cela que Qwant a construit son indépendance technologique, pour permettre à la France et à l'Europe de ne plus dépendre d'un moteur de recherche étranger, et aux individus de conserver leur libre arbitre et l'accès à une information de qualité.

La souveraineté numérique ne se décrète pas. Elle se pense, elle se travaille et se construit avec une vision de long terme. Chez Qwant, nous avons beaucoup investi et nous investissons de plus en plus dans la création de notre propre index et de nos propres algorithmes de recherche. L'objectif pour nous est de ne plus dépendre de plateformes numériques étrangères, pour construire une alternative crédible, assumer notre autonomie stratégique et notre indépendance technologique.

Il serait illusoire de prétendre créer, *ex nihilo*, en quelques clics et dès le premier jour, un service mondial comparable à de grandes plateformes numériques étrangères. Cela prend beaucoup de temps et d'énergie et nécessite beaucoup d'argent ! Chez Qwant, nous devons faire beaucoup avec peu, et nos utilisateurs et utilisatrices attendent que nous délivrions des résultats pertinents immédiats, des services complets et performants, et un niveau de qualité qui rivalise avec les *leaders* dont les services sont tout aussi gratuits que les nôtres.

Sans investir des centaines de millions d'euros, le recours partiel mais transitoire à des services fournis par des tiers est par conséquent nécessaire, du moment que cela ne remet pas en cause notre engagement fondamental à propos du respect total de la vie privée et la protection des données personnelles.

C'est ce que nous avons fait, notamment avec Bing, qui nous a permis d'avoir des résultats suffisamment pertinents dès le lancement de Qwant. Sans cela, nous n'aurions pas pu offrir dès le premier jour le niveau de service susceptible de fidéliser nos utilisateurs.

C'est aussi pour cela que nous avons signé un partenariat inédit et innovant avec Microsoft le mois dernier. Jusque-là, tout notre index et tous nos calculs - notamment pour l'intelligence artificielle - étaient réalisés exclusivement sur nos propres serveurs. Désormais, Microsoft met aussi à la

disposition de Qwant les capacités additionnelles de son *cloud* Azure, qui nous permet de stocker beaucoup plus de données dans notre index et d'exécuter des calculs beaucoup plus rapidement, avec une puissance que nous ne pouvons pas égaler aujourd'hui.

Toutefois Microsoft n'a accès à aucune donnée personnelle de nos utilisateurs. Tout est parfaitement cloisonné et étanche. Nous avons justement travaillé avec eux pour trouver un système qui le garantit. Si vous cliquez sur une publicité ou sur un résultat de recherche, nous ne contrôlons évidemment pas ce que les annonceurs ou les éditeurs de sites internet sur lesquels vous allez font de vos données mais, quand vous revenez sur Qwant, nous ne savons pas où vous êtes allé ni ce que vous avez recherché. Pour Qwant, vous demeurez anonyme.

Avec Microsoft, un des géants du numérique, nous pouvons désormais accélérer les choses en France et partout en Europe. Ce partenariat est surtout réalisé conformément à nos exigences et à nos valeurs françaises et européennes. C'est un partenaire industriel et commercial, comme Airbus en a aux États-Unis.

Qwant reste maître de sa technologie, du développement de son algorithme, de son index, de son infrastructure, et demeure soumis au respect de la vie privée de ses utilisateurs. La souveraineté numérique peut compter sur notre appui et sur d'autres entreprises françaises et européennes, qui font de l'excellent travail, comme OVH.

Nous avons encore beaucoup de travail à réaliser. Nous avons parfois pris du retard, ce dont certains profitent d'ailleurs pour nourrir leur entreprise de déstabilisation, à grand renfort de théories du complot. Vous en avez peut-être été destinataires. J'ouvre à ce sujet une parenthèse pour vous dire que nous avons introduit plusieurs recours judiciaires en diffamation et en dénigrement. Je n'en dirai pas plus, puisque des procédures sont en cours, mais ne nous y trompons pas : l'objectif est de démolir nos travaux et notre entreprise.

Il existe un point commun entre toutes ces attaques : ceux qui les relaient refusent systématiquement de s'intéresser à notre travail. Ceci démontre que nous sommes sur la bonne voie et que nous allons y arriver !

Nous savons ce que la France nous a donné, et nous voulons le lui rendre. C'est aussi pour cela que Qwant a choisi d'établir son siège fiscal en France, de créer un moteur de recherche spécialement adapté aux enfants, Qwant Junior, utilisé par dix académies sur dix-sept, de contribuer au financement de la presse ou encore d'aider les causes sociales et environnementales en reversant une part de ses gains aux associations.

Voici notre stratégie et notre contribution concrète à la souveraineté numérique en France et en Europe. C'est dire l'importance d'un moteur de recherche européen éthique, responsable et neutre.

La souveraineté numérique, c'est au fond l'affaire de tous, et je crois que nous y prenons toute notre part. Aujourd'hui comme hier, vous êtes évidemment les bienvenus chez Qwant pour rencontrer nos équipes et voir comment tout cela fonctionne de l'intérieur.

Je me tiens à présent à votre entière disposition pour répondre à toutes vos questions.

M. Franck Montaugé, président. - La parole est au rapporteur.

M. Gérard Longuet, rapporteur. - Je connais Qwant. J'apprécie son effort pour doter l'Europe d'un moteur de recherche autonome et indépendant. J'ai presque envie de dire que le fait d'avoir des ennemis est plutôt rassurant : cela prouve que vous êtes en train de percer !

M. Franck Montaugé, président. - La parole est aux commissaires.

M. Stéphane Piednoir. - On connaît tous la capacité de Qwant à protéger la vie privée en ne conservant aucune trace de l'utilisateur. Or, on peut considérer que la réponse est, de ce fait, moins pertinente. L'argument des moteurs de recherche qui ont moins de scrupules à l'égard de la vie privée des utilisateurs est d'apporter à ceux-ci des réponses plus proches de leurs attentes. Comment faire en sorte qu'un utilisateur préoccupé par la protection de sa vie privée reçoive en même temps des réponses qui correspondent à ce qu'il souhaite ?

M. Éric Léandri. - Nous avons fait plusieurs enquêtes avec d'autres compétiteurs du marché, comme Yandex. Les informations relatives aux utilisateurs améliorent surtout la pertinence de la publicité. Les réponses que l'on trouve sur le web concernent trois ou quatre liens mieux placés lorsqu'on connaît mieux l'utilisateur. Si celui-ci est par exemple informaticien et clique toujours sur un lien de site internet pour du code, le site en question devrait passer premier dans un moteur qui le connaît. Chez Qwant, ce site sera toujours troisième ou quatrième, bien que lorsque des milliers de gens cliquent sur le même lien pour la même requête, nous fassions remonter ce lien dans nos résultats.

Cependant, cela ne suffit pas. Les tests que nous avons réalisés prouvent qu'il faut aller plus loin. Pour cela, nous disposons de la technologie Masq, qui va être lancée ce mois-ci. Masq consiste à conserver vos recherches si vous le désirez sur votre téléphone, votre ordinateur, à l'intérieur d'un *cloud* qui vous appartient, là vous avez envie de les conserver, mais non chez Qwant.

Masq correspond à une partie totalement chiffrée du disque dur de votre téléphone ou de votre ordinateur qui n'est pas accessible aux autres et qui permet de savoir où vous avez cliqué les dernières fois afin de pouvoir transformer la requête pour placer en première, deuxième ou troisième position les résultats que vous préférez.

C'est en apportant à l'utilisateur la capacité de conserver ses données que nous allons régler ce problème. Nous travaillons depuis deux ans sur le chiffrement et la capacité de conserver ces informations et de les partager. C'est techniquement complexe, mais nous sommes prêts.

Nous avons également établi une cartographie pour réaliser Qwant Maps. Notre carte n'est évidemment pas destinée à savoir ce que vous avez fait hier ni où vous êtes allé. Cependant, vous aimeriez sûrement conserver des informations comme votre adresse ou celle de votre bureau plutôt que de les rentrer tous les jours. Vous pouvez le faire dans Masq et les voir s'afficher en ouvrant la carte de Qwant grâce à votre téléphone.

C'est un algorithme local, avec une intelligence artificielle locale et non globale. Cela permettra de protéger des millions de Français ou leurs enfants. Si vous allez chaque jour à l'hôpital, c'est peut-être pour y rendre visite à des personnes, y travailler, ou pour y suivre un traitement. Ce sont des informations qu'il n'est peut-être pas nécessaire de partager.

Les cartes deviennent très importantes dans notre monde. Lorsque vous montez dans une voiture de location, vous lui confiez votre répertoire. La plupart du temps, ce répertoire n'est pas effacé ! Cela ne devrait pas être possible ! C'est contre cela que nous mettons en place une technologie comme Masq.

M. Pierre Ouzoulias. - Vous avez dit que vos algorithmes de recherche étaient brevetés. Vous acceptez donc de les voir un jour tomber dans le domaine public. Est-ce à dire que ce n'est pas là que se situe la supériorité de votre moteur de recherche ?

Par ailleurs, un certain nombre de vos données sont accueillies par le *cloud* Azure de Microsoft, société américaine. Quelle protection pouvez-vous assurer aux données françaises face au *Cloud Act* ?

M. Éric Léandri. - Tout d'abord, nos brevets ne portent pas sur les algorithmes en eux-mêmes, mais ils donnent une idée globale de notre classement de l'internet. Ces brevets peuvent tomber un jour dans le domaine public, mais je pense qu'on les aura ouverts bien avant.

L'idée de Qwant est en effet depuis toujours de mettre un maximum d'éléments en *open source*. Masq est en *open source*, tout comme l'application Qwant pour mobiles. Tout le *front* de Qwant est également disponible en *open source*, ainsi que les indexeurs et les systèmes pour effectuer des graphes. Nous sommes aujourd'hui le moteur de recherche à avoir ouvert le plus grand nombre d'éléments.

Notre seul problème, c'est le classement, car si on choisit l'*open source* sans avoir parfaitement sécurisé celui-ci, on permet aux spécialistes du référencement de tricher à partir de nos résultats de recherche. C'est un problème qu'on a tous. Cela ne m'empêche pas de vous montrer comment je construis l'ensemble du système ou de vous donner la possibilité de voir nos

algorithmes en *open source*. Cela m'empêche simplement de vous dire comment je fais mon classement et la façon dont sont affichés les résultats.

J'ai proposé de lancer un concours de *SEO*, ces spécialistes du référencement sur les moteurs de recherche. En octobre-novembre, durant cinq mois, les meilleurs *SEO* français vont pouvoir tester nos algorithmes, donner des idées et voir si nous avons fait du bon travail pour éviter les *spams*.

Pour cela, j'ai besoin d'achever la deuxième partie de notre infrastructure...

Quelles données pourraient être soumises au *Cloud Act* dans le cadre de notre accord avec Microsoft ? Il s'agit de dizaines de milliards de pages internet. Pourquoi sommes-nous sur le *cloud* Azure et chez Microsoft et non chez OVH ? Microsoft est le deuxième plus grand moteur de recherche de la planète. Il a réalisé son *cloud* pour son moteur de recherche, avec des technologies spécifiques. C'est pourquoi nous avons passé cet accord inédit, qui garantit à l'Europe un moteur de recherche souverain européen, un accord gagnant pour l'Europe, pour la France et pour Microsoft sur la partie *cloud* dont j'ai besoin pour indexer le web.

Il n'y a pas la moindre donnée personnelle sur les serveurs de Microsoft. Bien évidemment, ce n'est pas le cas si vous cliquez sur les publicités de Microsoft, mais cela ne dépend pas de nous. Notre accord avec Microsoft nous permet d'avoir un moteur de recherche de taille mondiale, avec nos infrastructures et un complément sur la recherche et l'indexation des pages et des images. Vous nous demandez d'être plus souverains : c'est exactement ce que nous offre cet accord.

On va donc aller au bout et même accélérer les choses afin de vous donner les meilleurs résultats disponibles aujourd'hui sur internet, avec des technologies européennes - la plupart françaises - et des partenariats technologiques comme ceux que nous avons avec l'Institut national de recherche en informatique et en automatique (Inria).

M. André Gattolin. - Je n'ai pas l'impression que l'Union européenne, la Banque européenne d'investissement (BEI), etc., soient très sensibles à ce produit à haute valeur ajoutée et au contact direct des citoyens qu'est Qwant. Quel est votre sentiment à ce sujet ?

M. Éric Léandri. - Chacun d'entre nous a mis de l'argent dans Qwant. Les premiers investisseurs sont tous privés, et représentent plusieurs millions d'euros. Nous comptons ainsi Axel Springer, qui représente 20 %, et la Caisse des dépôts et consignations.

La BEI nous a permis de contracter un prêt remboursable en trois ans, avec des taux particulièrement intéressants. Nous ne sommes pas les seuls aujourd'hui à y avoir accès. Ce prêt a servi à de nombreuses autres entreprises européennes et leur a permis d'avancer. Ce type de prêt est fait

pour aider les entreprises européennes. Voilà ce que l'Europe a fait pour Qwant.

Par ailleurs, je suis président de l'*Open Internet Project*. Les milliers d'entreprises qui sont derrière sont celles qui ont fait une demande auprès de la Commission européenne pour examiner l'abus de position dominante de mon concurrent principal sur la partie *shopping*. Mme Vestager, grâce à son action, a permis de récolter 2,4 milliards d'euros.

Nous avons continué avec Android - le litige s'est soldé par une amende de 4,2 milliards d'euros. Qwant est le seul plaignant européen à demander l'accès au téléphone. Vous me demandiez comment nous bloquer. C'est facile : jusqu'à il y a peu, un fabricant de téléphone ne pouvait installer Qwant sur ses appareils. Il fallait aller dans Google Play et demander l'accès. Aujourd'hui, au démarrage du Play Store de Google, on vous demande de choisir entre Google, Ecosia, Qwant, Bing et autres moteurs de recherche. D'autres navigateurs sont également proposés. C'est là une conséquence du travail de Margrethe Vestager.

À l'échelon européen, tout ce qui est en train de se passer entre les États-Unis et la Chine démontre que nous devons accélérer notre capacité à indexer l'ensemble de l'Europe dans le domaine des moteurs de recherche, avoir plus de puissance dans le cas d'un *cloud* de type OVH, et développer la 5G avec Nokia. Je rappelle que Nokia est la deuxième société la plus avancée en matière de 5G et qu'elle est européenne.

Le modèle européen me convient sur beaucoup de points, mais un seul me pose problème : il est en effet quasiment impossible de créer un produit, de le rendre rentable et d'accélérer en même temps son développement. On doit à un moment choisir entre la possibilité de disposer de davantage d'ingénieurs afin de pouvoir indexer l'Europe ou continuer à se développer en étant rentable mais à petite échelle. Il faut avoir le choix - sans opter pour autant pour un modèle comme Uber, qui passe en bourse à 84 milliards de dollars en perdant 3 milliards de dollars ou 4 milliards de dollars par trimestre ! On ne peut créer des produits porteurs sans investissement ni ingénieurs. On ne peut mettre en place un moteur de recherche européen sans des centaines de serveurs. Cela prend du temps. Il va donc falloir régler cette question de coexistence de trois besoins différents : faire un produit rentable, accélérer son développement et être en capacité d'accélérer quand il le faut.

Qwant est un moteur de recherche. Les moteurs de recherche relèvent du domaine de l'industrie, non de celui des *start-up*. On ne cherche pas de *business model*. On le connaît très bien. C'est Omid Kordestani, numéro 3 de Google, qui l'a inventé avec AdWords, grâce auquel Google touche de l'argent lorsqu'on clique sur une annonce. C'est le principe des moteurs de recherche. Il fonctionne très bien et rend un moteur de recherche rentable dès lors qu'il a suffisamment de requêtes quotidiennes.

Ne vous y trompez pas : les bascules de l'administration, des banques, des grands groupes nous amènent à devenir très rentables, et c'est certainement le bon moment pour nous attaquer. Avec les bascules que nous avons aujourd'hui, nous estimons être à 5 % ou 6 % du marché français et avoir une très forte croissance sur les autres marchés. Entre la semaine dernière et aujourd'hui, notre chiffre d'affaires a crû d'environ 19 % par jour grâce à un plus grand trafic.

La souveraineté numérique passe par des outils qui respectent les citoyens et doivent fournir des résultats de très bonne qualité.

M. Gérard Longuet, rapporteur. - Procédez-vous à des investissements spécifiques pays européen par pays européen pour vous développer en adaptant votre projet aux réalités nationales, ou s'agit-il d'une démarche standard ?

M. Éric Léandri. - Tout dépend. La version Qwant junior comporte un volet que nous avons travaillé avec le ministère de l'éducation. En Allemagne, en Italie, nous formulons une demande auprès des ministères concernés pour que les résultats correspondent aux souhaits du gouvernement et surtout aux sites qui ont été référencés comme étant parfaitement adaptés à l'éducation des enfants.

Pour Qwant lui-même, nous avons aujourd'hui, grâce à l'intelligence artificielle, la capacité de travailler dans plusieurs pays et avec plusieurs langues à partir de la France. Certains pays comme la Suisse exigent la mise en place de serveurs destinés à anonymiser l'IP suisse. Celle-ci ne doit pas sortir du pays, c'est la législation. Nous nous adaptons donc en fonction des lois en vigueur.

Il faut ajouter des serveurs et de la puissance de calcul pour chaque pays où nous nous implantons, mais nous n'avons pas besoin de discuter avec chaque gouvernement.

L'effet d'entraînement est considérable : en prouvant qu'il est possible de basculer sur un moteur de recherche éthique, responsable, respectueux de l'ensemble des obligations européennes, du RGPD, de la protection de nos enfants et responsable sur le plan social et environnemental, on crée un précédent mondial et on apporte la preuve que respecter les règles, la législation, les obligations fiscales correspond à nos valeurs et à notre façon de considérer le monde.

M. Franck Montaugé, président. - Qu'attendez-vous des pouvoirs publics, eu égard à leur stratégie en matière de souveraineté numérique, pour faciliter et accompagner votre développement ? Repérez-vous des points faibles dans la stratégie de l'État français en la matière ?

M. Éric Léandri. - Tout a changé ces trois ou quatre dernières années pour l'ensemble des *start-up* françaises et européennes. Il était auparavant très difficile de discuter avec les pouvoirs publics, les chambres de

commerce, les différentes régions ou même avec les grandes entreprises. Ce n'est plus le cas aujourd'hui. Nous avons des passerelles, des ponts, des possibilités grâce à la *French Tech*, à nos ambassades, nos consulats, ou Business France, qui accomplissent un très gros travail.

Nous avons cependant un problème en matière de droit de la concurrence au niveau européen. Au niveau français, nous disposons dans notre arsenal de mesures conservatoires qui portent un arrêt à l'abus de position dominante. Mais ces mesures conservatoires ne seront jamais utilisées au niveau européen, car on doit prouver l'irréversibilité du dommage causé à l'entreprise. Or, si c'est irréversible, la société a déjà fermé le temps qu'on parvienne à le prouver. Je ne comprends pas le droit européen dans ce domaine.

Certaines règles européennes sont en outre assez étranges. Sur le plan européen, on peut détenir une position dominante « si on n'en abuse pas ». À l'échelle de l'Europe, personne n'a jamais 95 % du marché ! Que signifie ne pas abuser de sa position dominante quand on est condamné à payer des amendes de 50 millions d'euros pour non-respect du RGPD, de 2,4 milliards d'euros pour le commerce en ligne, et de 4,2 milliards d'euros pour le système d'exploitation Android ? Ne pourrait-on pas faire comme aux États-Unis où, quand on dépasse un certain niveau de parts de marché, on n'a plus le droit de faire quoi que ce soit pour se maintenir à ce niveau ?

Énormément de choses ont été faites en Europe pour aider les entreprises. Nous avons gagné le premier set, ainsi que le deuxième, en décidant de travailler tous ensemble. Ce n'est pas le moment de recommencer à perdre : il faut au contraire accélérer !

Nous pouvons installer Qwant dans toutes les administrations : faisons-le ! Vous en avez le courage, sans quoi vous n'auriez pas créé cette commission d'enquête et mis ce genre de problématique sur la table. Ce Gouvernement en a le courage. De grandes banques, de grandes entreprises, des millions d'utilisateurs le font déjà. La BEI passe à Qwant. *Die Welt*, l'un des plus grands journaux allemands, utilise également Qwant, tout comme le *Corriere della Serra*, ou la *Gazzetta dello Sport* en Italie. Une ville près de Milan vient également de passer à Qwant. Il va falloir aller jusqu'au bout, car nous n'aurons pas de deuxième chance. À partir de 2021-2022, il faudra tenir compte des Chinois.

Il ne faut pas opposer les Américains, les Chinois et les Européens, mais les entreprises qui choisissent de protéger la vie privée, de recourir à l'intelligence artificielle éthique, de placer l'*open source* au coeur de leur stratégie et les autres. C'est pour cela que j'ai décidé de travailler avec Microsoft. Certaines entreprises ont décidé de savoir tout sur tout, de bloquer la concurrence. C'est pourquoi je ne travaille pas avec elles. D'autres feront peut-être demain du *dumping* sur les prix. La souveraineté, notre façon de travailler et nos choix doivent être dictés par nos valeurs européennes.

M. Pierre Ouzoulias. - Qwant fonctionne en corse, en breton, en catalan, en basque. À quand l'occitan ?

M. Éric Léandri. - Je précise que Qwant fonctionne également en gaélique, en écossais, en irlandais. Je n'ai pas choisi que des autonomistes - même si ce n'est pas l'endroit pour ce genre de remarque ! Qwant fonctionne dans toutes ces langues pour une raison culturelle. En Corse, la plupart du temps, les gens ont *Corse Matin* sous le bras, rarement *Le Parisien*. On a donc placé *Corse Matin* en premier dans les réponses liées à l'actualité, mais *Le Parisien* est juste derrière. Personne n'est ostracisé. Ce serait avec plaisir que nous proposerions Qwant en occitan, mais il n'existe pas de nom de domaine dans cette langue. Nous avons en fait indexé tous ceux qui en possèdent. Nous sommes sur le point d'ajouter l'alsacien. Je précise cependant que nous sommes sur Occitanie Data. Dès que vous aurez un nom de domaine, nous l'indexerons sur internet avec grand plaisir.

M. Gérard Longuet, rapporteur. - On connaît Qwant, on sait ce que représente le défi que vous relevez, on a de la sympathie pour votre combat, et on s'intéresse à ce que vous faites par le biais des dispositions législatives et fiscales.

Je retiens votre formule à propos du courage qu'il faut avoir d'y aller. Il faut aussi défendre la souveraineté par des gestes appropriés. C'est ce que vous faites, et vous nous invitez à le faire.

M. Franck Montaugé, président. - Merci.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible en ligne sur le site du Sénat.

Audition de M. Cédric O, secrétaire d'Etat auprès du ministre de l'Economie et des Finances et du ministre de l'Action et des Comptes publics, chargé du Numérique,
le 20 juin 2019

M. Franck Montaugé, président. - Mes chers collègues, notre commission d'enquête poursuit ses travaux avec l'audition de M. Cédric O.

Cette audition sera diffusée en direct sur le site Internet du Sénat. Elle fera également l'objet d'un compte rendu publié.

Enfin, je rappelle, pour la forme, qu'un faux témoignage devant notre commission d'enquête serait passible des peines prévues aux articles 434-13, 434-14 et 434-15 du code pénal. Monsieur O, je vous invite donc à prêter serment de dire toute la vérité, rien que la vérité, levez la main droite et dites : « *Je le jure.* ».

Conformément à la procédure applicable aux commissions d'enquête, M. Cédric O prête serment.

M. Franck Montaugé, président. - Depuis avril dernier, vous êtes secrétaire d'État auprès du ministre de l'Économie et des Finances et du ministre de l'Action et des Comptes publics, chargé du Numérique. Autant dire que vous êtes l'un des acteurs publics les mieux à même de venir répondre aux questions de notre commission d'enquête !

Je commencerai donc, logiquement, par vous demander comment vous appréhendez cette notion de souveraineté numérique. Est-ce une idée que vous revendiquez ? Comment la défendre ? Avez-vous un « plan de bataille » sur ce sujet ?

Un pays ne peut être souverain s'il ne parvient pas à réglementer les activités qui affectent son territoire. Quelle est votre approche de la régulation des géants du numérique ? Doit-on distinguer chaque secteur ? Prévoir un régime général des plateformes ? Doit-on réglementer ou co-réguler ?

Un pays ne peut également être souverain sans technologies clés. Vous avez récemment affirmé que « la défense de nos valeurs passe par l'émergence de champions technologiques européens ». À quelles technologies pensez-vous en particulier et comment pensez-vous faire émerger ces « champions » ? Le directeur général des entreprises a évoqué les semi-conducteurs, le supercalculateur et l'intelligence artificielle. Il a évoqué le « *cloud* de confiance » défendu par Bruno le Maire et, à terme, les ordinateurs quantiques.

Enfin, notre rapporteur vous interrogera sur les cryptomonnaies. J'aimerais aussi que vous vous exprimiez sur la technologie des blockchains et son impact sur notre souveraineté nationale.

M. Cédric O, secrétaire d'État auprès du ministre de l'Économie et des Finances et du ministre de l'Action et des Comptes publics, chargé du Numérique. - Avant d'être nommé ministre en charge du numérique, je me suis occupé à l'Élysée à la fois des sujets numériques et des participations de l'État, donc de grandes entreprises comme Thales, EDF et de toutes celles où la BPI est au capital. J'ai donc eu l'occasion de voir assez largement le sujet technologique du point de vue de l'État, un sujet absolument fondamental dans le numérique.

Mon propos sera d'abord économique : si l'on veut être au meilleur niveau technologique pour défendre nos intérêts, on doit avoir les meilleures entreprises du monde et un écosystème au meilleur niveau mondial en termes d'investissement ou de R&D. En 2017, nous avons lancé un travail sur l'intelligence artificielle, avec un énorme sentiment d'urgence : les grandes entreprises américaines investissent chaque année 30 à 40 milliards d'euros, tout comme les entreprises et l'État chinois, selon les chiffres de 2016. Le montant investi par l'Europe dans son ensemble ne s'élève lui qu'à 4 ou 5 milliards d'euros. L'intelligence artificielle n'est pas une technologie en soi, elle vient irriguer l'ensemble des secteurs de l'industrie, de la défense, de l'aéronautique, de la mobilité, de la cybersécurité. Cette différence d'investissements ne prépare que du chômage et la sortie technologique de l'histoire de l'Europe : il y a donc un impératif absolu à ce que l'Europe en général, et la France en particulier, prennent conscience qu'elles ont l'obligation d'investir dans des technologies critiques pour défendre leurs emplois et leur souveraineté.

Je veux commencer par cette approche offensive, condition de tout : nous devons faire émerger des champions parce qu'une stratégie qui ne se concentrerait que sur une approche défensive de régulation ou de législation ne fonctionnerait pas. En effet, dans le numérique, nous sommes toujours dépassés par les usages. Nous avons tous certaines réserves sur la domination que les GAFA exercent sur le monde, mais nous utilisons tous leurs produits. Si l'on veut imposer notre souveraineté, nos normes et notre modèle social dans un modèle internet qui est celui du *winner-takes-all*, on doit aussi avoir des vainqueurs qui prennent tout. Cela nécessite des actions transversales pour le développement de cet écosystème, et notamment le financement, qui doit d'abord être privé. Quand on parle de 30 à 40 milliards d'euros par an, aucun État n'est capable de dépenser autant dans une seule technologie. Pour avoir du financement privé, il faut augmenter la part du capital qui va vers les entreprises et attirer les investisseurs privés, notamment étrangers.

Le deuxième sujet est celui de la formation. Aux États-Unis, le numérique représente entre un tiers et la moitié des emplois nets créés bien loin du niveau atteint en France ou en Europe. Pour préparer les emplois à tous les niveaux de qualification, on doit accélérer sur le sujet numérique. On le fait déjà : 2,8 milliards d'euros investis dans les *start-up* françaises il y a

deux ans, 3,5 milliards l'année dernière et 5 milliards cette année. Nous avions trois licornes - ces entreprises valorisées plus d'un milliard d'euros - en 2017, et neuf aujourd'hui, dont quatre ou cinq apparues ces quatre derniers mois. Cette accélération constatée au sein de l'écosystème des *start-up* ne suffit pas : il faut aussi y impliquer les grands groupes et les ETI-PME. Le premier facteur qui limite l'expansion de cet écosystème en France et en Europe, c'est la formation : aujourd'hui 80 000 postes ne sont pas occupés dans le secteur du numérique, à tous les niveaux de formation. On estime que ce sera 200 000 en 2022 et le chiffre de 900 000 postes ouverts et non pourvus en Europe circule.

Outre ces deux sujets transversaux que sont le financement et la formation, nous avons une approche plus « verticale » : l'Europe et la France ne peuvent pas se permettre d'être absentes d'un certain nombre de technologiques critiques - intelligence artificielle, calcul quantique, blockchain, semi-conducteurs... Il faut donc être capable de mettre les bonnes masses d'investissement et le bon effort public et privé sur un certain nombre de technologies, faute de quoi nous laisserons les clés de notre avenir économique et souverain aux mains des Américains et des Chinois.

C'est ce que le Gouvernement a commencé à faire avec une stratégie spécifique sur l'intelligence artificielle, à partir du rapport du député Cédric Villani. Une mission conduite par une parlementaire, un entrepreneur et un chercheur est également en cours sur le calcul quantique.

Il faut que les efforts entrepris au niveau national sur les nouvelles technologies - formation, investissements, stratégie - soient poursuivis au niveau européen, où l'on assiste à une vraie prise de conscience dans le cadre du programme de travail de la prochaine Commission.

La première clé de notre souveraineté, ce n'est pas la défense mais l'attaque, c'est-à-dire la capacité à se dire que c'est une priorité nationale. La France dépense 2,25% de son PIB en R&D, l'Allemagne est autour de 3%. Elle a pour ambition d'être à 3,5% en 2025. Ainsi, si nous restons à 2,25% en 2025 et que l'Allemagne atteint son objectif, les Allemands investiront chaque année 60 milliards d'euros de plus que la France. Nous devons avoir ces éléments en tête au moment des arbitrages budgétaires ; ces chiffres montrent l'ampleur du sujet et du problème. L'effort de recherche publique n'est, en fait, pas en cause, puisque nous sommes au-dessus des Allemands en termes de dépense publique, le problème concerne la recherche et l'investissement privés, d'un niveau bien inférieur. Il nous faut, là encore, créer un écosystème privé d'entreprises capables d'investir autant, voire plus, que nos principaux compétiteurs.

La partie plus défensive reste tout aussi indispensable. Il y a toujours eu des affrontements technologiques entre les grands blocs. Ce qui change aujourd'hui, c'est que nous voyons émerger des acteurs d'une taille inédite. Le problème n'est d'ailleurs pas tant leur taille que la manière dont

ils fonctionnent, puisqu'ils sont systémiques. Certains de ses acteurs, les Gafam, ont atteint une taille et bénéficient d'effets de réseaux, grâce à la masse des données dont ils disposent, qui en font des acteurs de base de pans entiers de notre économie. Facebook, par exemple, représente 2,4 milliards d'utilisateurs, dont 40 millions de Français. Cela pose des problèmes économiques et juridiques : ce sont des acteurs établis aux États-Unis et donc, lorsque l'on veut adopter une nouvelle législation, contre la propagation des discours de haine sur internet par exemple, on fait face à des complexités administratives : les conventions bilatérales entravent nos actions. Se posent aussi des problèmes technologiques : aujourd'hui, une bonne partie du quotidien des Français est régie par des algorithmes. Si nous voulons jouer notre rôle d'État et assurer aux Français que le traitement de leurs données est à la fois légal et juste, alors l'État doit être au bon niveau technologique pour comprendre, tester, décoder voire infirmer le fonctionnement des algorithmes. C'est particulièrement vrai pour l'intelligence artificielle, mais cela va se généraliser aux autres secteurs. Aujourd'hui, personne dans l'État n'est capable de parler avec les programmateurs de Facebook, ne serait-ce que parce que les salaires que proposent les Gafam leur permettent d'attirer les meilleurs. Si les seuls pays, hors des Etats-Unis, à savoir efficacement réguler les plateformes sont les pays autoritaires, c'est un problème pour nos démocraties. Si les citoyens estimaient que la puissance publique ne peut plus protéger leurs droits, ils pourraient se tourner vers des solutions plus radicales.

Sur la régulation de ces acteurs devenus systémiques, il convient d'appliquer une régulation spécifique, probablement trans-sectorielle. Le sujet n'est pas de savoir s'il faut une régulation spécifique sur les données, sur la vie privée, sur les contenus haineux, sur les rapports entre fournisseurs et sous-traitants, etc. Dès lors qu'un acteur est une brique de base de l'économie, alors une régulation systémique, qui peut ressembler à la régulation bancaire, à base de supervision, de régulateur technique dédié et de capacité technologique du régulateur au bon niveau, doit être développée. C'est ce que la France porte au niveau européen, le vrai niveau d'efficacité.

Le dernier sujet que je souhaitais aborder est celui de la capacité à défendre les intérêts européens dans certaines technologies critiques : la France et les États membres peuvent impulser, innover, mais, *in fine*, la masse critique nécessaire aux négociations avec les acteurs économiques, et leurs pays d'origine, n'est autre que le marché européen fort de 500 millions de consommateurs ; le marché français ne suffit pas. Nous devons donc définir des règles communes de souveraineté européenne. Les choses progressent - par exemple le contrôle des investissements étrangers -, d'autres restent à mettre en place - sur le *cloud* ou la 5G. Là-encore, il faut prendre conscience que la question de la souveraineté européenne est essentielle. Il y a donc toute une partie défensive, qui vient en complément

de la partie offensive, la seule à pouvoir garantir notre souveraineté à long-terme.

Le sujet de l'identité numérique est un autre élément transversal et essentiel : il n'y a rien de plus régalien ou souverain que l'identité, et c'est un bon exemple du défi qui est posé à l'État. Les usages dans le numérique bousculent les pratiques : l'État peut certes développer une carte d'identité numérique mais si elle n'est pas pratique ou aussi simple d'usage que le dispositif d'identité numérique développé par Google ou Facebook, alors les citoyens ne l'utiliseront pas. Pour tous les usages privés qui nécessitent une identification forte - ouvrir un compte en banque, etc. - ils utiliseront les dispositifs les plus faciles à utiliser. L'État a donc une obligation de résultat. Il doit penser et développer des solutions qui sont au bon niveau technologique et au bon niveau d'usage. Ce sujet va rapidement arriver au Parlement puisque toutes les cartes d'identité seront changées en 2021.

M. Patrick Chaize. - Le constat que vous dressez est partagé, et il est redoutable : une quasi absence de la France sur plusieurs sujets clés... mais nous restons sur notre faim concernant les pistes concrètes pour y remédier. Est-ce à dire, à vous entendre, qu'il est déjà trop tard pour réagir et conserver notre souveraineté numérique ?

Nous sommes pourtant confrontées à des initiatives régulières qui font peser de vrais risques à cet égard, comme en témoigne encore récemment l'annonce du lancement prochain d'une monnaie électronique. Quel est votre avis sur ce sujet ?

Des comités de normalisation fixent les règles techniques à l'échelle mondiale. Il en existe deux principaux, en Europe et aux États-Unis. Alors que nous pesions en leur sein ces dernières années, on constate aujourd'hui que peu d'européens y siègent : comment redonner du poids à nos positions et inciter nos chercheurs à s'investir dans leurs travaux ?

Vous avez, à juste titre, indiqué que le niveau européen était l'échelon le plus adapté pour agir, mais quelle structure précisément nous permettra-t-elle de peser ?

Concernant les infrastructures, petite lueur d'optimisme personnel, il me semble que la France a fait des choix ambitieux qui devraient donnent une longueur d'avance sur ses concurrents. Comment capitaliser sur ces choix nationaux stratégiques ?

M. Cédric O. - Nous pouvons effectivement être optimistes ; d'abord, la compétition mondiale pour la technologie est essentiellement une compétition pour le recrutement des talents. Or l'excellence de l'école française et de nos ingénieurs, mathématiciens et informaticiens est reconnue - la présence de Français à la tête des départements d'intelligence artificielle de plusieurs géants du numérique en atteste. La question reste bien sûr de savoir comment les garder ou les faire revenir en France.

En outre, la psychologie de nos entrepreneurs est particulièrement porteuse : nos jeunes ne veulent plus travailler dans la banque mais se donnent comme objectif d'être les Mark Zuckerberg de demain. En témoigne le nombre de « licornes » françaises, ces entreprises valorisées à plus d'un milliard d'euros : elles étaient trois lors de l'élection d'Emmanuel Macron, elles seront 25 à 30 d'ici 2025 ou 2030, et l'état d'esprit de leurs dirigeants est bien celui des dirigeants qui ont créés les géants américains actuels : une ambition à toute épreuve.

J'en viens au détail des actions que nous envisageons de mener.

Notre premier sujet est celui de l'investissement. Investissement sectoriel d'abord, dans certaines technologies, comme l'intelligence artificielle, en faveur de laquelle l'État débloquera 1,5 milliard d'euros en 3 ans. Cela peut sembler comparativement modeste, mais c'est inédit et cela doit favoriser le développement d'un véritable écosystème de recherche en la matière, comme en attestent les annonces de recrutements et de créations de laboratoires en France par les grands groupes du secteur.

Le véritable problème de financement auquel nous souhaitons nous attaquer est celui des « gros tickets », ces levées de fonds réunissant plus de 100 ou 200 millions d'euros. Malgré des réussites ponctuelles - encore tout récemment un record a été battu avec les 205 millions d'euros récoltés par Meero -, le financement de ces grosses levées de fond reste difficile. Cela s'explique, notamment, par la structure du financement de l'économie en France et en Europe et nous y travaillons avec les investisseurs institutionnels. Nous pouvons agir à législation constante, des annonces seront faites en septembre. Le marché boursier est l'autre sujet qui concentre toute notre attention en matière de financements : nous n'avons pas de Nasdaq européen. Philippe Tibi, professeur à l'École polytechnique, a été missionné pour travailler sur ce sujet, ses conclusions donneront lieu à plusieurs annonces également à la rentrée.

Concernant la régulation, nous avançons aussi : la proposition de loi dite « Avia » de lutte contre les contenus haineux sur internet envisage une approche particulièrement intéressante de régulation des réseaux sociaux, calquée sur celle - systémique - que connaît déjà actuellement le secteur bancaire. Elle ne concerne actuellement que le sujet de la haine en ligne mais, le principe pourrait très bien ensuite être décliné pour d'autres sujets. Nous en discutons d'ailleurs au niveau européen. Le parallèle avec la régulation bancaire semble particulièrement adapté : une banque ne peut, certes, être tenue responsable d'un virement frauduleux réalisé par son biais, mais elle est responsable de la mise en place d'un système de contrôle interne efficace pour l'empêcher, supervisé et audité par le régulateur. De façon générale, la puissance publique n'a pas la capacité de vérifier tout ce qui se passe sur les plateformes, elle doit donc pousser les plates-formes à mettre en place des systèmes humains et technologiques à cet effet, et être capable de les auditer. À cet égard, vont bientôt être rendues publiques les conclusions des travaux

de Marie-Anne Frison-Roche, professeur de droit à Sciences-po, sur la « compliance » - ou approche par la supervision.

Vous m'avez interrogé sur la « monnaie Facebook », bien mal nommée s'agissant d'un projet porté par une trentaine de partenaires - dont Visa et Mastercard, ainsi que l'entreprise française Illiad - et s'agissant d'un système qui ne s'apparente pas aux crypto-monnaies sans sous-jacent - à chaque Libra devrait ici correspondre un panier d'unités monétaires très classiques. En ce sens je ne vois pas de risque de dépossession de la souveraineté monétaire des États dans la présentation du projet telle qu'elle a été faite. Les pays du G20 vont missionner Benoît Coeuré pour travailler sur ce sujet. Outre la question purement monétaire, une vraie question est soulevée par les normes applicables à ces services de paiement : derrière le choix des lois applicables, il y aura aussi un enjeu critique de souveraineté. Rappelons toutefois qu'à ce stade, ce n'est encore qu'un projet - prévu pour l'horizon 2020 - qui répond d'ailleurs à des besoins réels, comme l'accès du plus grand nombre au paiement en ligne, mais qui appelle toute notre vigilance et celle des régulateurs.

Je partage votre préoccupation sur le désinvestissement des européens des instances de normalisation comme le World Wide Web Consortium (W3C), alors que d'autres, comme les Chinois, ont compris l'intérêt stratégique d'y peser.

Concernant enfin l'Europe, il me semble que le sujet de la souveraineté numérique mérite d'être porté à cette échelle directement par l'ensemble de la Commission européenne. Imaginons que l'Europe prenne la décision de démanteler une grande plateforme américaine pour des raisons démocratiques ou d'innovation - l'idée circule après tout dans le débat académique américain -, il ne faut pas perdre de vue que les seuls acteurs économiques qui nous garantissent actuellement un niveau d'investissement substantiel dans des secteurs aussi importants que l'intelligence artificielle, ce sont bien les GAFA et les acteurs chinois : 30 à 40 milliards d'euros investis de part et d'autre. Il faut donc pouvoir penser en même temps tous les aspects du sujet : l'antitrust et la politique commerciale. Seule la Commission européenne me semble à même d'avoir cet aspect transversal.

Concernant l'innovation, le projet de création d'une DARPA (Defense Advanced Research Projects Agency) pour l'Europe avance. L'agence d'innovation américaine, très liée au secteur de la défense, investit énormément sur des technologies clés : SpaceX utilise ainsi une technologie développée dans ce cadre, et bénéficie donc d'argent à l'origine public. Le budget de la DARPA -3 milliards d'euros par an - et les risques énormes consentis contribuent à asseoir la domination technologique américaine, mais ce n'est évidemment pas transposable tel quel en Europe. Après avoir porté le sujet avec nos partenaires allemands, la Commission européenne a déjà fait des annonces qui devraient aboutir au sein d'un prochain Conseil

européen de l'innovation. Mais cela implique aussi d'accepter de prendre des risques et d'être prêt à abandonner l'idée de juste retour national...

M. André Gattolin. - Face à nos État nations reposant sur des territoires, nous avons vu se développer des acteurs transnationaux et systémiques - des « quasi États », avec bientôt leur monnaie - qui reposent eux sur une idéologie apolitique et purement solutionniste...

Créer des champions, des « licornes », c'est naturellement une bonne chose, mais encore faudra-t-il les garder et ne pas se retrouver, comme dans la situation israélienne, à servir d'incubateur aux géants américains. Contrôle du capital, levée des obstacles à l'accès au marché... comment bien accompagner financièrement et juridiquement ces efforts d'investissement européens pour qu'ils ne profitent pas, *in fine*, à d'autres ?

M. Cédric O. - Il faut qu'un écosystème soit international pour être dominant : acheter et être acheté fait partie de la vie normale des entreprises. Nous ne pouvons interdire de façon générale les acquisitions par des investisseurs internationaux, et pour qu'une entreprise soit achetée il faut aussi qu'il soit possible de la vendre. À part dans le cas limité de secteurs touchant à la sécurité nationale, je n'ai donc aucun problème à ce que des entreprises françaises se fassent racheter par des entreprises américaines. Cela n'a pas vocation à être la règle, mais il n'y a aucune raison de l'empêcher, car nous ne pouvons nous passer d'investisseurs étrangers et c'est l'amorce même d'un système vertueux de financement : les petits tickets amènent les gros, les capital-risqueurs attirent les fonds de pensions et les institutionnels. Autre exemple : Dans le domaine de l'intelligence artificielle, les meilleurs talents sont chez les géants du numérique ; pour créer en France un écosystème de recherche sur ce sujet, il faut donc avoir attiré ces grandes entreprises et permettre à leurs talents d'enseigner en les intégrant à notre système de formation. Il nous faut donc rester sur cette ligne de crête : favoriser le développement de champions et rester ouverts aux investisseurs étrangers.

M. Pierre Ouzoulias. - Le Gouvernement a demandé au Sénat de voter une loi sur la manipulation de l'information : a-t-elle été utile ?

Dans nos auditions, le sujet du logiciel libre comme instrument pouvant aider à reconquérir notre souveraineté nationale est revenu à plusieurs reprises. Quel est le plan proposé par votre Gouvernement pour développer l'usage des logiciels libres ? Ne serait-il pas intéressant que le Gouvernement apporte une aide aux associations bénévoles qui développent ces logiciels ? Cela permettrait de garantir la pérennité de ces solutions informatiques transparentes, qui répondent à un objectif de souveraineté numérique en permettant d'accéder au code-source.

M. Cédric O. - Nous n'avons pas eu d'alertes sur une immixtion problématique lors des élections européennes. Le dispositif introduit par la loi n'a donc pas été testé « en conditions réelles ». Nous avons cependant

connu quelques difficultés de mise en oeuvre. Par exemple, pour chaque vidéo, s'il y a une publicité, la loi impose d'afficher qui l'a payée, quel public est visé... Certaines plateformes ont considéré que c'était trop compliqué à mettre en oeuvre et n'ont donc diffusé aucune vidéo à caractère politique, y compris celle du gouvernement français incitant les citoyens à aller voter. Si nous demandons des choses totalement infaisables aux plateformes, nous nous exposons à ce genre de réaction. Il faut donc que ce soit mordant... mais faisable. Ces plateformes sont souvent protégées par des conventions bilatérales qui nous empêchent d'aller aussi loin que nous le souhaiterions, et s'assurer de l'applicabilité des normes que nous votons est donc essentiel.

Je suis un grand défenseur du logiciel libre. Pour autant, pour qu'un logiciel fonctionne, il faut qu'il y ait une communauté derrière, ce qui ne se décrète pas, même si l'État lui-même, et notamment la DINSIC, peuvent le promouvoir. Par exemple, le dernier système de messagerie « Tchap » développé par la DINSIC vient d'un logiciel libre. Nous sommes donc promoteurs du logiciel libre, mais ce n'est pas la solution à tout. Il faut trouver le bon équilibre. Quant à un éventuel soutien aux associations, c'est avant tout un sujet de communauté d'utilisateurs et de produits.

M. Gérard Longuet, rapporteur. **-** Parmi les approches des entreprises du numérique développées par des pays tiers, on observe une grande différence entre la perspective d'un système démantelé, à l'image de ce qu'ont fait les États-Unis dans le pétrole et les télécoms, et le système chinois, dans lequel la séparation entre la décision politique et les entreprises n'est pas claire. Les Européens n'ont bien sûr pas la possibilité de démanteler les GAFA mais ils peuvent en accompagner la demande. Est-ce que celle-ci vous paraît aujourd'hui probable aux États-Unis ou l'excluez-vous totalement ?

Vous avez également évoqué les financements en matière de défense aux États-Unis. La transposition en Europe est très difficile, les pays européens étant profondément divisés en matière de défense, un certain nombre d'entre eux considérant que leur véritable défense est l'intégration dans l'OTAN avec le rôle prééminent des États-Unis. On imagine mal ces pays décider de financer par des budgets européens une recherche qui puisse être conflictuelle.

Quel est donc l'intérêt européen vis-à-vis des entreprises américaines : doit-on considérer qu'elles sont incontournables et qu'elles équilibrent leurs homologues chinoises ? Ou que leur démantèlement permettrait de rééquilibrer les intervenants sur ce marché ?

Enfin, quel jugement portez-vous sur Qwant ?

M. Cédric O. - La question du démantèlement se pose en soi et pour soi. Le livre de Tim Wu, *The Curse of Bigness*, paru récemment aux États-Unis, dresse un parallèle entre le démantèlement de la Standard Oil et d'AT&T et ce qui se passe aujourd'hui avec les GAFA. Il appelle à leur démantèlement

en disant que l'approche récente et centralisée de la politique anti-concurrence sur le prix que paie le consommateur n'est pas l'objectif politique qui a présidé à la création des lois antitrust : une entreprise trop grande pose par essence des problèmes démocratiques, économiques... Le sujet progresse au niveau américain, à l'intérieur des États-Unis, notamment au sein du camp démocrate. Je crois assez peu à l'idée que les Européens seraient en position d'imposer ces éléments-là, fût-ce pour des raisons d'innovation ou de démocratie. J'ai qualifié cette approche d'excessivement agressive non pas en soi, mais parce que je pense que c'est excessivement agressif pour les plateformes et que les États-Unis ne nous laisseront pas faire. Quoi qu'on en pense, ce sera d'abord une affaire américaine. Au-delà du démantèlement, la question de la régulation se pose de manière plus urgente : même si Facebook était divisé par 10, cela ferait toujours 240 millions d'utilisateurs par entité et cela n'aurait réglé aucun problème lié à la protection de la vie privée.

Même pour l'Europe, la question de l'antitrust se pose en même temps que la politique commerciale. Dans un certain nombre de secteurs de l'intelligence artificielle, les entreprises chinoises, parce qu'elles ne respectent pas les mêmes règles, seront plus fortes que les entreprises américaines et européennes. Devons-nous laisser entrer de telles entreprises sur le marché européen ? C'est pour cela qu'il faut réfléchir de manière transversale. Il ne faut pas oublier une partie du problème : certes les acteurs trop gros sont problématiques mais se focaliser sur la taille de ces acteurs ne permet pas de bien appréhender l'ensemble des problèmes qu'ils posent.

Si les Européens créent une agence de l'innovation, ce ne sera pas sur les sujets défense. Par ailleurs, la DARPA investit aussi dans des entreprises, y compris européennes, qui développent des technologies civiles. Il y a des continuités entre défense et civil. Le sujet de la souveraineté, y compris dans la défense, est d'abord un sujet économique : il faut avoir des acteurs suffisamment puissants pour faire de la R&D.

Qwant est une vraie réussite, malgré une part de marché limitée. C'est le seul qui grignote des pourcentages de parts de marché à Google en France et en Europe. Nous faisons ce que nous pouvons pour les aider à se développer. Qwant remplissant certaines conditions, notamment en matière de protection des données, nous avons décidé de recommander son installation par défaut sur les ordinateurs des administrations françaises. À court-terme, ce ne sera toutefois pas un élément de souveraineté, sauf pour l'utilisateur qui fait le choix de ne pas fournir ses données aux GAFA. À court terme, Qwant n'est en effet pas un compétiteur du niveau, ni même du dixième de niveau, de Google.

M. Gérard Longuet, rapporteur. **-** Est-ce qu'il y a au gouvernement une réflexion sur la gestion des données et la consommation d'énergie ? Nous avons un projet de programmation pluriannuelle de l'énergie (PPE) qui ne prend manifestement pas en compte ce que peut représenter la

consommation énergétique liée à la gestion des données. Est-ce que ce sujet fait l'objet d'un rapprochement des points de vue ? Cette question se posera si on défend l'idée d'un *cloud* protégé ou d'un hébergement des données sur le territoire national ou européen.

M. Cédric O. - La plus grande partie de la consommation d'énergie liée aux données des Français n'est pas en France, il me semble. Le sujet du *cloud* souverain est important. La consommation d'énergie du numérique de manière générale est un sujet de préoccupation. C'est le cas par exemple pour la *blockchain*. Il est vrai qu'on n'a pas lié les données et la PPE. À court-terme, je considère à titre personnel que les sujets prioritaires sont davantage ceux de la sécurisation des données et de la capacité à développer un *cloud* souverain. Le sujet écologique doit en faire partie, mais ce n'est pas le premier.

M. Franck Montaugé, président. - Quelle est la position du Gouvernement sur le statut juridique des données ? Quelle responsabilisation pour ceux qui utilisent ces données ? Faut-il prévoir une localisation géographique en France des infrastructures - datacenters, plateformes ? On évoque souvent l'intérêt de développer un système d'exploitation (OS) souverain, est-ce une piste à creuser ? Quel développement européen dans le secteur des supercalculateurs ?

Enfin, si le commissariat aux communications électroniques de défense (CCED) dépend bien de votre ministère, considérez-vous qu'il a bien actuellement les moyens de ses missions ?

M. Cédric O. - Sur cette dernière question, je souhaite vous répondre précisément mais n'étant pas complètement sûr d'en avoir effectivement la tutelle, je vous propose de revenir vers vous ultérieurement par écrit.

Concernant les données et leur statut, sans que notre opinion soit définitivement faite sur le sujet, il nous semble d'abord que certaines pourraient être déclarées d'intérêt général. En outre, la portabilité des données est un enjeu essentiel, qui doit être posé au niveau européen et dans le cadre d'éventuelles régulations systémiques : pourquoi ne pas imposer des obligations renforcées en la matière à certains acteurs dominants, par exemple pour les données de géolocalisation. Il s'agit d'un mode de régulation que j'ai pu, récemment, qualifier d'« agressif », signifiant par là que pour pouvoir être imposé face à la capacité de résistance juridique des géants du numérique, il faudra agir à l'échelle européenne pour avoir tout le poids d'un marché de 500 millions de consommateurs.

Des obligations de localisation géographiques en France des infrastructures sont bien sûr importantes, mais insuffisantes. Si les données sont physiquement stockées en France cela ne suffit pas pour les protéger si elles relèvent d'opérateurs chinois ou américains.

Nous aurons un OS européen le jour où un acteur privé européen sera capable d'un investissement comparable à celui réalisé par Google,

Microsoft ou Apple. Là encore, n'oublions pas que c'est l'usager qui tranche : inutile de mobiliser autant de fonds si nos concitoyens préfèrent *in fine* utiliser celui des concurrents privés américains... La véritable solution passe par le développement d'un véritable écosystème d'initiatives privées capables de faire concurrence à ces géants du numérique.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible en ligne sur le site du Sénat.

Audition de M. Nadi Bou Hanna, directeur interministériel du numérique et du système d'information et de communication de l'État au ministère de l'action et des comptes publics,
le 25 juin 2019

M. Franck Montaugé, président. - Notre commission d'enquête poursuit ses travaux avec l'audition de M. Nadi Bou Hanna, directeur interministériel du numérique et du système d'information et de communication de l'État au ministère de l'action et des comptes publics.

Cette audition sera diffusée en direct sur le site internet du Sénat. Elle fera également l'objet d'un compte rendu publié.

Enfin, je rappelle, pour la forme, qu'un faux témoignage devant notre commission d'enquête serait passible des peines prévues aux articles 434-13, 434-14 et 434-15 du code pénal.

Conformément à la procédure applicable aux commissions d'enquête, M. Nadi Bou Hanna prête serment.

M. Franck Montaugé, président. - Voilà quelques mois, vous avez pris la tête de la direction interministérielle du numérique et du système d'information et de communication de l'État, ou Dinsic, poste qu'occupait avant vous Henri Verdier, que nous avons également reçu dans le cadre de ses nouvelles fonctions.

Votre direction, placée sous l'autoritéì du ministre en charge du numérique et rattachée au secrétariat général du Gouvernement, a de très nombreuses missions. Ces dernières vont bien au-delà de celles d'une simple « DSI » de l'État, comme la Dinsic est parfois surnommée.

Le décret définissant ces missions la charge, par exemple, « par les réponses apportées aux besoins propres de l'État en matière de technologies de l'information et de la communication, de promouvoir l'innovation et la compétitivitéì dans ce secteur de l'économie nationale ».

Elle abrite également la mission Étalab, chargée de gérer la politique d'ouverture des données de l'État, ou encore l'incubateur des start-ups d'État.

Monsieur le directeur, l'informatique de l'État est au coeur du sujet de notre commission d'enquête relative à la souveraineté numérique. Je vous propose donc de nous présenter les actions de votre direction qui concourent au recouvrement, par notre pays, de sa souverainetéì numérique.

Dans la présentation de votre stratégie intitulée « Tech. Gouv », vous écrivez que « l'État doit retrouver la maîtrise de son environnement numérique ». Il l'aurait donc perdue... Dans cette situation dégradée, quelle action l'État et votre direction conduisent-ils pour recouvrer cette maîtrise ?

M. Nadi Bou Hanna, directeur interministériel du numérique et du système d'information et de communication de l'État. - Comme vous l'avez rappelé, monsieur le président, j'ai pris la tête de la Dinsic voilà six mois.

Au cours de ma carrière, j'ai eu l'occasion de diriger les communications du Quai d'Orsay, de prendre en charge la stratégie des douanes électroniques et également, en tant qu'entrepreneur, de créer des PME spécialisées dans le numérique.

Ces trois expériences m'ont permis d'appréhender les problématiques de compétitivité et d'autonomie, mais également de comprendre le rôle des grands acteurs du marché du numérique et les déséquilibres qu'ils peuvent engendrer. Ces problématiques me semblent essentielles au moment de développer une stratégie de l'État dans le domaine du numérique.

Nous nous appuyons notamment sur quatre indicateurs pour conduire notre action : il s'agit tout d'abord du baromètre européen DESI relatif à l'économie et à la société numériques. Sur le segment du service public numérique, la France a gagné une place par rapport à l'année dernière, mais n'occupe que la quinzième sur vingt-huit...

Le deuxième indicateur que nous regardons est en lien avec le grand débat national. Il s'agit de la perception du service public numérique par les usagers. Comme l'a souligné à plusieurs reprises le secrétaire d'État chargé du numérique, Cédric O, une demande claire s'exprime pour davantage de procédures numériques simples et accessibles et pour ne pas laisser sur le bord du chemin une partie de la population.

Le regard des agents publics constitue notre troisième indicateur. Les baromètres permettant de mesurer régulièrement les irritants placent systématiquement le numérique dans le top 3. Les agents publics expriment une véritable attente en matière d'évolution des méthodes de travail et d'élaboration de nouveaux outils.

J'en viens au quatrième indicateur. Il me semble d'ailleurs que le Sénat a récemment saisi la Cour des comptes pour mener une mission d'audit sur le pilotage des grands projets de l'État. Depuis des années, le taux de glissement calendaire ou budgétaire de ces grands projets oscille, pour des raisons variées, entre 30 et 35 %, contre 18 à 20 % dans les grands groupes.

La dynamique que nous voulons mettre en place doit jouer sur ces quatre indicateurs. Il s'agit d'améliorer la performance de l'État, de conseiller les ministères, de soutenir l'innovation - par exemple, à travers les start-ups d'État - et de développer et d'animer les partenariats. L'État ne peut pas et ne veut plus tout faire : le numérique est un secteur extrêmement compétitif, ne serait-ce qu'en matière de recrutement des bons talents.

Nous menons également une mission de contrôle de l'exécution des politiques des ministères. La Dinsic est clairement dans un rôle de subsidiarité : les ministères sont en charge de leur politique numérique verticale. Notre rôle est d'animer, de soutenir, d'orienter et de susciter les ruptures et l'innovation nécessaires sur l'ensemble du champ du numérique - infrastructures, systèmes d'information, usagers et données.

Il existe deux formes de souveraineté : celle des pays autoritaires et celle des démocraties. À partir du moment où nous choisissons l'approche démocratique, la souveraineté passe nécessairement par la performance. On ne peut envisager de souveraineté numérique sans une capacité à piloter performante. Il faut pouvoir fournir aux usagers - citoyens et agents publics - les solutions attendues.

Aujourd'hui, tout le monde possède un ordinateur dans sa poche et donc un accès immédiat à tout un tas de services, la plupart du temps gratuits. Si l'État n'est pas en mesure de fournir des services de confiance avec le même niveau d'ergonomie et de qualité que ceux des grandes plateformes, la souveraineté numérique en restera au stade de l'ambition.

La souveraineté numérique est la capacité de l'État à définir sans entrave les bons choix de court, moyen et long termes pour la société et à assurer la réversibilité des orientations - quelques années après avoir pris une décision, il faut en effet être capable de changer de prisme si les priorités ont évolué. À défaut, nous sommes pieds et poings liés, nous restons dépendants. Et la dépendance est le contraire de la souveraineté.

L'État doit également garantir les libertés fondamentales des usagers : accès au service public, libre arbitre, intimité numérique... Nous devons veiller à préserver ces îlots de liberté.

La souveraineté est-elle menacée aujourd'hui ? Je considère que oui, ne serait-ce que parce que nous sommes entrés dans une course contre la montre. Comme l'a souligné le secrétaire d'État en charge du numérique, la tendance est bonne en matière de champions du numérique : voilà quelques années, notre pays ne comptait que trois licornes ; il en compte aujourd'hui quasiment une dizaine.

Toutefois, notre retard reste considérable au regard des 150 licornes américaines et des 80 licornes chinoises. Si nous ne disposons pas d'acteurs capables de produire les infrastructures, de construire les services, de gérer la relation de premier niveau avec les usagers et de maîtriser les interfaces, nous serons probablement relégués en deuxième division en matière de souveraineté.

Il y a tout de même de vrais espoirs : la qualité de nos écoles est très bonne. Le dernier baromètre du Medef et du BCG les classe à la sixième ou septième place mondiale.

De même, nous continuons d'attirer énormément d'investissements, notamment grâce à notre politique en matière de crédit impôt recherche.

Par ailleurs, l'action de l'ANSSI, l'Agence nationale de la sécurité des systèmes d'information, en matière de cybersécurité permet de renforcer encore notre souveraineté.

Comment faire pour conserver et développer cette souveraineté numérique ? Le premier levier sur lequel agir est celui de l'adaptation à la réalité.

La société Michelin, par exemple, existe depuis 130 ans. Cette entreprise est passée de la vente de pneus à la vente de services de mobilité à la demande. Cette évolution correspond à une tendance de fond : la « servicisation » de l'économie. Les technologies numériques nous permettent aujourd'hui de souscrire à un service plutôt que de l'acquérir.

Si l'on veut développer notre autonomie, il faut nous appuyer sur des champions du numérique et pas seulement sur des infrastructures.

Le week-end dernier, Thierry Breton déclarait que seuls 55 % des salariés de son entreprise étaient embauchés en CDI. Les plus jeunes, et notamment les talents du numérique, cherchent davantage à se focaliser sur le sens des projets qu'à se lier de manière durable à une entreprise. Il s'agit d'une tendance de fond dénommée « uberisation » de l'économie. S'adapter à cette société qui évolue est un des moyens pour l'État de monter en puissance.

Nous disposons d'un autre levier : l'achat public. Je pense à l'autorisation de souscrire des achats en direct jusqu'à 100 000 euros pour toutes les actions d'investissement. Cette disposition, en vigueur depuis le début de l'année, permet à des acheteurs publics, à des porteurs de projets, de prendre davantage de risques que par le passé, de traiter en direct avec des acteurs qui vont porter l'innovation et expérimenter.

Si nous ne développons pas cette culture de l'expérimentation, nous ne trouverons pas les bonnes réponses aux problèmes d'aujourd'hui. Nous continuerons de reproduire les schémas de pensée et les solutions d'hier. La culture de l'innovation me paraît donc essentielle pour défendre notre souveraineté nationale numérique.

Lors de ma prise de fonction, j'ai constaté que la dynamique interministérielle et l'ambition collective pour construire une stratégie, méritaient d'être réaffirmées. Il s'agit donc, à travers Tech.Gouv, de remobiliser les capacités de chacun des ministères sur des objectifs communs, sur des chantiers transversaux, raison pour laquelle nous avons consacré les premiers mois de cette année à clarifier les enjeux du numérique.

Le premier enjeu consiste à simplifier la vie des gens.

Le deuxième enjeu, c'est l'inclusion : une partie de la population est aujourd'hui à l'écart non du volet numérique, mais de l'inclusion administrative. Il s'agit de personnes très à l'aise avec leur *smartphone,* mais qui ont du mal à comprendre la manière dont l'État leur parle. Ils ne sont pas capables, par exemple, de remplir un Cerfa. L'État se doit donc de changer la manière de projeter les services publics et les obligations incombant aux uns et aux autres.

Le troisième enjeu réside dans l'attractivité. Si l'État n'est pas capable d'attirer les meilleurs talents, il n'y aura pas de souveraineté. Il faut changer les pratiques managériales, fluidifier la circulation de l'information, associer les agents publics à la décision à travers des solutions numériques. Il s'agit d'un changement de paradigme managérial.

Comme vous l'avez souligné, monsieur le président, le quatrième enjeu concerne la maîtrise. J'ai effectivement pu déclarer que la maîtrise des infrastructures, des projets, des solutions entre les mains des usagers et des agents s'était effritée au fil des années. Lors de chaque audit de pilotage, on s'aperçoit que les grands projets sont externalisés à hauteur de 90 %. Or je ne connais pas un directeur capable de piloter un projet externalisé à 90 % chez un tiers, voire chez plusieurs tiers - cabinet de conseil, éditeur, intégrateur...

Le fait d'internaliser de nouveau une partie de ces compétences me paraît indispensable pour s'assurer de l'exécution des grands projets et de la fluidité du parcours des usagers.

Le cinquième enjeu consiste à générer les économies qui seront les investissements de demain en matière d'innovation.

La question des alliances constitue le dernier enjeu. Il s'agit de constituer, autour de l'État, un écosystème d'acteurs de confiance afin de démultiplier notre capacité à faire. Je pense, par exemple, à l'identité numérique. Mes services portent ce projet à travers le dispositif France connect qui rassemble aujourd'hui 10 millions de Français. Nous dénombrons quasiment 500 000 utilisateurs supplémentaires chaque mois. Pourquoi ce dispositif fonctionne-t-il aussi bien ?

M. Jérôme Bascher. - Parce que les Français n'ont pas le choix !

M. Nadi Bou Hanna. - Au contraire, ils peuvent choisir d'autres dispositifs.

Si France connect fonctionne aussi bien, c'est justement qu'il n'est pas obligatoire et qu'il permet de rassembler un grand nombre de services en ligne - fournisseurs d'identités, fournisseurs de services privés... Nous voulons qu'utiliser France connect devienne un réflexe pour les Français, chaque fois qu'ils auront une démarche administrative à entreprendre, qu'ils se rendront sur le site d'une collectivité territoriale ou qu'ils voudront, par exemple, ouvrir un compte en banque...

Si nous parvenons à constituer cet écosystème autour d'une ambition commune de respect de l'usager, nous pourrons renforcer encore notre souveraineté numérique.

M. Gérard Longuet, rapporteur. - Je partage totalement votre analyse : la performance est la condition première de la souveraineté numérique.

Au regard de votre expérience du secteur privé et du secteur public, pensez-vous possible d'être performant sans mobiliser de capitaux privés pour porter des projets, sur le marché français comme sur les marchés internationaux ?

Vous avez récemment lancé la messagerie sécurisée « Tchap » pour les agents de l'État. Qu'en attendez-vous ?

Vous avez évoqué les grands projets publics externalisés à 90 %. Que pensez-vous de nos grands échecs ? J'ai été en partie responsable de celui du logiciel Louvois et j'ai dénoncé, en tant que rapporteur du budget de l'éducation nationale, le système d'information des ressources humaines de l'Éducation nationale, dénommé Sirhen, qui s'est révélé catastrophique. L'extrême externalisation que vous avez évoquée peut-elle expliquer ces échecs ?

M. Nadi Bou Hanna. - À titre personnel, je considère qu'il n'existe aucune difficulté pour trouver des capitaux en France.

Pour avoir approché d'assez près les start-ups et les acteurs de l'innovation, je pense que les difficultés apparaissent seulement pour les grands tickets de plusieurs centaines de millions d'euros. Les entreprises qui s'appuient sur une bonne idée n'ont aucun souci pour trouver des financements.

Il est plus difficile de trouver des porteurs ayant une ambition. Or sans ambition démesurée on ne peut créer de géant du numérique. Le point commun de toutes les grandes entreprises du numérique, et notamment celles de la Silicon Valley, est de vouloir changer le monde, voire de prendre possession d'une partie du monde.

L'Assemblée nationale, le Sénat et un grand nombre de collectivités territoriales nous ont demandé d'ouvrir Tchap. Nous espérons pouvoir bientôt répondre favorablement à cette demande.

La création d'une messagerie instantanée garantissant que les données échangées entre agents publics, cabinets ministériels ou parlementaires ne se baladent pas aux quatre coins du monde nous a semblé indispensable. Nous avons donc noué un partenariat avec une PME franco-anglaise. Après nous être assurés que l'accès au code source était ouvert, afin de favoriser son développement, nous avons investi en mobilisant des développeurs de l'État aux côtés de ceux de l'entreprise. Au final, avec un budget relativement limité, nous avons produit une application de

messagerie instantanée sécurisée qui semble très appréciée des usagers. Sans publicité, nous dénombrons quasiment 35 000 agents publics utilisateurs en moins de deux mois.

M. Gérard Longuet, rapporteur. - Pouvez-vous nous donner des précisions sur l'économie du projet ?

M. Nadi Bou Hanna. - Il s'agit d'un investissement pur, assez léger en termes de coûts de fonctionnement, si ce n'est pour l'hébergement des machines. Il n'y a aucune licence. Nous avons voulu offrir aux agents l'équivalent de WhatsApp ou de Telegram sans leurs inconvénients.

Il est assez difficile de mesurer le retour sur investissement de ce dispositif dont le coût global s'élève environ à 1 million d'euros et qui devrait, à terme, concerner l'ensemble des agents publics et une grande partie des collectivités territoriales. À l'aune des grands projets de l'État, nous sommes donc très en-deçà des périmètres habituels.

Nous sommes en train de faire de même avec la web-conférence et avec les solutions collaboratives. Nous voulons favoriser la gestion des grands projets en transcendant les clivages administratifs classiques.

Comme l'a annoncé le Premier ministre, nous déploierons demain 300 maisons « France service » supplémentaires sur l'ensemble du territoire. Si nous ne mettons pas à disposition de ces maisons les outils de travail nécessaires pour échanger avec le reste de l'administration, elles ne pourront qu'expliquer à leurs usagers le contenu du site service-public.fr sans entreprendre aucune démarche d'accompagnement ni les renseigner sur l'avancement de leurs demandes. Sans outils efficaces, nous passerons à côté de la constitution d'un lien durable et de qualité avec les usagers.

Il serait trop facile de tenir leur large externalisation pour responsable de l'échec des grands projets. Certains grands projets externalisés dont on a su maîtriser le pilotage ont réussi. Une autre clé de lecture tient à la difficulté de savoir arrêter un projet. Lancer un projet, tout le monde sait le faire. Tenir des points réguliers d'avancement et d'interrogation sur la trajectoire suivie est tout autre chose. J'essaie d'insuffler une telle dynamique en développant davantage les rendez-vous réguliers avec les ministères.

Ces interventions plus en amont nous font défaut depuis des années. Nous voulons agir comme un cabinet de conseil interne à l'État dont les priorités et les orientations sont parfaitement alignées avec les siennes.

Je souhaite que les ministères puissent saisir cette force de frappe au sein de la Dinsic bien avant que les trajectoires ne soient dessinées, les cahiers des charges écrits et les prestataires retenus. Si nous arrivons à développer ce partenariat de confiance interne à l'État, nous devrions voir le taux de glissement baisser dans les prochaines années.

M. Franck Montaugé, président. - Avec tout notre savoir technologique, j'ai du mal à comprendre que l'on avance aussi peu sur la question du dossier médical partagé, ou DMP. Les enjeux sont pourtant considérables...

M. Nadi Bou Hanna. - Jusqu'à présent, les grands projets de la sphère santé n'étaient pas complètement supervisés par la Dinsic.

En ce qui concerne le DMP, un élément me semble très important : on est passé d'un dossier médical « patient » à un dossier médical pour les « professionnels » de santé. Le fait d'avoir une gouvernance et une orientation non pérennes n'a pas facilité les choses. Je ne pourrais pas vous en dire beaucoup plus, n'ayant pas du tout suivi cette question.

Sur les grands projets, si l'on manque de constance, si l'on essaie de toucher une cible mouvante dans le temps, il y a de fortes chances de la rater. Le pilotage du numérique de santé vient d'être remis en place au sein du ministère, avec une équipe constituée de spécialistes, de praticiens. La stratégie mise en place part des usagers, des parcours que suivent les citoyens, ce qui me paraît particulièrement prometteur et convaincant. J'ai fait une offre de services et d'appui à cette équipe. Je pense que nous allons avancer en étroite coopération pour développer le numérique de santé au plus près des besoins des utilisateurs.

Mme Catherine Morin-Desailly.- J'aimerais comprendre comment vous fonctionnez avec les différents ministères qui restent maîtres de leur secteur. J'imagine que vous intervenez de manière transversale, sans doute dans le cadre de certaines réunions stratégiques.

Comment se fait-il que l'on assiste parfois à des discordances en matière de stratégie ? Je pense notamment à un ministre de l'économie et des finances qui annonce vouloir lutter contre les abus de position dominante des entreprises extra-européennes du numérique, alors que le ministère de l'éducation nationale, par exemple, souscrit des contrats sans appel d'offre avec Google ou Microsoft, faute de doctrine arrêtée en la matière. Comment améliorer les choses et mieux coordonner les stratégies ?

Que faites-vous pour répondre concrètement aux attentes des agents publics en matière de formation et d'information ? En plein débat sur le projet de loi portant transformation de la fonction publique, ces sujets mériteraient d'être très clairement évoqués.

Existe-t-il une réflexion en matière de formation des ingénieurs réseau ? À quel type d'entreprise fait-on appel sur cette question ?

M. Nadi Bou Hanna. - Il peut en effet exister une certaine dualité entre les orientations politiques visant à favoriser le développement de champions nationaux et européens - c'est notamment le rôle de la Direction générale des entreprises et du ministère de l'économie et des finances - et l'activité au quotidien des ministères pour se doter de solutions de travail.

Comme je l`ai souligné, la vraie question est celle de la performance des solutions retenues. Si l'on ne trouve pas sur le marché d'alternative aux grandes suites bureautiques auxquelles vous faisiez allusion et que l'on oblige les usagers à utiliser des solutions non ergonomiques, ils iront chercher des solutions gratuites sur internet, au mépris de toute protection et de toute souveraineté en matière de données.

Nous développons une approche pragmatique à même de garantir que l'usage attendu est au rendez-vous, que les solutions retenues permettent d'accéder aux données et que la réversibilité est possible. Une des missions de Tech.Gouv concerne ainsi la labellisation des solutions de confiance. Il s'agit de définir les règles du jeu permettant de distinguer entre une bonne et une mauvaise solution parmi le panel de produits que l'on trouve sur l'étagère.

Nous serons ravis de pouvoir labelliser des éditeurs français sur les critères d'interopérabilité, de réversibilité, d'accès aux données... On n'interdira pas non plus aux autres éditeurs, européens ou non, de candidater. Ce qui est important, c'est le respect des référentiels des bonnes pratiques pour garantir l'autonomie de l'État dans la durée.

Mme Catherine Morin-Desailly. - Avez-vous identifié une problématique de souveraineté par rapport à certaines solutions auxquelles l'État a recours, à défaut d'autres solutions potentiellement labellisables ?

Voilà quelques années, la Bibliothèque nationale de France, la BNF, avait renoncé à une offre très séduisante de Google pour développer d'autres solutions. De quels moyens dispose-t-on pour encourager les administrations à recourir à d'autres solutions que celles entrant en contradiction avec l'affirmation de notre souveraineté ?

M. Nadi Bou Hanna. - Nous n'avons pas d'approche idéologique en la matière.

Nous avons choisi, avec Tchap, de développer en propre une solution qui n'existait pas sur le marché. Tout ce que le marché avait à nous offrir compromettait la sécurité des communications, en particulier celles des cadres dirigeants de l'État.

Une suite bureautique doit essentiellement permettre aux agents de travailler. Privilégier l'une ou l'autre solution ne relève pas d'une problématique de souveraineté. Nous sommes dans le domaine de la commodité, non dans celui de l'information sensible.

Chaque fois que c'est possible, nous choisissons une solution de marché qui garantisse une certaine forme d'autonomie. Lorsque ce n'est pas possible, mais que le risque de compromission est faible, nous choisissons la meilleure solution existante. Enfin, lorsqu'aucune solution du marché ne permet de répondre à l'enjeu en question, nous la développons.

En matière d'archivage électronique, par exemple, l'État a choisi de développer une plateforme dénommée Vitam, faute de solution de marché répondant aux enjeux de volumétrie dans de bonnes conditions. Nous choisissons les solutions au cas par cas, en fonction des problématiques.

La mission « talents » de Tech.Gouv vise à développer la culture numérique dans l'encadrement supérieur et à développer l'émergence d'un vivier du numérique au sein de l'État. Ce vivier peut être constitué non seulement de fonctionnaires du numérique, de cadres qui vont accomplir une grande partie de leur carrière au sein de l'État, mais aussi des meilleurs éléments que nous essayons de recruter, ne serait-ce que pour quelques années. Le projet de loi de transformation de la fonction publique devrait justement permettre de favoriser les allers et retour entre secteur public et secteur privé. C'est un des leviers sur lesquels nous voulons nous appuyer pour renforcer la capacité de l'État de piloter en propre sa stratégie numérique.

M. Franck Montaugé, président. - Pourriez-vous nous donner quelques précisions sur la mission Etalab et sur la politique d'ouverture des données ?

M. Pierre Ouzoulias. - J'ai bien compris que c'est la sécurité qu'il apportait et le recours à des codes sources ouverts qui vous avaient convaincu de développer Tchap. Qu'en est-il des autres logiciels utilisant des codes source libres ?

Vous avez évoqué à plusieurs reprises les suites bureautiques. On a le sentiment que l'État, et notamment en son sein les ministères de la défense et de l'éducation nationale, a préféré les suites développées par les Gafam à celles des logiciels libres, lesquelles offraient pourtant les garanties que vous avez identifiées.

Dans l'attente de votre instrument de labellisation, il semble que l'État nous encourage à acquérir des systèmes privés, payants, plutôt que les solutions libres offrant les mêmes garanties que Tchap. On a du mal à comprendre cette logique...

M. Jérôme Bascher. - J'ai été chef de projet « statistiques » à l'époque où il existait encore des chefs de projet « informatique ». Les choses fonctionnaient plutôt bien : les statisticiens étaient formés à comprendre les informaticiens, ils leur donnaient les spécifications et savaient arrêter un projet. L'État sait-il encore suffisamment spécifier ses projets pour éviter les échecs ? Informaticiens et donneurs d'ordre savent-ils se comprendre et clairement identifier qui doit décider quoi ?

M. Nadi Bou Hanna. - Chaque fois que l'usage est bon, le logiciel libre a sa place.

Un certain nombre de ministères a choisi des suites bureautiques *open source* avant de faire marche arrière, une partie des fonctionnalités

espérées n'étant pas au rendez-vous. D'autres ministères ont continué à utiliser ces suites bureautiques. Je fais partie de ceux qui ont lancé, voilà un peu plus de quinze ans, la suite Open office au sein des douanes.

Si l'on force la main des agents pour des raisons de modèle économique, ils utiliseront probablement Google docs en ligne.

De plus, cela fait bien longtemps que plus personne ne croit que l'*open source* est gratuit. On regarde aujourd'hui les coûts de maintenance et les écosystèmes constitués avant de choisir telle ou telle solution *open source*. Chaque fois que l'on a la certitude de l'existence d'un écosystème, et non d'un acteur unique fonctionnant sur un autre mode que la licence, on regarde de plus près pour voir si cette solution est adéquate sur le segment concerné.

Enfin, le coût complet des logiciels libres n'est pas si éloigné de celui des logiciels propriétaires...

Une des constantes de l'échec des grands projets réside dans leur durée : entre cinq et quinze ans. Une grande inflexion consiste à conduire des projets avec la méthode « Agile », c'est-à-dire adopter une approche beaucoup plus itérative. Plutôt que de viser tout de suite la cible exhaustive avec l'ensemble des fonctionnalités attendues par l'ensemble des parties prenantes, il faut être capable d'avoir des temps d'atterrissage beaucoup plus courts, à six, à douze, à dix-huit mois. Il s'agit des points de rendez-vous que j'évoquais voilà quelques instants pour être capable d'infléchir, voire d'arrêter des projets. C'est cette méthode qui nous permettra, demain, d'améliorer le pilotage des projets de l'État.

M. Franck Montaugé, président. - Pouvez-vous répondre à ma question sur la mission Etalab et la mise à disposition des données, au risque d'affaiblir notre souveraineté numérique ? La loi pour une République numérique impose la mise à disposition des données. Sommes-nous capables d'en tirer davantage profit que les grands groupes qui ont des capacités que nous n'avons pas aujourd'hui ?

M. Nadi Bou Hanna. - On a tendance à accoler le terme « ouverture » à chaque fois qu'il est question de données, notamment au sein de l'État.

La loi pour une République numérique a généralisé l'ouverture des données. En évoquant la performance, je soulignais que le numérique devait nous permettre d'exploiter les données pour produire le meilleur service possible. La question de la circulation de la donnée au sein de l'État et entre l'État et les collectivités territoriales a sans doute été sous-priorisée ces dernières années. Si l'on veut vraiment simplifier, il faut arrêter de demander plusieurs fois les mêmes choses aux Français et généraliser enfin l'interconnexion des données tout en préservant les libertés individuelles. La question de la circulation me paraît plus importante que celle de l'ouverture des données.

À qui profite l'ouverture et qui va s'en saisir ? Voilà quelques semaines, les données des transactions immobilières ont été ouvertes. Une PME française s'en est alors saisie pour proposer un service à valeur ajoutée. On peut également craindre que les grandes plateformes qui disposent des ingénieurs et des volumes financiers ne captent d'autres données pour les exploiter au mieux et créer leurs propres services à valeur ajoutée.

Cette crainte s'exprime dans certains territoires. J'y suis réceptif. C'est la raison pour laquelle je préfère focaliser l'énergie de la Dinsic sur la circulation de la donnée et la simplification induite pour les services rendus aux usagers et sur la construction des nouvelles politiques publiques.

Nous avons ainsi mis en place un pôle « intelligence artificielle » au sein de la Dinsic, recruté des *Data scientists*, recruté des entrepreneurs d'intérêt général pour relever un défi porté par un ministère ou un autre... Nous devons arriver à diffuser largement cette culture de la donnée au sein de l'État.

M. Jérôme Bascher. - Créer une identité numérique relève-t-il de votre rôle ?

M. Nadi Bou Hanna. - La Dinsic a pour rôle aujourd'hui de porter France connect, dispositif fédérateur d'identités.

M. Jérôme Bascher. - Il s'agit alors d'« identités » au pluriel, non d'une identité.

M. Nadi Bou Hanna. - La promesse n'en reste pas moins vertueuse pour l'usager. Il s'agit de lui donner le choix de l'identité qu'il souhaite utiliser pour toutes ses démarches et ne pas lui imposer une solution plutôt qu'une autre.

Un certain nombre de pays, de plus petite taille que le nôtre et émanant de l'ancien bloc soviétique, ont fait le choix d'une identité généralisée. Aujourd'hui le compromis trouvé consiste à simplifier la vie des usagers tout en leur permettant de choisir parmi les identités agrégées dans France connect.

M. Gérard Longuet, rapporteur. - De quels moyens humains disposez-vous ?

M. Nadi Bou Hanna. - La Dinsic dispose de 144 équivalents temps plein, dont une quarantaine dédiée au fonctionnement du réseau interministériel de l'État.

M. Franck Montaugé, président. - Pouvez-vous nous dire un mot de la formation des ingénieurs réseau évoquée par Mme Morin-Desailly ?

M. Nadi Bou Hanna. - La Dinsic anime la pérennisation et la montée en puissance de la filière des ingénieurs des systèmes d'information et de communication. Il est essentiel que l'État se dote d'une force en propre de cadres A et qu'il renforce sa filière de cadres « A+ » dans le domaine du

numérique. Ses effectifs ne me semblent aujourd'hui pas suffisamment étoffés pour pouvoir reprendre la main sur une partie de la stratégie et du pilotage des grands projets. Si nous n'y arrivons pas, nous risquons de compromettre notre capacité à assurer notre souveraineté numérique.

Mme Catherine Morin-Desailly. - Qui forme actuellement les ingénieurs réseau ? S'agit-il d'entreprises privées ?

M. Nadi Bou Hanna. - Nous nous appuyons sur les centres de formation de la fonction publique - IGPDE, écoles de fonctionnaires développant des cursus en la matière...

Mme Catherine Morin-Desailly. - Cisco est impliquée dans la formation des ingénieurs réseau. Que pouvez-vous en dire ?

M. Nadi Bou Hanna. - Tous les industriels peuvent prendre en main certaines formations thématiques. Lorsque vous voulez développer une compétence en matière d'exploitation des routeurs, ce que l'on fait de moins en moins au sein de l'État, mieux vaut se tourner vers ceux qui créent et qui disposent aujourd'hui de la plus grande part de marché...

Toutefois, la formation des ingénieurs n'est pas assurée par les entreprises privées.

M. Franck Montaugé, président. - Vous avez parlé de mise en circulation des données dans la sphère publique. Existe-il des projets de modélisation des politiques publiques pouvant aboutir à des outils d'évaluation de ces mêmes politiques ?

M. Nadi Bou Hanna. - Pas à ma connaissance.

M. Franck Montaugé, président. - Nous vous remercions.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible en ligne sur le site du Sénat.

Audition du Général François Lecointre, chef d'État-Major des armées (CEMA),
le 25 juin 2019

M. Franck Montaugé, président. - Notre commission d'enquête poursuit ses travaux avec l'audition du Général François Lecointre, chef d'état-major des armées. Il est accompagné du général de division Olivier Bonnet de Paillerets, commandant cyber de l'état-major des armées et du général de brigade Jean-Jacques Pellerin, chef de la division de l'état-major des armées, en charge du numérique et de la cohérence des programmes interarmées.

Cette audition sera diffusée en direct sur le site Internet du Sénat. Elle fera également l'objet d'un compte rendu publié.

Une commission d'enquête fait l'objet d'un encadrement juridique strict. Je vous informe qu'un faux témoignage devant notre commission serait passible des peines prévues aux articles 434-13 à 434-15 du code pénal.

Conformément à la procédure applicable aux commissions d'enquête, MM. François Lecointre, Olivier Bonnet de Paillerets et Jean-Jacques Pellerin prêtent serment.

M. Franck Montaugé, président. - La revue stratégique de défense et de sécurité nationale de 2017 et la revue stratégique de cyberdéfense de février 2018 ont reconnu le rôle majeur de la cyberdéfense militaire. Notre pays s'est doté d'une doctrine militaire en lutte informatique offensive tout en renforçant la politique de lutte informatique défensive du ministère des Armées. La capacité à se protéger contre les attaques informatiques, à les détecter, à en identifier les auteurs mais également à riposter, est devenue l'un des éléments clefs de notre souveraineté.

Je commencerai donc, général Lecointre, par vous demander comment vous appréhendez la notion de souveraineté numérique. Distinguez-vous la souveraineté classique, de défense du territoire, de la souveraineté numérique, par nature dématérialisée ? Pouvez-vous nous présenter la doctrine prenant en compte et les modifications de la souveraineté classique par le monde numérique : quelle est la place du numérique dans ce cadre ?

Un pays ne peut être souverain s'il ne parvient pas d'une part à contrôler les activités numériques qui affectent son territoire, et s'il ne dispose pas d'autre part des technologies clés et des infrastructures critiques. Un pays ne peut être souverain sans les armes lui permettant de garantir son autonomie et sans la maîtrise des théâtres opérationnels affectés par de nouvelles menaces numériques. Avons-nous aujourd'hui les moyens de nos ambitions dans tous ces domaines ?

Général François Lecointre, chef d'état-major des armées. - Ma mission est d'assurer à la France la capacité d'une part à agir de manière souveraine dans l'espace numérique, d'autre part de conserver une capacité autonome d'appréciation, de décision et d'action, et de préserver également les composantes les plus traditionnelles de sa souveraineté vis-à-vis de menaces nouvelles, qui tirent parti de la numérisation croissante de la société. Les menaces et les risques s'accroissent, en témoignent les graves incidents tels que Wanacry ou Notpetya, ou celui observé lors des élections américaines. Les opérations de désinformation sont difficiles à contrer car nous sommes ouverts au niveau européen, l'article 10 de la convention européenne des droits de l'homme nous y oblige. Le débat, en outre, est permanent entre sécurité collective et droits individuels...

Un certain nombre de réponses ont visé à réduire les tensions et les menaces, en particulier par la régulation internationale et la création de normes, je songe au Règlement général sur la protection des données ou au *Cloud act* du 23 mars 2018.

Les armées sont la cible d'attaques informatiques particulièrement nombreuses. Ainsi, en 2018, 831 événements significatifs ont été recensés par le commandement de la cyberdéfense (Comcyber), soit une augmentation de l'ordre de 20% par rapport à 2017. Une centaine consiste en des attaques informatiques avérées, dont six sont caractéristiques de modes d'action de groupes structurés affiliés à des États. Toutes ces attaques ont été menées à des fins d'espionnage de hauts responsables du ministère ou de fonctions opérationnelles.

En 2018, le ministère des armées a été la cible d'attaques par un mode d'action connu de nos services, que certains attribuent à Turla, groupe affilié au service fédéral de sécurité russe. Les cibles identifiées sont des membres du ministère ayant des responsabilités dans le domaine des relations internationales, ou des fonctions opérationnelles d'intérêt, comme l'approvisionnement en carburant des bâtiments de la marine nationale, afin de suivre les escales de nos bâtiments. Aucune attaque de groupe affilié à la Chine n'a été observée ; les cybermenaces iranienne et nord-coréenne ne semblent pas non plus, à ce stade, viser les armées ou le ministère.

En tant que chef d'état-major des armées (CEMA), j'assume des responsabilités et des prérogatives - de nature défensive - définies dans la revue nationale cyber de février 2018. Cette revue organise la gouvernance cyber de l'État autour de quatre piliers aux gouvernances spécifiques : la prévention, sous la responsabilité de l'Agence nationale de la sécurité des systèmes d'information et du Premier ministre ; le renseignement, avec la DGSE, la DGSI et les ministères de tutelle ; l'action judiciaire qui relève à la chancellerie, et l'action militaire, conduite par le chef d'état-major des armées et le Président de la République.

Chaque pilier a une gouvernance autonome et tous se coordonnent autour d'un comité de coordination des crises cyber ou « C4 », qui articule le cycle de la cyber défense - détection, attribution, réponses, car il s'agit de définir les stratégie de réponse qui sont soumises au politique.

Les orientations prises par la revue fonctionnent très bien ; le CEMA dépositaire de la conduite des opérations militaires a été renforcé dans sa responsabilité de cyber défense sur le périmètre du ministère des armées, et pour la conduite des opérations numériques. Le commandement cyber a été créé il y a moins de deux ans, il me seconde dans cette double responsabilité. Le rôle stratégique, central, de la cyberdéfense militaire a été parfaitement reconnu.

Dans mon périmètre de responsabilités, je vise une numérisation maîtrisée, qui doit profiter des opportunités offertes par les technologies émergentes tout en maintenant les systèmes à un très haut niveau de sécurité. La souveraineté numérique est dans l'ADN du ministère et des armées ! Nous sommes parfaitement conscients des vulnérabilités de nos systèmes et nous avons le souci constant de préserver à la fois l'intégrité, la confidentialité et la disponibilité des données. Celles-ci sont la matière première de nos systèmes d'information. Elles sont maîtrisées sur toute la durée de leur utilisation, dans la collecte comme dans le stockage, en fonction de leurs niveaux de sensibilité. Les données opérationnelles sont les plus sensibles, mais les données médicales ou relatives aux ressources humaines, par exemple, sont sensibles également. Leur exploitation exige un personnel habilité et des systèmes homologués par les armées, elles transitent sur des réseaux maîtrisés et chiffrés.

La direction interarmées des réseaux d'infrastructures et des systèmes d'information de la défense (Dirisi), opérateur du ministère, assure la gestion des réseaux qui lui sont dédiés, administre plus de 1500 systèmes d'information et héberge les données du ministère au sein d'infrastructure réparties sur tout le territoire.

L'utilisation de l'internet par les armées fait l'objet d'une attention particulière : surveillance permanente des échanges de fichiers, sécurisation des sites, anonymisation des recherches sur source ouverte.

Enfin, tous, du cadre au soldat, sont sensibilisés et formés à l'hygiène numérique.

Il demeure que nous traversons une période charnière de fragilité : l'utilisation des dernières technologies disponibles doit être intégrée à nos systèmes pour garantir notre supériorité informationnelle ; mais ce, avec une grande prudence lors de l'intégration, afin de conserver un haut niveau de sécurité.

C'est pourquoi nous poursuivons nos efforts en termes de *big data* et d'intelligence artificielle, pour développer le traitement et l'analyse de quantités de données qui ne sont pas humainement exploitables afin de

produire une information valorisée à partir de la très grande masse de données disponibles. La ministre a annoncé un investissement de 100 millions d'euros par an dans ce domaine. Le point le plus crucial est celui du recrutement de spécialistes.

Il s'agit aussi de mener une stratégie *cloud* robuste. Les armées vont devoir appuyer leur transformation numérique, désormais permanente, sur un opérateur de confiance en mesure de garantir la souveraineté numérique du ministère. La stratégie industrielle doit nous permettre de construire un écosystème national de confiance, s'appuyant sur des niveaux de *cloud* différenciés, selon le niveau de confidentialité des données. Cela exige, j'y insiste, une sensibilisation de tous, soldats et cadres, quant aux risques : il nous revient d'instruire nos soldats sur la grammaire et l'orthographe de l'espace numérique, objets connectés compris. L'ensemble du personnel du ministère de la défense doit maîtriser l'utilisation d'internet, au plan professionnel ou privé, tous étant présents sur les réseaux sociaux, en France comme sur les théâtres d'opération... Enfin, il faut adapter les organisations à la gouvernance du risque cyber.

La collecte et l'exploitation des données doivent évoluer pour que nous profitions de la pleine capacité offerte par les nouveaux capteurs spatiaux et numériques, inscrits dans la loi de programmation. La direction du renseignement militaire (DRM) s'appuiera ainsi sur le programme Demeter pour exploiter efficacement les giga-octets de données techniques issues des programmes électromagnétiques. Cela implique de recourir à l'intelligence artificielle.

Il faut également maîtriser la projection de puissance en tout point du globe - une des caractéristique de l'armée française - avec une sécurité des raccordements des systèmes d'information et de communication projetés aux réseaux d'infrastructure : le « bout en bout » numérique, depuis Balard jusqu'aux échelons tactiques de base, sur le terrain, est fondamental. Les réseaux doivent donc augmenter leurs capacités et consolider leur fiabilité, en maîtrisant la cryptologie. La Dirisi assure le chiffrement des réseaux, y compris pour le déclenchement de la dissuasion nucléaire.

Dans le cadre de ma mission cyber, je dois disposer d'une autonomie d'appréciation, pour proposer au pouvoir politique des options dans le champ de mes responsabilités, et d'une capacité automne d'opérations cyber, au profit des opérations en cours. Le cyber est en effet considérée comme une arme d'emploi, pour la défense de nos intérêts et de notre souveraineté.

Cela exige de maîtriser la détection, la caractérisation et l'attribution d'une attaque - donc de disposer d'un équipement en sondes souveraines. D'où la montée en puissance des capacités cyber du Comcyber et des services de renseignement, avec une mutualisation entre les deux.

Il est impératif de pouvoir proposer au pouvoir politique une option de réponse en cas de crise majeure, y compris dans le champ cyber, par

l'engagement de moyens militaires autonomes, en particulier la capacité à produire des effets cyber à partir de moyens militaires.

Il convient aussi sur le champ de bataille de développer une capacité d'actions numérique propre, intégrée à la manoeuvre militaire. Cela est de plus en plus nécessaire sur des champs de bataille qui se numérisent de plus en plus. Notre supériorité opérationnelle passe par la capacité à protéger nos moyens et à démultiplier les effets que nous produisons : obtention de renseignement opérationnel, neutralisation d'un système de commandement adverse, désorganisation de centres de propagande adverses,...

Il nous faut aussi développer des partenariats pour consolider notre appréciation de situation et nos coalitions. Mais peu de pays disposent de la maturité conceptuelle, organisationnelle et opérationnelle suffisante pour nous permettre de nouer des échanges de confiance.

Il importe de jouer un rôle moteur dans la promotion d'une culture militaire cyber partagée entre partenaires européens, au sein de l'OTAN ou de l'Union européenne : nous y travaillons notamment à travers l'initiative européenne d'intervention (IEI). Autre exigence, promouvoir au plan international un comportement responsable, facteur de stabilité.

Enfin, il s'agit d'opérer un rapprochement avec le monde industriel numérique, pour que nos armées restent connectées au progrès et pour garantir les ressources humaines dont nous avons besoin. C'est notre premier défi, car contrairement à ce que nous avons connu au sortir de la Deuxième guerre mondiale et jusqu'à la fin de la guerre froide, aujourd'hui, c'est de moins en moins la recherche militaire qui tire la recherche civile. Les technologies civiles, duales, nous imposent de rester étroitement connectés à ce monde industriel qui innove sans cesse. En janvier dernier, le ministère a signé une convention avec les industriels de défense.

Il nous faut une famille professionnelle RH SIC armée et structurée, or nous avons enregistré à fin 2018 un déficit de 1 300 emplois militaires et civils, en retrait de 8% par rapport aux besoins, compte tenu de la menace cyber, de la transformation numérique et du plein emploi des cadres dans le secteur civil des systèmes d'information. Nous avons de plus en plus de mal à fidéliser une main d'oeuvre qui est très recherchée. Nous nous efforçons donc à favoriser les recrutements d'agents civils sous contrats (ASC), voie qui n'est pas entièrement satisfaisante.

En matière d'intelligence artificielle et de *big data*, des compétences spécifiques sont nécessaires également au plus près des opérationnels pour répondre au besoin des armées selon des « approches agiles ». Dans le domaine cyber, l'objectif est de disposer de 1000 cyber-combattants supplémentaires d'ici à 2025. La ressource humaine en sortie des écoles et sur le marché du travail n'est pas suffisante. Il faut donc développer une politique spécifique pour le recrutement, la fidélisation, la formation. Cela

nous amène également à réfléchir sur le rôle du personnel civil dans l'action militaire cyber.

Le numérique a envahi toute les activités humaines, dans les sphères étatiques, professionnelles, privées. Il gomme toutes les frontières physiques sans pour autant les faire disparaître, autorise une circulation quasi instantanée de l'information et permet un niveau d'interaction jamais atteint. Il peut remettre en question la notion d'État, de souveraineté. Il inquiète par ses potentialités vertigineuses et ses conséquences sur nos sociétés et organisations étatiques.

Mais les armées, investies de la responsabilité de préserver la souveraineté nationale, sont plutôt en avance. La donnée occupe depuis longtemps une place centrale ; sa protection et son utilisation ont toujours été une préoccupation. Dans ce champ comme ailleurs, l'autonomie stratégique, garante de la souveraineté, est l'objectif que nous nous fixons.

Aujourd'hui, notre organisation, qui repose sur la Dirisi et le Comcyber, est mature. Nos capacités d'action et de protection sont de très bon niveau, comme le montre notre victoire récente lors de l'exercice international *Locked shields*.

Il nous faut rester à la pointe de l'innovation technologique ; et recruter, former et fidéliser les meilleurs cyber-combattants. Tels sont nos défis actuels.

M. Gérard Longuet, rapporteur. - Il est passionnant de vous entendre. Notre audition est captée, j'essaierai de ne pas vous mettre dans une situation difficile par mes questions.

La guerre est chose connue. Les cyberattaques le sont moins. Vous parlez des problèmes de détection, caractérisation, identification : c'est une question majeure, qui n'est pas facile à traiter, car il s'agit de manoeuvres autour du conflit, qui ne sont pas en elles-mêmes le conflit, tout en étant conflictuelles...

Vous avez parlé avec beaucoup de pudeur des pays qui ne nous ont pas attaqués. Vous n'avez pas cité, parmi eux, l'Islande, Andorre, Monaco ou Saint-Martin. Je m'interroge !

Plus sérieusement, selon vous, les outils cyber, l'espace numérique facilitent-ils les conflits dissymétriques ? Le monde numérique est à dominante civile, où les technologies civiles ont un effet d'entraînement. La taille est-elle un facteur essentiel d'autorité, ou au contraire, la modestie des moyens à mettre en oeuvre, la subtilité voire la perversité des procédures, la difficulté pour attribuer une attaque renforcent-elles le risque de conflit dissymétrique, opposant un pays à des forces non identifiées et dotées de moyens importants ? La fragilité provient non des systèmes militaires, car vous avez la culture de la sécurité, mais de la société. Vous avez parlé à bon droit d'hygiène numérique... Le plus grand pays allié, avec lequel nous

entretenons des relations anciennes, a été pris la main dans le sac, si l'on peut dire, et à plusieurs reprises, notamment avec ses bons alliés de l'OTAN, pour sa capacité à s'intéresser à ce qui n'est pas sur la place publique. Les plus petits peuvent-ils tout autant déstabiliser un système de défense ?

Les champs d'opérations extérieures sont contrôlés et commandés par l'intermédiaire des réseaux, qu'il s'agisse d'apporter un appui aérien aux combattants ou de prendre une décision politique. Tout est relié, en instantané, les temps de réaction sont minimes : dans cette chaîne, où sont les maillons faibles ? Existe-t-il des risques plus importants sur tel ou tel théâtre ? Où sont les fragilités éventuelles de notre système militaire ?

La gestion des effectifs spécialisés est une affaire difficile, en raison de la concurrence du secteur civil et des carrières que l'on y peut faire. L'actualisation des compétences et des savoirs est une exigence permanente. Quels outils vous manque-t-il ? Il y a la défense du pays, la sécurité des armées, la sécurité des particuliers, des industries de défense, des administrations étatiques. Une attaque frappant le secteur privé peut affaiblir le pays, je pense à la déstabilisation de Saint-Gobain via une filiale en Ukraine.

La défense est un tout. Quels hommes et quelle coordination avec les services de l'État, afin que vous soyez correctement informés ?

Général François Lecointre. - Voilà des questions simples ! Le champ cyber facilite-t-il des agressions dissymétriques ? Oui, mais ce n'est pas le principal sujet pour moi. Un ennemi peut capter des innovations d'usage et être inventif dans le détournement de moyens, pour nous agresser, comme sur les théâtres du Sahel ou du Levant. N'importe qui, surtout dans la génération montante, peut s'emparer de ces outils, ce qui facilite des modes d'attaque dissymétriques. Ce sont des compétences répandues, duales, qui n'exigent pas d'armée structurée. Plus ennuyeux à mon sens, cette situation favorise les conflits hybrides, combinant des attaques sur plusieurs fronts, dans plusieurs champs, dont le champ cyber, et visant aussi la désinformation et la propagande. C'est une difficulté supplémentaire dans l'art de la guerre et la défense de notre souveraineté. Au-delà de quel seuil dois-je considérer qu'il faut mener des contre-attaques, des rétorsions, et dans quel champ ?

Général de division Olivier Bonnet de Paillerets, commandant cyber de l'état-major des armées. - Il y a aussi une difficulté, pour une société très numérisée, à répondre face à une société qui l'est moins.

Aujourd'hui, les menaces et le nombre des attaquants augmentent, mais la capacité d'attaques complexes appartient encore aux États. Les investissements en organisation, doctrine d'emploi, recrutement d'experts, nécessitent une cohérence qui n'existe que dans certains États. Cela nous donne tout de même un avantage comparatif dans une guerre même dissymétrique.

Général François Lecointre. - Concernant les OPEX et le danger pour nos forces, là où l'adversaire est capable d'agir dans le champ cyber, je précise que nous utilisons l'arme cyber comme une arme du champ de bataille. La ministre et moi-même l'avons dit lorsque nous avons présenté la doctrine de lutte informatique offensive : nous savons désorganiser un ennemi, le positionner, le traiter. Nous utilisons couramment cet outil ! Il y faut des moyens et des spécialistes, mais il nous donne un avantage très net au Sahel ou au Levant.

Il n'existe aujourd'hui aucun ennemi potentiel, à part l'Iran, voire la Russie (mais nous ne sommes pas confrontés à eux), qui puisse menacer nos réseaux et notre capacité à agir dans un espace numérisé. Tous nos systèmes d'armes sont de plus en plus numérisés, mais ils intègrent nativement la nécessité d'une protection - je pense à Scorpion ou au Scaff par exemple. Sur le champ de bataille, seules des puissances très élaborées pourraient nous menacer et nous prenons bien garde à préserver une supériorité opérationnelle qui dépend essentiellement de la mise en réseau et de la capacité à agir de façon partagée avec des effets sur une même cible mais à partir de lieux différents et selon des champs et dans des domaines différents. Nous sommes très attentifs à protéger cette capacité de transmission des données.

Général Olivier Bonnet de Paillerets. - Sur les OPEX, la gouvernance du risque cyber (lequel n'est pas sous-évalué) est descendue jusqu'au décideur opérationnel, elle relève de la responsabilité pleine et entière de celui qui commande sur le terrain. Nous avons organisé une cyber défense de bout en bout, avec une coordination entre les réseaux déployés et Paris, totalement interconnectés.

Autre axe sur lequel l'état-major a progressé : l'intégration du cyber dans toutes les composantes de toute opération interarmée ou de milieu. Pas de déploiement sans processus, équipements et gouvernance particulière autour de ce risque cyber.

Général de brigade Jean-Jacques Pellerin, chef de la division de l'état-major des armées, en charge du numérique et de la cohérence des programmes interarmées. - Un mot des maillons faibles. Le risque zéro n'existe pas. Il faut donc assurer la résilience de nos systèmes, grâce à des redondances. Ce n'est pas tant l'intégrité ou la confidentialité de la donnée qui pourrait être le maillon faible que leur acheminement : nos moyens de communication satellitaire sont très fragiles : d'où la nécessaire mise en place de moyens pour la transmission de l'ordre par plusieurs chemins. Si ce maillon faible est attaqué, toutes les fonctions ne sont pas conservées, certaines seront dégradées, mais nous pourrons mener à bien la mission qui nous a été confiée.

Général François Lecointre. - Cela explique aussi toute la réflexion conduite aujourd'hui sur l'action dans l'espace pour nous protéger contre des attaques visant nos moyens satellitaires.

Quant aux ressources humaines, nous sommes face à un défi, car la ressource est rare, mais elle peut être mutualisée, nous y reviendrons. Soit dit en passant, la condition militaire reste un sujet central : le décalage par rapport à la condition civile ne se réduit pas, ce qui pose le problème du recrutement et de la fidélisation dans toutes les spécialités rares, alors que nous avons besoin de compétences de plus en plus pointues, sur des équipements de plus en plus sophistiqués. Nous conduisons une réflexion : qu'est-ce qu'être militaire, que signifie mettre en oeuvre la force de façon délibérée pour préserver la souveraineté, en quoi y a-t-il une obligation de confier la défense de la nation à des gens dont le statut comporte des obligations de disponibilité et de discipline ? Selon moi, il faut limiter le nombre de civils dans la fonction de cybercombattant, pour laquelle nous avons réellement besoin de militaires.

Général Olivier Bonnet de Paillerets. - Les métiers sont en cours de redéfinition, car on passe de métiers sur les systèmes d'information et d'administration à des métiers sur la donnée et de la cyberdéfense. Le processus n'est pas terminé et l'on s'interroge sur la meilleure façon de mener la transition.

Quant à la valorisation des parcours, c'est une bonne surprise : nombre de jeunes supertechniciens nous rejoignent, parce qu'ils cherchent du sens à leur activité professionnelle. Il faudrait pouvoir leur proposer des parcours au-delà de trois ou six ans, au-delà desquels le décrochage de rémunération est trop important, il est difficile de les retenir. Avec l'Anssi et les services de renseignement, nous avons entrepris l'an dernier une gestion croisée des parcours, sur des cycles de six à dix ans, suffisants pour nous. Et pourquoi ne pas organiser des parcours croisés avec le monde de l'entreprise ? Autre bonne surprise, les groupes privés sont intéressés, car ils trouveraient là des cadres intermédiaires capables de structurer une partie de leur organisation - et nous obtiendrions de notre côté une partie de leur expertise.

Nous sommes en train de réécrire notre politique de formation. Les armées ont un rôle à jouer dans la formation préliminaire ; il ne faut pas s'acharner en revanche, selon moi, à faire de la formation continue, mieux vaut « up-skiller » des technicités venues du monde de l'entreprise. Enfin, nous ne sous-estimons pas l'importance de la réserve, composée de professionnels qui ont envie de nous apporter leur expertise - celle-ci est à portée de nos armées, reste à organiser la rencontre optimale de l'offre et de la demande.

La réforme de la réserve cyber est engagée depuis un an : elle n'est pas une réserve de non emploi, en attente du Pearl Harbour cyber, elle est sollicitée au quotidien, y compris dans les structures opérationnelles, car ces réservistes sont dépositaires d'expertises que nous n'avons pas. Cela n'est pas facile à mettre en oeuvre mais nous nous y attelons.

M. Jérôme Bascher. - Vous avez beaucoup parlé de cyber défense, le ministère ayant pris l'habitude de ce terme. Je pense quant à moi aux cyber attaques, on a vu ce qu'il en était avec les Iraniens ou les Américains... Travaillez-vous sur les cyber combattants, afin d'éviter une ligne Maginot du numérique ? Formez-vous le personnel cyber combattant, comme autrefois les conducteurs de chars : avez-vous pris le virage ? Utilisez-vous pleinement les dispositions que le législateur vous a données en termes d'achat, par rapport au code des marchés publics, non seulement pour les forces spéciales, mais aussi pour le numérique, car les appels d'offre sont si lents qu'à leur achèvement, la technologie achetée est dépassée !

Mme Viviane Artigalas. - Vous avez évoqué l'évolution technologique. Le futur déploiement de la 5G peut avoir une grande importance pour vos activités. Il s'accompagnera d'évolution dans les structures des réseaux de télécommunications. Votre stratégie de cloud robuste s'appuiera sur un opérateur de confiance. Utiliserez-vous un système complètement dédié pour transmettre les flux de données (et quel en est le coût) ou préférerez-vous les réseaux ouverts, dans le cadre d'un abonnement peut-être, avec un niveau de sécurité amélioré ?

M. Rachel Mazuir. - Aujourd'hui les écoles d'État ont un taux de remplissage de 70% seulement. C'est un problème de fond. Votre démarche me semble intéressante. Dans l'Ain, nous avons un centre de météorologie qui semble employer de nombreux civils, et ceux-ci se reclassent ensuite facilement. Que vous apporte la 5G dans vos démarches extérieures ? Un schéma vertical de chiffrement sera possible, il intéresse aussi les entreprises.

M. Franck Montaugé, président. - Les armées françaises pourraient utiliser un cloud sécurisé opéré par Thales : Microsoft en est partie prenante, de manière non négligeable. Comment avez-vous appréhendé cette situation, et le risque induit, surtout après l'adoption du Cloud act ?

Général François Lecointre. - Nous sommes susceptibles dès aujourd'hui de lancer des cyber attaques sur le champ de bataille, pour neutraliser un adversaire ; et nous nous préparons à agir dans le champ cyber - nous serons prêts lorsque le politique nous le demandera. Je vous rappelle que le ministère de la défense est devenu ministère des armées, ce qui illustre la dimension offensive.

Je n'ai guère de compétence sur le code des marchés publics...

Général Olivier Bonnet de Paillerets. - Utilisons-nous suffisamment les régimes que vous évoquez ? Sans doute pas, mais nous les utilisons. Tout l'effort fait avec la DGA consiste précisément à revoir la relation entre le besoin opérationnel et la réponse programmatique - qui n'est pas synchronisée dans le monde cyber, c'est certain. Nous mettons en place des mécanismes qui permettent à la DGA d'intervenir en maîtrise d'oeuvre et non seulement en maîtrise d'ouvrage, donc avec une ingénierie propre, capable d'innover sur les réseaux du Comcyber : cela nous donne une vraie

souveraineté de développement, même en adaptation de ce qui existe dans le public, mais en en maîtrisant les codes. C'est fondamental. Nous permettrons aussi dans l'avenir à des entreprises d'accéder à une partie de nos données pour faire de l'expérimentation sur nos besoins : il s'agit là encore d'une souveraineté autour de l'innovation adaptée aux opérations militaires. Ce n'est pas tant aux règles des marchés publics qu'il faut déroger, mais aux processus actuels. La DGA lance des défis, injecte par ce biais de l'argent dans les entreprises pour la recherche-développement ou pour parvenir rapidement à la preuve de concept, en six mois, temps acceptable pour la cyber défense. Nous multiplions les *process* pour répondre au temps court, au temps moyen, au temps long.

Sur la 5G, j'ai réuni des réservistes spécialistes, auxquels j'ai demandé de nous dire en quoi la 5G va modifier la cyber défense. La relation entre le monde de l'expertise et le monde militaire est indispensable pour préparer une réponse aux questions stratégiques.

Général Jean-Jacques Pellerin. - La 5G va faire évoluer l'environnement. On se souvient comment la Tour Eiffel fut équipée par les premiers transmetteurs : les armées étaient en avance ! Aujourd'hui, c'est le monde civil qui tire la défense, mais les militaires sont vigilants pour préparer l'utilisation des nouvelles technologies à des fins de défense. La 5G pourra être utilisée au niveau tactique, et sur le théâtre national, pour Vigipirate par exemple. C'est un domaine maîtrisé et maîtrisable, et nous aurons le temps de nous adapter, dès lors que la technologie existante, la 4G, satisfait les besoins actuels.

Quant au *cloud*, nous avons entamé une réflexion sur ce qui pourrait être fait et à quel coût. *Cloud* n'est pas synonyme de « ouvert ». Nous avons identifié trois niveaux de *cloud* : privé, correspondant à des éléments actifs qui seraient maîtrisés par la Dirisi ; dédié, accessible à un opérateur de confiance ; et celui accessible à un opérateur plus public. Les données transiteraient sur l'un ou l'autre niveau selon le niveau de confidentialité et selon les besoins.

Thales s'est allié à Microsoft pour présenter une offre de cloud. C'est une proposition qu'ils nous font. Nous réfléchissons sur la pertinence de nous orienter vers cette technologie. Il faudra en tout état de cause faire une analyse de la valeur et savoir si le *cloud*, qui paraît effectivement une voie d'avenir, est la meilleure réponse aux besoins.

M. Jérôme Bascher. - Le numérique ne peut-il être une nouvelle composante de la dissuasion ?

Général François Lecointre. - J'ai en charge la planification des frappes et la validation des plans de frappe par le Président de la République. La destruction garantie par l'arme nucléaire en fait un outil de dissuasion extra-ordinaire. Je n'identifie pas de capacité numérique susceptible de provoquer autant de dégâts...

M. Rachel Mazuir. - Pour l'opinion publique, le numérique, c'est la guerre dans les étoiles. N'accrédite-on pas l'idée que des robots s'en chargeront, et que plus personne ne sera confronté aux dégâts ? Pourtant, une cyber attaque peut neutraliser les ambulances britanniques, on l'a vu, ou arrêter un pacemaker, Dick Cheney avait été sensibilisé à cela. La cyber guerre ne se passera ni au cinéma, ni dans les étoiles, pourtant rares sont les personnes aujourd'hui qui imaginent le danger numérique, considérable.

Général François Lecointre. - Nous intégrons dans les scénarios des attaques dans le domaine cyber ou sur des systèmes très numérisés. Un adversaire par définition peu scrupuleux agirait sur tous les champs, y compris les réseaux et les transmissions, mais aussi les hôpitaux, les aéroports, etc. Ce ne serait pas l'équivalent d'une attaque nucléaire. Mais les militaires, eux, le savent : la guerre fait mal aux hommes.

M. Franck Montaugé, président. - Nous vous remercions de cette contribution.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible en ligne sur le site du Sénat.

Audition de Me Alexis Fitzjean O Cobhthaigh, avocat, et de M. Axel Simon (La Quadrature du Net), de M. Étienne Gonnu, chargé affaires publiques (April - Promouvoir et défendre le logiciel libre) et de Me Olivier Iteanu, avocat (ISOC France),
le 9 juillet 2019

M. Franck Montaugé, président. - Mes chers collègues. Nous recevons maintenant les représentants de plusieurs associations de défense des droits et libertés des citoyens sur Internet :

- pour La Quadrature du Net, Maître Alexis Fitzjean O Cobhthaigh, avocat, et Monsieur Axel Simon ;

- pour l'association April - Promouvoir et défendre le logiciel libre, Monsieur Etienne Gonnu, chargé des affaires publiques ;

- et pour l'Internet Society France, Maître Olivier Iteanu, avocat.

Cette audition sera filmée et diffusée en direct sur le site Internet du Sénat. Elle fera également l'objet d'un compte rendu publié.

Un faux témoignage devant notre commission d'enquête serait passible des peines prévues aux articles 434-13, 434-14 et 434-15 du Code pénal. Je vous invite chacun à tour de rôle à prêter serment de dire toute la vérité, rien que la vérité ; levez la main droite et dites : « je le jure ».

Conformément à la procédure applicable aux commissions d'enquête, MM Alexis Fitzjean O Cobhthaigh, Axel Simon, Étienne Gonnu et Olivier Iteanu prêtent successivement serment.

M. Franck Montaugé, président. - Avec des différences de sensibilités et certaines nuances, vos associations sont toutes résolument engagées sur les enjeux de régulation des géants d'Internet, qui intéressent tout particulièrement les travaux de notre commission. Vos associations ont ainsi pris des positions remarquées sur la protection des données personnelles, parfois même en engageant des actions en justice contre les Gafam, ou pour la promotion d'outils alternatifs à ceux développés par les grandes entreprises dominant le marché du numérique.

Maître Alexis Fitzjean O Cobhthaigh, avocat. -Notre association existe depuis une dizaine d'années. Elle peut se prévaloir d'une expérience importante dans les sujets évoqués ici, et notamment sur le plan contentieux. À titre d'exemple, je peux citer notre action collective menée à l'encontre de Google devant la CNIL, qui a abouti à la condamnation de cette entreprise à une amende de 50 millions d'euros. D'autres dossiers similaires sont en cours, ils ont été renvoyés devant l'équivalent irlandais de la CNIL.

Une autre thématique qui nous est chère est celle de l'interopérabilité des plateformes numériques. Cette notion est aisée à comprendre : lorsque nous sommes abonnés à un opérateur téléphonique

donné, aucun obstacle ne s'oppose à ce que nous communiquions avec une personne abonnée auprès d'un autre opérateur. Il en est de même pour les messageries électroniques : rien n'empêche le titulaire d'une adresse email fournie par un prestataire donné d'échanger des courriels avec une adresse relevant d'un autre gestionnaire. Il s'agit à chaque fois de standards ouverts et interopérables. À l'inverse, lorsque vous ouvrez un compte sur Facebook ou sur Twitter, vous ne pouvez pas interagir avec un utilisateur d'une plateforme extérieure alternative. Ainsi, au moment où vous clôturez votre compte, l'ensemble des contacts créés par ce biais est perdu. Notre objectif est donc d'imposer à ces plateformes l'utilisation d'un standard ouvert, commun, , permettant d'assurer l'interopérabilité de celles-ci avec leurs alternatives.

Cette interopérabilité constituerait d'ailleurs un moyen efficace de lutter contre les causes - et pas simplement contre les symptômes - des dérives haineuses auxquelles nous sommes confrontés sur Internet.

M. Franck Montaugé, président. - En quoi l'interopérabilité à laquelle vous aspirez pourrait-elle contribuer à lutter contre la haine sur Internet ?

M. Alexis Fitzjean O Cobhthaigh. -Le modèle économique des grandes plateformes repose désormais sur une économie de l'attention. Les géants de l'Internet exploitent de manière publicitaire l'intérêt des utilisateurs. Ils recherchent donc à capter l'attention d'un maximum d'internautes le plus longtemps possible. Or ce sont justement les contenus polarisés qui attirent le plus de visiteurs, et génèrent donc le plus de profits. C'est un cercle vicieux auquel il faut mettre un terme.

Mettre en place l'interopérabilité constitue une solution à ce problème. En effet, la seule raison qui pousse les utilisateurs de Facebook ou d'autres réseaux sociaux à ne pas clôturer leur compte est la peur de perdre tous les liens qu'ils s'y sont créés. On parle ainsi d' « effet de réseau » : ce n'est pas la plateforme en tant que telle qui les attire ou les retient, mais bien les liens qu'elle permet de nouer.

À ce jour, les quelques offres alternatives à ces géants ne parviennent à attirer qu'un nombre minime d'utilisateurs. L'interopérabilité permettrait de casser ce modèle. Elle remettrait en cause la stratégie de ces géants. L'architecture même de ces plateformes joue sur l'économie de l'attention. Leurs algorithmes repèrent justement les contenus les plus clivants - voire violents - et s'efforcent de les mettre en avant en raison de leur caractère viral particulièrement lucratif.

M. Franck Montaugé, président. - Votre proposition suppose qu'il existe bien une alternative et une contre-offre de plateformes « éthiques »...

M. Alexis Fitzjean O Cobhthaigh -Elle existe déjà ! D'ailleurs, au sein de La Quadrature du Net, nous avons une telle plateforme, utilisée par 13 000 personnes et d'ores et déjà interopérable avec l'ensemble de ceux qui

recourent à la même technologie. Ce n'est pas une technologie de niche, elle est labellisée par World Wide Web Consortium (W3C), l'organisme de régulation et de normalisation du Web. Plusieurs centaines de milliers de personnes utilisent par exemple Mastodon. Les moyens technologiques sont donc bien déjà disponibles, mais ce sont des effets de réseau qui freinent actuellement leur développement.

M. Axel Simon. - N'oublions pas à quel point les grandes plateformes privées du web sont devenues énormes en termes de nombre d'utilisateurs.. C'est cette échelle qui les rend inhumaines : le volume des contenus rend impossible un contrôle sérieux de ce qui est mis en ligne - plusieurs dizaines d'heures de vidéos sont mises en ligne sur Youtube chaque minute, c'est tout bonnement impossible à superviser humainement et ces plateformes ont nécessairement recours à d'autres méthodes automatisées et intrinsèquement limitées.

Revenir à des plateformes d'une taille plus réduite permettrait de mieux superviser leur activité. Le contrôle en serait donc simplifié. Selon nous, l'interopérabilité est un moyen qui rendrait possible l'existence d'alternatives sérieuses : il s'agit simplement de donner le choix aux usagers de préférer d'autres plateformes, par exemple celles avec les conditions de modération des contenus mieux adaptées à leurs attentes. À titre de comparaison, considérons les modèles de gestion des foules : face à une foule énorme dans laquelle seraient signalés des individus dangereux, une méthode éprouvée de gestion est d'abord simplement de scinder la foule - dans certains concerts une barrière centrale vient ainsi scinder en deux l'assistance pour prévenir les mouvements de foule. Ce changement d'échelle, à lui seul diminue automatiquement la capacité de nuisance.

D'après nos observations, le cantonnement des personnes tenant un discours de haine produit des effets positifs et permet de ramener les conversations dans un registre acceptable - cela ouvre d'autres débats, notamment sur la formation de bulles informationnelles ou le risque de vase clos, mais c'est une première solution.. Cette nouvelle approche conduirait à réintroduire un véritable choix pour les utilisateurs, qui sont aujourd'hui enfermés dans les réseaux actuels.

M. Alexis Fitzjean O Cobhthaigh. -Nous avons d'ailleurs déjà procédé de la sorte il y a un siècle contre les conglomérats du chemin de fer, du pétrole...Il s'agissait alors de s'élever contre certaines industries en situation de monopole dont la taille finissait par nuire à l'intérêt général. De ces réflexions est né le droit de la concurrence. Ce que nous proposons, c'est la transposition de cet exemple au monde du numérique.

M. Axel Simon. - Parmi les sujets fondamentaux, j'aimerais insister sur la volonté des GAFA de s'introduire au fur et à mesure dans toutes les différentes couches de nos relations humaines. Ils ont commencé à faire de l'intermédiation dans l'information - à travers leurs annuaires ou moteurs de

recherche -, puis dans nos contacts - imposant de passer par eux pour entrer en relation avec nos proches -, puis dans notre identité - nous sommes devenus dépendants d'acteurs tiers pour prouver sur Internet qui nous sommes, et de nombreuses plateformes nous proposent désormais de nous connecter grâce à notre compte chez eux -, et même désormais dans la monnaie. Ces différentes évolutions démontrent clairement une stratégie d'être omniprésents.

Cela doit nous pousser à réfléchir sérieusement à la nécessité d'utiliser des alternatives et des logiciels libres. À l'heure actuelle, nous dépendons entièrement du travail d'autres personnes à qui nous sommes contraints d'accorder notre confiance.

Toutes les questions relatives à la vie privée et à la confidentialité - préalables à d'autres droits et libertés comme la liberté d'expression ou de réunion - doivent être reliées à celle du chiffrement de bout en bout. L'accès à des techniques de chiffrement fort pour l'ensemble de la population est la seule garantie fiable de protection pour nos données personnelles. D'ailleurs, sans cette protection de la vie privée, nous perdons tout droit de nous tromper. La protection est la clé qui permet d'évoluer et de changer en tant qu'êtres humains.

La vie privée reste un pilier essentiel de notre Droit. De ce fait, la question du chiffrement de bout en bout doit être l'un de nos combats.

M. Franck Montaugé, président. - Le chiffrement de bout en bout existe-t-il d'ores et déjà ?

M. Axel Simon. - Tout à fait. Certaines applications le proposent, à l'instar de Whatsapp ou des établissements bancaires. L'ensemble du commerce en ligne repose également sur cette technologie.

M. Alexis Fitzjean O Cobhthaigh. - Les logiciels libres et les standards ouverts sont particulièrement importants en ce qu'ils permettent de voir ce qui est fait. À l'inverse, les logiciels fermés rendent opaque l'information, le code est inaccessible. Confrontées à des logiciels fermés, les analyses menées dans le cadre de nos travaux ont été fortement complexifiées. En effet, l'observation d'un logiciel fermé est nécessairement extérieure et peut donc difficilement aller dans détails.

M. Etienne Gonnu. -Je représente l'association April, qui promeut les logiciels libres dont l'utilisation revêt une dimension éminemment politique. Notre association a été fondée en 1996 et comporte actuellement 4 000 membres, à la fois des particuliers et des personnes morales de droit privé ou de droit public.

Notre activité n'est pas technique, mais vise à défendre les libertés informatiques. De ce fait, nous menons des actions de sensibilisation destinées au grand public et portons un plaidoyer politique fort.

April n'a souscrit aucun engagement auprès de ses membres. Il s'agit uniquement de partager une certaine conception de l'intérêt général. À ce titre, nous considérons que la priorité doit être donnée au logiciel libre tant à l'échelle individuelle qu'au sein des administrations publiques : c'est un enjeu de souveraineté fort. Pour reprendre les propos tenus par les représentants de La Quadrature du Net, je tiens à rappeler que l'utilisateur d'un logiciel fermé ne peut pas avoir accès au code source. Dans ce contexte, comment pourrait-il lui accorder sa confiance ?

Qu'est-ce qu'un logiciel libre ? Il ne s'agit pas d'une caractéristique technique ni d'un mode de développement particulier. En réalité, c'est une manière d'appréhender le logiciel, la technologie et l'innovation, en partant du point de vue des utilisateurs pour leur garantir la pleine maîtrise de leurs outils, mais aussi la certitude que le logiciel sert effectivement leurs propres intérêts et non ceux d'un tiers.

Est qualifié de « logiciel libre » le logiciel qui permet d'assurer quatre libertés fondamentales : la liberté d'utilisation sans restriction d'usage, le droit d'étudier ce logiciel et de le modifier pour qu'il réponde à nos besoins - y compris en en corrigeant les erreurs -, le droit de redistribuer le logiciel et le droit d'en partager les versions modifiées. Si l'une de ces quatre libertés fait défaut, le logiciel n'est pas considéré comme libre. Dans ce cas, c'est un logiciel dit « privateur ».

L'oeuvre fondatrice du logiciel libre, *Code is Law*, a été écrite par Lawrence Lessig en 1999. Avocat et professeur de droit constitutionnel à Harvard, Lawrence Lessig est parti d'un constat simple : chaque époque possède son propre régulateur. Selon lui, dans l'ère du cyberespace, c'est le code informatique qui va réguler et conditionner l'ensemble de nos interactions sociales et l'exercice de nos libertés individuelles. La question qu'il a posée prend une importance d'autant plus grande que les outils informatiques occupent un rôle central dans nos sociétés actuelles. En réalité, les développeurs qui écrivent du code informatique créent du Droit, car leur logiciel interagit avec d'autres utilisateurs et façonne les conditions d'expression et l'exercice des libertés fondamentales sur les réseaux informatiques.

À ce titre, les entreprises du net que sont Facebook, Twitter ou YouTube agissent de plus en plus comme des États en ce qu'ils régissent, au sein de leur silo technologique, la liberté d'expression des citoyens utilisant leurs outils.

Dans cet environnement, nous considérons que le logiciel libre peut incarner un rapport démocratique à la technologie : il garantit d'une part la connaissance des procédures d'élaboration de ces règles et d'autre part la capacité des utilisateurs à y participer voire à les remettre en cause. Selon nous, le logiciel libre doit être la réponse politique à la question de la souveraineté numérique.

La souveraineté numérique peut être définie de différentes manières. Je rejoins la vision de la secrétaire générale de la défense et de la sécurité nationale, Claire Landais. Il s'agit de la capacité à contrôler et à définir les conditions de l'expression des libertés fondamentales sur un réseau numérique. L'enjeu est donc de déterminer les meilleures conditions de garantie de cette souveraineté.

Cette souveraineté ne doit pas constituer une fin en soi, mais plutôt un moyen d'assurer aux citoyens que l'outil informatique est bien à leur service. Du point de vue des pouvoirs publics, le numérique doit être un vecteur de libertés, et en aucun cas un outil de contrôle et d'aliénation. Malheureusement, les potentiels de surveillance résidant dans ces outils font ressortir des intérêts antagonistes.

Il n'existe pas de réponse miracle à ces questions. Au sein de notre association, nous sommes néanmoins convaincus que le logiciel libre est une condition minimale pour atteindre ces objectifs.

Par ailleurs, je tiens à réagir aux propos tenus devant cette commission par Nadi Bou Hanna, directeur interministériel du numérique et du système d'information et de communication de l'État(DINSIC). Il donnait l'impression de n'aborder ces questions que d'un point de vue technique. Or il n'est évidemment pas question de forcer les agents à une transition vers le logiciel libre. Ce sont des politiques de transition et d'accompagnement qui méritent plutôt d'être mises en place, et elles pourraient l'être aisément. La compatibilité du recours à des logiciels libres avec le droit de la commande publique a d'ores et déjà été démontrée, le Conseil national du numérique a rendu un avis en ce sens et le Conseil d'État avait validé en 2011 la légalité d'un marché public portant sur un logiciel libre gratuit. Certaines idées reçues sur les logiciels libres doivent être déconstruites.

En outre, Monsieur Nadi Bou Hanna avait récusé une approche « idéologique » du logiciel libre. Nous ne cachons effectivement pas notre conviction politique. Pour autant, cela ne nous empêche pas d'adopter une vision pragmatique de la situation. De notre point de vue, la question de la confiance est centrale et doit être soutenue par des garanties juridiques claires. Or, à l'heure actuelle, la confiance dans le secteur informatique est trop souvent déléguée à des tiers. La question est donc de savoir sur quelle base accorder sa confiance. L'un des critères capital, selon nous, de cette confiance est la possibilité de vérifier ce qui se cache dans le logiciel... et donc de recourir à un logiciel libre.

Nous menons des actions déterminées afin que soit mis un terme aux soi-disant partenariats conclus par l'État avec certains GAFA. Je pense notamment à de l'Éducation nationale déjà évoqué devant vous, ou encore celui annoncé par la Garde des Sceaux avec Microsoft dans le cadre du plan de transformation numérique de la Justice, sans qu'il n'y ait eu aucun appel d'offres. Cette situation est très inquiétante. Un tel cas de figure serait

inimaginable dans d'autres domaines économiques, et l'avantage ainsi donné à ces marques n'est pas neutre.

Le problème que nous dénonçons est particulièrement criant avec l'accord-cadre passé depuis 2009 entre Microsoft et le ministère des Armées, revu deux fois depuis et empreint d'une forte opacité. Cet accord « *open bar* » illustre un contournement massif de l'ensemble des règles relatives à la commande publique et nous faisons nôtres les constatations du rapporteur de la commission des marchés publics de l'État qui allait jusqu'à émettre de fortes réserves sur l'objet du contrat, et à suggérer l'existence de favoritisme.

Au final, ces différents accords sont autant de risques pour notre souveraineté : dans le cas de Microsoft, le groupe d'experts militaires mandaté pour en analyser les risques pointait une situation propice à la création d'une dépendance à l'égard de cette entreprise et à un affaiblissement de l'industrie française et européenne du logiciel. C'est sur la base de ces éléments, comme vous le savez, que votre collègue sénatrice Joëlle Garriaud-Maylam a proposé la création d'une commission d'enquête pour faire la lumière sur cet accord-cadre.

Dernier point, la question de la communauté, essentielle dans le monde du logiciel libre. Le logiciel est une série de connaissances - un commun informationnel - transcrites en langage informatique. Les pouvoirs publics se doivent de soutenir le logiciel libre, ressource commune et enjeu de souveraineté qui peut bénéficier à tous : individus, collectivités publiques, entreprises. Il peut être encouragé par l'État, par exemple au moyen d'appels d'offres, ou en soutenant les contributions des agents publics. Cela passe notamment par l'application effective du référentiel général d'interopérabilité, hélas encore ignoré par un trop grand nombre d'administrations, tout comme le socle interministériel des logiciels libres, catalogue de référence des logiciels libres répondant aux besoins des administrations françaises recommandés par l'État. L'accent doit enfin être porté sur des initiatives promouvant le logiciel libre lors des actions de formation, au-delà de l'apprentissage du code, pour appréhender la dimension tant scientifique que sociale de l'informatique. C'est cela qui permettra véritablement aux jeunes générations de devenir des adultes pleinement informés dans notre société où l'outil informatique et le logiciel sont omniprésents.

Maître Olivier Iteanu, avocat. -J'ai l'honneur de représenter l'association Internet Society France. C'est une association Loi 1901 qui a été créée en 1996 et dont je suis désormais Président d'honneur.

Je suis également l'avocat de cette association, et à ce titre, nous avons engagé une action de groupe à l'encontre de Facebook - non pas devant une autorité administrative, comme l'a fait La Quadrature du Net, dont je salue la démarche - mais directement devant les juridictions judiciaires pour obtenir réparation au nom du millier de plaignants ainsi

représentés. Actuellement, nous avons mis en demeure cette entreprise de réagir aux sept griefs que nous avons listés. Nous avons lancé une tentative de conciliation et à défaut, nous saisirons le TGI (tribunal de grande instance) de Paris dès le mois de septembre 2019. J'exerce le métier d'avocat spécialisé dans le numérique depuis 29 ans. J'ai également écrit plusieurs livres sur ce sujet et j'enseigne au sein des universités Paris I et Paris XI.

Tout d'abord, j'évoquerai le refus de ces entreprises de se soumettre à la loi. Ce problème est central. Nous pouvons adopter toutes les réglementations que nous voulons, si ces entreprises s'y soustraient, elles ne produiront aucun effet.

Ensuite, j'expliquerai que ces entreprises veulent appliquer leurs propres concepts. Or la liberté d'expression est une conception française qui ne doit pas être confondue avec les notions américaine de « *free speech* » ou « *hate speech* ».

Enfin, je me pencherai sur les causes de cette situation. Je constate en effet que l'Europe est la seule zone géographique dans laquelle il existe des oligopoles dans le monde du numérique. Cette particularité est liée à la notion de souveraineté numérique, ces entreprises considérant qu'elles ne sont pas soumises aux règles européennes. Il ne faut pas dès lors s'étonner de ce qu'il n'existe aucun leader européen dans ce secteur économique.

Premier point : le refus de ces entreprises de se soumettre à la loi. En introduction de l'un de mes ouvrages, je me suis mis dans la peau d'une jeune fille de 15 ans, passant au cours d'une journée type d'un réseau social à l'autre - Facebook, Twitter - et allant sur les plateformes de partage de vidéos telles que YouTube ou Netflix.. J'ai observé les conditions générales de ces services Elles sont encadrées par les lois et juridictions californiennes ! Dans ces conditions, il apparaît très compliqué de discuter avec un interlocuteur précis en cas de problème. À l'époque où des critiques étaient dirigées contre des entreprises telles que Mac Donald, ce problème n'existait pas : Au moins, il était possible d'interpeller directement le gérant de l'un de ces restaurants. Avec ces entreprises numériques, tout contact requiert de remplir un formulaire en ligne.

Leur refus de respecter la loi peut être illustré par plusieurs exemples. Dans le cadre de la transposition de la directive européenne dite « e-commerce » en 2004, nous avions mis en place un système spécial de responsabilité pour les intermédiaires techniques, comparable à celui mis en place aux États-Unis à l'époque. En effet, le cadre classique appliqué aux organes de presse ne pouvait pas être transposé tel quel aux intermédiaires techniques. Le régime juridique mis en place par cette loi prévoyait donc une responsabilité limitée, applicable uniquement si les plateformes ne retirent pas les contenus illicites dans un délai raisonnable. En contrepartie, elles s'engagent à collaborer étroitement avec les autorités judiciaires, ce qui implique de conserver les données pendant un an pour les communiquer le

cas échéant en cas de réquisition judiciaire. La sanction en cas d'infraction à ces règles est un an d'emprisonnement et 75 000 euros d'amende. Le cadre mis en place était donc parfaitement acceptable par eux et équilibré. Toutefois, en 2013, à l'occasion d'une affaire très médiatisée de tweets antisémites, le Parquet a demandé en vain à Twitter les données relatives aux comptes impliqués. Le refus de Twitter a été motivé - je me réfère aux arguments que la société a officiellement présentés devant la juridiction - par le fait que les contenus étaient hébergés aux États-Unis et ne pouvaient donc pas être concernés par la loi française. Face à cette attitude, le Parquet français n'a pas réagi.

Cet exemple démontre bien qu'il existe un réel problème de volonté et de détermination face à ces entreprises.

Un second exemple illustre encore le type de comportement auquel nous faisons face. Alors que Facebook a été condamné par la CNIL en avril 2017 à verser une amende de 150 000 euros -ce qui était alors le maximum encouru - la société a joué la politique de la chaise vide tout au long de la procédure. Est-ce admissible ? Connaissez-vous une autre entreprise européenne qui aurait adopté le même comportement ? Je pourrais vous donner des dizaines d'autres exemples similaires...

Ces entreprises sont présentes sur le marché français et y gagnent beaucoup d'argent. Elles proposent une gamme élargie de services que nous utilisons tous mais dans le même temps elles refusent d'assumer leur responsabilité et de se soumettre à la justice française. Il y a là un problème majeur.

Deuxième point : le problème des concepts importés. Notre liberté d'expression n'est pas assimilable au concept anglo-saxon du « *free speech* ». En Europe, nous l'encadrons car nous considérons qu'il existe un lien fort entre la parole publique et le passage à l'acte, tel n'est pas le cas aux États-Unis. Quand bien même ces entreprises prendraient des engagements forts en matière de modération interne des contenus, c'est bien la loi qui doit s'appliquer. De la même manière, il convient de distinguer les notions de vie personnelle et de « privacy ».

Considérons les problématiques liées au droit d'auteur. Nous avons harmonisé les droits nationaux en la matière. Aux États-Unis, l'industrie d'Hollywood est très puissante et dans ce domaine, les GAFA prennent réellement au sérieux le droit d'auteur. Je citerai le cas d'un producteur américain qui avait notifié à YouTube que 100 000 vidéos portaient atteinte à ses droits. Dès le lendemain, elles avaient été retirées de la plateforme. Cela démontre bien que les droits sont respectés dès lors que des risques judiciaires sérieux sont encourus.

J'ai d'ailleurs pu le constater à l'occasion d'une affaire dont je m'occupais. Une personne avait vu son image utilisée pour créer un groupe Facebook insultant à son égard. Lorsque nous avons tenté d'argumenter en

nous fondant sur l'injure pour obtenir la fermeture du compte, cela n'a eu aucun effet. En revanche, en remplissant le formulaire et en motivant notre demande par une violation du droit d'auteur, le groupe a pu aussitôt être fermé. Cet exemple doit nous convaincre qu'une réelle volonté associée à un risque de sanction porte ses fruits.

Je terminerai en évoquant les causes de cette situation. le courant porté par les libertariens constitue selon moi le cheval de Troie de l'industrie de la Silicon Valley. Comment se fait-il qu'entre l'industrie chinoise et les GAFA, nous ne soyons alertés que des problématiques possibles de la première et laissions les secondes prospérer ? Il me semble que cette différence dans notre perception découle justement des discours avant-gardistes sur la liberté mis en avant par les acteurs américains. Les mots et les concepts qui nous sont vendus ont paralysé la réflexion. Personne ne peut être opposé à la liberté. Toutefois, quand nous analysons leur comportement de plus près, nous ne pouvons que constater à quel point la réalité est éloignée de leurs grands discours, tant la guerre qu'ils mènent à l'encontre de leurs concurrents est rude.

La lecture de *The New Digital Age* d'Éric Schmidt et Jared Cohen est plaisante, au début - ils nous décrivent le nouveau monde de liberté qui s'ouvre -... jusqu'à ce que les auteurs expliquent qu'il faudra quand même tenir compte du référencement Google pour choisir un prénom à son enfant...

Je pense que notre action doit être menée au niveau de nos valeurs, notamment sur le plan juridique. Pour autant, nous devons prendre conscience que la situation actuelle est aussi une véritable guerre des mots.

M. Gérard Longuet, rapporteur. - Ces propos sont passionnants. La souveraineté est une notion qui implique en premier lieu que nos lois nationales soient appliquées sur l'ensemble du territoire. Se pose alors la question de la définition d'un territoire. J'ai été très sensible aux propos de Maître Olivier Iteanu sur les libertariens. L'idée d'un monde virtuel peut paraître très séduisante.

Au niveau des propositions développées, je souhaiterais revenir sur le droit à la portabilité. Comment l'imaginez-vous concrètement ? Un réseau est une entreprise commerciale, et il tente de se positionner en fonction de sa cible commerciale, en fonction de critères sociologiques. Dans ce contexte, un réseau social connaît-il des cycles dans son existence ? La portabilité est-elle une réponse pour pouvoir passer de l'un à l'autre ?

M. Alexis Fitzjean O Cobhthaigh. -Au niveau terminologique, distinguons bien la notion d'interopérabilité, que nous appelons de nos voeux, de la notion de portabilité, qui existe déjà en droit.

Dans la jeune histoire du web, certains réseaux communautaires ont effectivement disparu qui étaient centrés sur certaines catégories d'utilisateurs. Le cas des réseaux actuels doit être appréhendé différemment.

Aujourd'hui, Facebook compte quasiment deux milliards de comptes. Même en écartant les faux comptes de notre analyse, nous sommes forcés de constater que cette plateforme a changé de nature. Elle exerce un pouvoir concret sur nos vies et sur nos États.

En réalité, il ne s'agit plus seulement d'un réseau social, tant les possibilités qu'elle offre sont nombreuses. J'ai été très surpris de constater que la SNCF allait proposer la vente de billets de train via le tchat de Facebook. La SNCF n'avait pourtant pas besoin de recourir aux services de cette entreprise américaine, et cela va créer une forme d'assujettissement à un service tiers. Que se passera-t-il demain si Facebook met fin à ce service, souhaite le monétiser ou met en place des conditions générales déséquilibrées ?

De même, ces géants n'hésitent pas à acquérir à prix d'or les nouveaux réseaux émergents à la mode.

M. Gérard Longuet, rapporteur. - Tout à fait. Leur stratégie de destruction de la concurrence par des acquisitions sélectives à des prix très important pose problème.

M. Alexis Fitzjean O Cobhthaigh. - La qualification d'un cycle est possible, dans une certaine mesure, et certains réseaux sociaux ont aujourd'hui disparu. Toutefois, à l'échelle de ces puissances, ce n'est pas la question principale : aujourd'hui, les plateformes ont acquis une puissance inédite dans l'histoire, elle ne se contentent plus de vendre un service, mais bien de capter une multitude d'informations qui leur permet de développer des modèles prédictifs de comportements et d'offrir des prestations grâce à une granularité des données extrêmement fine sur une masse d'individus.-

À ce titre, ayons à l'esprit le scandale Cambridge Analytica qui a révélé au grand jour la manipulation dont ont été victimes énormément de personnes. Si la publicité et la propagande n'ont rien de nouveau, pour autant, les plateformes Internet les ont portées aujourd'hui à un niveau inédit dans l'histoire de l'humanité.

M. Gérard Longuet, rapporteur. - Et l'interopérabilité peut constituer une solution, selon vous ?

M. Alexis Fitzjean O Cobhthaigh. - Absolument, car l'une des forces de ces plateformes actuellement réside dans la puissance de l'effet de réseaux et la difficulté de pouvoir s'en passer pour beaucoup de personnes. Ces réseaux sont devenus des moyens de communication sans lesquels la population se coupe de ses contacts sociaux. L'interopérabilité permettrait de mettre un terme à cette situation en rendant possible de poursuivre les échanges avec les contacts de son propre réseau tout en changeant de plateformes à sa guise.

M. Olivier Iteanu - La portabilité des données nous rappelle les débats autour de la notion controversée de propriété des données. Notre

conception juridique fermement ancrée en Europe est que les données à caractère personnel ne sont pas cessibles, mais qu'elles constituent bien un attribut juridique de la personnalité des individus, hors commerce. Si un internaute consent à ce que ses données soient collectées, il peut dans la seconde suivante demander qu'elles lui soient restituées.

À l'inverse, les Anglo-saxons tendent à adopter une vision patrimoniale des données. Dans cette logique, la cession des données personnelles aux géants du numérique, au prétexte d'en recevoir un hypothétique et dérisoire bénéfice, va en fait de pair avec une perte de contrôle des individus sur leur utilisation. Selon moi, nous devons donc rester fermement attachés à la conception européenne qui qualifie les données personnelles comme des attributs de la personnalité juridique.

Quand on parle de droit à la portabilité des données, de quelles données s'agit-il ? N'oublions pas qu'outre celles qui ont été renseignées, par exemple lors de l'ouverture d'un compte, il y a aussi celles qui ont été collectées durant l'utilisation du réseau. De même, il faut tenir compte des données issues de croisement et partagées entre les différents réseaux, à l'instar de Whatsapp et Facebook.

Ces données là aussi devraient pouvoir faire l'objet du droit à la portabilité, mais on s'attaque alors ici directement le modèle économique de ces grandes entreprises : leur valorisation boursière repose uniquement sur leur capacité à collecter et exploiter ces données ! Face à cela, nous devons affirmer nos valeurs fondamentales. Nous en avons encore les moyens, car si nous avons certes perdu la guerre technologique, l'accès à un marché convoité de 500 millions de consommateurs nous autorise encore à en fixer les règles.

M. Gérard Longuet, rapporteur. -J'aimerais adopter le point de vue d'un libertaire : de quel droit les autorités publiques priveraient-elles les 500 millions d'Européens de la possibilité d'utiliser Google ?

M. Alexis Fitzjean O Cobhthaigh. - C'est justement tout l'intérêt de l'interopérabilité : elle n'empêche personne d'appartenir à un réseau donné. Le principe est juste d'offrir le choix de leur plateforme à tous les utilisateurs de ces réseaux. Il permet de continuer à communiquer avec l'ensemble de ses contacts, quels que soient leurs réseaux.

M. Gérard Longuet, rapporteur. - Il me semble difficile de restreindre l'utilisation des grands réseaux. Les populations risqueraient de mal comprendre l'objectif d'un tel cadre.

M. Olivier Iteanu. - Notre position vise simplement à s'assurer de ce que les GAFA respectent nos lois, mais aussi à proposer des alternatives aux citoyens.

M. Pierre Ouzoulias. - J'aimerais revenir sur les propos précédemment tenus devant notre commission par M. Nadi Bou Hanna,

directeur interministériel du numérique et du système d'information et de communication de l'État. Il nous a expliqué que c'étaient les choix des usagers, la manière dont les fonctionnaires utilisaient leur logiciel, qui était déterminante. À titre personnel, je suis fier de ne recourir qu'à des logiciels libres.

Ce qui m'inquiète profondément est l'absence totale de prise en compte du critère de souveraineté dans le cadre des achats publics réalisés par l'État - à l'exception notable du ministère des Armées dont nous avons entendu les représentants.

Aujourd'hui, lorsque nous achetons un réfrigérateur, nous sommes en mesure de connaître sa dépense énergétique grâce à un affichage obligatoire. Serait-il envisageable d'adopter un système de labellisation comparable en termes de souveraineté et de protection des données personnelles ? M. Etienne Gonnu, votre association April pourrait-elle agir en tant que certificateur d'un tel système ?

À l'heure actuelle, lorsque je recherche un logiciel libre, je me renseigne sur le site Internet de l'Université de Lausanne qui regorge d'informations et de conseils pertinents. Je déplore qu'aucun site français ne dispose de ce type d'informations. Il serait également intéressant d'y songer, pourquoi pas à travers une collaboration entre votre association et le Gouvernement.

M. Etienne Gonnu, chargé affaires publiques (April). - S'agissant d'un système de certification, il me semble que l'association April n'a pas cette vocation-là.

Concernant le manque d'information relative aux logiciels libres que vous regrettez, nous devons porter notre attention vers l'éducation des jeunes. Il faut leur apprendre ce qu'est un logiciel libre, mais aussi insister sur son importance. Toute la population n'est pas constituée d'informaticiens ou d'experts en informatique, mais chacun gagne à être formé sur le principe des logiciels libres, la nécessité d'avoir un recul critique sur l'outil informatique, et la possibilité de collaborer au savoir commun par ces technologies... Prenons l'exemple de la presse : si tout le monde n'a pas vocation à devenir journaliste, la liberté de la presse est un principe qui protège et bénéficie à l'ensemble des citoyens.

La mise en place d'une labellisation me semble une entreprise délicate, en raison de la difficulté à dégager des critères pertinents autres que les quatre critères de base du logiciel libre que je vous ai exposés.

Un autre aspect essentiel en termes de souveraineté est celui de la mémoire et de l'archivage : format ouvert et logiciels libres sont des garanties de pérennité des services.

M. Gérard Longuet, rapporteur. -La mémoire est-elle un atout ou un inconvénient ?

À ce titre, l'Institut National de Recherche en Informatique et en Automatique (INRIA) a lancé le projet *Software Heritage* visant précisément à archiver l'ensemble des codes sources à l'origine des logiciels produits dans le monde.

M. Alexis Fitzjean O Cobhthaigh. -La mémoire est à la fois un atout et inconvénient, mais surtout le choix doit nous appartenir collectivement et la décision ne doit pas être déléguée à des sociétés privées. Lorsque nous faisons des choix technologiques qui reposent sur des logiciels qui peuvent devenir obsolètes quand leur mise à jour ou leur maintenance n'est plus assurée, la mémoire est un atout.

En revanche, quand il s'agit d'assurer l'exercice du droit à l'oubli ou du droit à l'erreur, la mémoire peut s'avérer dommageable sur Internet...Mais en toute hypothèse, il doit s'agir de choix déterminés par la société, par le Parlement : nous ne devons pas laisser des entreprises commerciales décider par exemple des durées de conservation des données !

M. Gérard Longuet, rapporteur. - Mais les utilisateurs ne préfèrent-ils pas justement bénéficier d'un service gratuit en échange de l'acceptation de l'utilisation de leurs données, plutôt que d'avoir à payer l'opérateur ?

M. Alexis Fitzjean O Cobhthaigh. -Un tel comportement est totalement illégale au regard des dispositions du RGPD En effet, l'utilisateur ne donne pas un consentement libre et éclairé lorsqu'il doit accepter que ses données soient collectées comme condition pour accéder au service. Cette analyse est d'ailleurs partagée les régulateurs et ressort des lignes directrices de la CNIL.

Par ailleurs, les ministères déboursent des sommes colossales pour s'équiper en logiciels fermés... mais à quel prix ? Certes, on l'a dit, la praticité pour l'usager est importante dans les administrations, mais si cet argent était utilisé pour la formation des personnels et pour des logiciels libres, cela serait bien moins coûteux Cela permettrait de modifier ledit logiciel pour l'adapter directement à ses besoins, voire pour changer facilement de prestataire tout en ayant des effets bénéfiques sur l'ensemble du système. En réalité, il s'agit d'un enjeu de nature politique.

J'insiste aussi sur le fait que les logiciels propriétaires fonctionnent sur la base d'un code fermé. Dès lors, nos administrations ne sont pas en mesure de savoir réellement ce qui se cache derrière - conformité aux annonces, voire présence de portes dérobées. Nous ne voyons que ce que l'entreprise est disposée à révéler.

M. Olivier Iteanu. - La question du logiciel libre est intimement liée à celle de la souveraineté. Même au sein de l'association Cigref, qui regroupe les DSI des grandes entreprises et administrations publiques autour de la question du numérique, et dont les membres étaient traditionnellement divisés en groupes de travail selon leur choix de fournisseur - par exemple le groupe Microsoft, le groupe Oracle ou le groupe Google - un groupe

spécifique sur le logiciel libre a récemment été mis en place tant cette question est cruciale.

Une illustration personnelle et concrète de l'importance de l'interopérabilité : J'avais moi-même tenté d'organiser mon activité professionnelle sous l'égide d'un logiciel libre. J'ai été contraint d'abandonner l'expérience en raison des dysfonctionnements observés dans ma communication avec certains clients qui ne parvenaient pas à lire mes fichiers. Le logiciel en tant que tel fonctionnait parfaitement bien, mais les interactions avec mes partenaires professionnels étaient parfois délicates.

M. Gérard Longuet, rapporteur. - Il me semble intéressant que les consommateurs se réunissent au sein d'associations afin d'équilibrer les rapports de force entre les vendeurs et les utilisateurs. En se groupant, les particuliers acquièrent un certain poids vis-à-vis des entreprises.

M. Franck Montaugé, président. - Je vous remercie d'avoir ainsi restitué la dimension politique et sociétale forte du sujet qui occupe nos travaux. Nous avons reçu il y a peu le philosophe Bernard Stiegler, philosophe de la technique, qui en appelle à un « web néguentropique ». Selon lui, la direction prise par l'Internet relève plus de la destruction que de l'élévation.

Vos solutions peuvent-elles participer à ce projet de sauvetage du web ?? Est-ce une adaptation du capitalisme 2.0 qu'il faut appeler de nos voeux, qui engloberait en son sein l'ensemble des problématiques universelles auxquelles nous sommes confrontés à l'heure actuelle telles que le climat et les transitions que nous vivons ?

J'ai beaucoup apprécié vos propos sur les plateformes : vous déploriez que leurs échelles actuelles détruisent plus qu'elles ne créent de valeurs intrinsèques, il me semble que vous rejoignez certains des écrits de. Bernard Stiegler qui va même jusqu'à affirmer qu'il faudrait sauver le capitalisme de lui-même.

M. Axel Simon. - Les questions que vous soumettez sont très profondes. Le système économique capitaliste fonctionne sur une capacité à tout absorber pour l'intégrer à son propre fonctionnement. Son but est de réaliser du profit. .

Or, à l'heure actuelle, il semblerait que les limites soient atteintes. J'ai entendu plusieurs acteurs évoquer la notion de capitalisme de surveillance : à son tour, la surveillance devient une source de profits. Cela démontre à quel point les échelles atteintes par certains acteurs du système sont dangereuses. Dans ce contexte, les masses atteintes deviennent critiques à tous les niveaux : pour consommer, pour être manipulées, voire dominées.

Quelle sera l'espérance de vie de ces entreprises ? Un réseau géré par une trentaine de personnes depuis les États-Unis et englobant deux milliards d'utilisateurs a atteint des dimensions inédites et incommensurables dans

l'histoire humaine. C'est aussi pour cela que ces acteurs, malgré leur hégémonie, répètent sans cesse, pour nous rassurer, qu'ils sont neutres, qu'ils offrent une simple infrastructure de communication et de rapprochement entre les gens, dont le caractère profitable serait un à-côté heureux mais purement fortuit. En réalité, ce n'est pas le cas. Le nombre, la répétition et l'ampleur des scandales qui les compromettent le démontrent.

Auparavant, le système était moins centralisé et cela donnait lieu à un paysage différent. Malgré tout, les époques sont difficilement comparables tant les technologies ont évolué. Si Internet était aujourd'hui moins dépendant de ces entreprises, le résultat serait sans doute différent de cette époque. Dans tous les cas, nous devons nous interroger sur les moyens de revenir à un système moins centré sur ces grands acteurs centraux, au besoin par la contrainte publique.

M. Olivier Iteanu. - Notre société repose sur trois piliers : la vérité, la justice et la paix. Derrière, le terme de souveraineté, trop souvent connoté politiquement, se situent en réalité des enjeux de paix.

M. Etienne Gonnu. - La question de la centralisation d'Internet est cruciale. Il faut que nous évitions les noeuds de pouvoirs - c'était la promesse fondatrice de l'internet, créé sur une base a-centrée et distribuée. Or je ne peux que déplorer l'attitude qui tend à capituler face à ces grandes plateformes. Antiterrorisme, lutte contre les fausses informations, application du droit d'auteur... Nous devons arrêter d'adopter des textes qui ont pour effet de renforcer la centralisation du système. Nous leur déléguons de véritables prérogatives de puissance publique !

Au contraire, il faudrait leur opposer une réponse judiciaire - et pour cela allouer des moyens suffisants à nos services publics en la matière -, et non pas adopter une attitude de résignation.

M. Gérard Longuet, rapporteur. - Afin de compléter nos travaux, je serais demandeur d'une note de synthèse sur la forme que peut prendre l'organisation internationale des usagers. J'aimerais en apprendre davantage sur le poids des usagers, tant aux États-Unis qu'en Europe. Cela permettrait de prendre la mesure de leur force.

M. Alexis Fitzjean O Cobhthaigh. - La question de l'organisation d'Internet est transversale et occuperait facilement plusieurs thèses.

Elle renvoie d'abord à l'idée que la technologie n'est pas neutre. Ainsi, la conception technologique d'Internet induit des choix dans son utilisation. Le fait de choisir une technologie centrée ou acentrée a effectivement des conséquences réelles. Dans les années 90, la technologie choisie pour le web - l'hyperlien qui permet en un seul « clic » d'être redirigé vers d'autres ressources- a été acentrée.

Par ailleurs, il convient de distinguer le capitalisme et le libéralisme. Le libéralisme est un préalable incontournable lorsqu'une société aspire à la

transparence de l'information. C'est dans ce contexte libéral que le droit de la concurrence a pu naître et se développer. Notre association considère que l'interopérabilité aurait pour effet positif la conservation de cette transparence. Elle permettrait d'assurer à chaque utilisateur une réelle liberté de choix entre les opérateurs. Il me semble donc que nos propositions ne sont pas du tout opposées au libéralisme. Bien au contraire, elles apportent une dose de liberté plus élevée.

La réunion est close à 16 h 30.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible en ligne sur le site du Sénat.

Audition de M. Daniel Bursaux, directeur général de l'IGN,
le 10 juillet 2019

M. Franck Montaugé, président. - Mes chers collègues, nous recevons M. Daniel Bursaux, directeur général de l'Institut national de l'information géographique et forestière (IGN), accompagné de MM. Sylvain Latarget, directeur général adjoint, et de Claude Pénicand, délégué à la stratégie de l'établissement.

Cette audition sera diffusée en direct sur le site internet du Sénat. Elle fera également l'objet d'un compte rendu publié.

Enfin, je rappelle, pour la forme, qu'un faux témoignage devant notre commission d'enquête serait passible des peines prévues aux articles 434-13, 434-14 et 434-15 du code pénal. Je vous invite chacun à tour de rôle à prêter serment de dire toute la vérité, rien que la vérité ; levez la main droite et dites : « Je le jure ».

Conformément à la procédure applicable aux commissions d'enquête, MM Daniel Bursaux, Sylvain Latarget et Claude Penicand prêtent serment.

M. Franck Montaugé, président. - L'Institut national de l'information géographique et forestière (IGN) entretient des bases de données multithématiques de qualité maitrisée qui décrivent le territoire et les phénomènes qui s'y produisent afin d'appuyer la définition, la mise en oeuvre ou l'évaluation des politiques publiques.

En s'appuyant notamment sur vos données, ainsi que celles de la Poste, une base des adresses géolocalisées est disponible en open data et permet d'asseoir maintenant des systèmes industriels sérieux sur des informations ne venant pas d'une plateforme privée. Il me semble que, de cette manière, vous contribuez à la souveraineté numérique de notre pays.

Comment définissez-vous la souveraineté numérique ? Comment y participez-vous ?

Identifiez-vous des angles faibles dans votre domaine de compétence ou pensez-vous que la politique menée permet à la France de garantir son autonomie et sa souveraineté ?

M. Daniel Bursaux, directeur général de l'IGN. - Je vous remercie de me donner l'occasion d'exposer en quoi l'Institut national de l'information géographique et forestière constitue un outil essentiel d'information géolocalisée au service de la puissance publique afin que celle-ci préserve sa souveraineté, à l'heure de la transformation numérique de la société.

Dans un monde devenu tout numérique, la géolocalisation joue un rôle tout à fait particulier. Le développement des terminaux mobiles de communication et des moyens de positionnement par satellite, tels les

smartphones, les GPS et autres objets connectés, permet la production, la circulation et l'échange au quotidien d'un très grand nombre de données géolocalisées. Chacun d'entre nous est d'ailleurs producteur de telles données, parfois à son insu.

La géolocalisation est ainsi devenue très rapidement l'une des clés principales pour le croisement d'une multitude de données souvent hétérogènes et pour le développement d'applications numériques devenues omniprésentes, au niveau tant de la sphère professionnelle que de la sphère privée.

Pour exploiter cette géolocalisation, il est cependant nécessaire de s'appuyer sur des référentiels géographiques fiables et partagés, qui permettent de rapprocher et de mettre en cohérence ces diverses données. Ces référentiels jouent ainsi un rôle essentiel en termes de croisement et d'exploitation des données et constituent un point de passage obligé pour le traitement d'une très grande variété d'informations.

Les grands acteurs de l'internet, au premier rang desquels les GAFA, ont investi très fortement dans la constitution de fonds géographiques en support de leur stratégie de développement. Leur simplicité d'utilisation et leur gratuité relative - les usages non basiques étant payants -en ont fait des produits de consommation courante pour les citoyens.

Néanmoins, la transformation numérique confronte la puissance publique à un défi inédit en matière d'exercice de sa souveraineté, entendue au sens large. Elle doit en effet garder dans ce contexte très évolutif la capacité d'agir de manière indépendante et d'exercer l'autorité dont elle est démocratiquement investie.

Pour cela, il est indispensable que la puissance publique conserve la maîtrise des données qui fondent ses décisions, au même titre qu'elle conserve celle de ses autres infrastructures essentielles, et ce notamment face aux majors de l'internet qui fondent leur puissance sur l'aptitude à concentrer et exploiter une quantité sans cesse croissante de données.

Cette maîtrise conditionne non seulement l'efficience de l'action publique, qui doit pouvoir se fonder sur des données qualifiées, mais aussi la confiance que les citoyens placent en elle. On se souvient encore, en 2014, de la complaisance de Google vis-à-vis des régimes russe et ukrainien lors de la crise de Crimée : selon le pays dans lequel on se connectait, les frontières n'étaient pas tout à fait les mêmes. On peut également citer la question du Tibet vue par les Chinois ou encore celle du Sahara occidental vue par le Maroc.

Cette maîtrise de l'information géographique contribue également à la souveraineté nationale entendue dans son acception économique, en permettant aux entreprises nationales de ne pas dépendre de grandes plateformes étrangères pour développer leur activité.

La donnée géographique présente donc, plus que n'importe quelle autre, un lien étroit avec la souveraineté.

De fait, la puissance publique mobilise quotidiennement des données géographiques et plus largement des données géolocalisées à l'appui de ses décisions et de son action, dans des domaines aussi variés que la défense nationale, la sécurité, la prévention des risques, la préservation de la biodiversité, l'aménagement du territoire, l'agriculture, la forêt, les transports...

En tant qu'opérateur de l'État, l'IGN, établissement public administratif, produit et entretient, comme cela a été dit, des données géographiques de qualité maitrisée qui décrivent le territoire et les phénomènes qui s'y produisent afin d'appuyer la définition, la mise en oeuvre ou l'évaluation des politiques publiques. Organisées sous forme de référentiels interopérables, ces données multithématiques constituent des données d'autorité qui offrent aux décideurs publics des informations au service de la souveraineté nationale.

L'IGN élabore par exemple des modèles numériques de terrain très précis, qui permettent à la Direction générale de la prévention des risques de réaliser des modèles de prévision de crues. De même, lorsque des crues surviennent, l'institut réalise des prises de vue aériennes en urgence et pour l'appui à la prévision des inondations. Ces photographies constituent des preuves opposables pour la délimitation précise de l'étendue des inondations. Elles servent également de « vérité terrain » pour affiner les modèles de prévision, accroître l'efficacité des mesures de prévention et définir les règles d'urbanisme.

L'IGN est aussi chargé de l'entretien du Registre parcellaire graphique, qui sert de référence pour les déclarations des exploitants agricoles. Il permet à l'Agence de services et de paiement (ASP) de connaître les surfaces pour le calcul des aides versées aux agriculteurs dans le cadre de la politique agricole commune (PAC). Depuis 2014, il s'agit d'une activité soutenue, car la Commission européenne avait menacé la France d'une amende substantielle, lui reprochant de ne pas apporter suffisamment de preuves sur le calcul qu'elle opérait pour le versement des aides aux agriculteurs.

L'IGN entretient également un inventaire statistique permanent des ressources forestières permettant notamment de disposer d'une connaissance objective sur la captation du carbone et sur les ressources en bois mobilisables pour différents usages. Cette connaissance contribue également aux réflexions prospectives pour l'adaptation au changement climatique. Cette activité explique notre nouveau nom depuis 2012, même si nous avons conservé l'ancien sigle.

Par ailleurs, l'IGN s'implique actuellement dans la mise au point d'une méthode de description de l'occupation des sols à partir d'imagerie

satellitaire et aéroportée et de technologies d'intelligence artificielle, telles que l'apprentissage profond. Cette méthode doit permettre au ministère de la transition écologique et solidaire de mettre en place un dispositif innovant de suivi de l'artificialisation des sols, en application de l'action 7 du plan Biodiversité. Il s'agit d'un exercice extrêmement complexe.

L'IGN travaille en étroite collaboration avec la Délégation à la sécurité routière. Nous avons mis au point un dispositif qui permet aux autorités de contrôle de prouver une infraction en faisant le lien entre le lieu du véhicule et la vitesse autorisée. Nous construisons également une base de données des vitesses limites autorisées en licence ouverte.

Je citerai encore la base de données hydrographique, dite BD Topage, développée en collaboration avec l'Agence française pour la biodiversité, pour les besoins de la police de l'eau. Ce référentiel hydrographique, en licence ouverte, mettra à la disposition de l'ensemble des acteurs de l'eau une base de données exhaustive, collaborative et interopérable, d'ici à la fin de 2019.

Par ailleurs, les capacités de recherche, de formation, d'ingénierie, d'innovation et de production dont dispose l'IGN lui confèrent un savoir-faire unique en France en matière de maîtrise de l'ensemble des techniques de l'information géographique ainsi que d'une expérience inégalée en termes de précision des données produites. L'expertise de l'institut est reconnue internationalement.

À titre d'illustration, l'IGN est un acteur clé à l'échelle mondiale dans le domaine de la géodésie, la science qui étudie la forme et les dimensions de la Terre. Dans ce cadre, l'institut est chargé de la détermination du système national de coordonnées de haute qualité, indispensable pour pouvoir déterminer des coordonnées géolocalisées d'un point, sous la forme de repères de nivellement. Ces points précis au centimètre près sont utilisés par un grand nombre de professionnels : géomètres, aménageurs, urbanistes, ingénieurs, hydrologues, forestiers... La sécurité publique dépend souvent de la fiabilité de ces informations. Dans ce contexte, les mouvements de certaines zones sensibles sont particulièrement observés, comme l'affaissement des anciens bassins miniers ou les conséquences de l'activité sismique sous-marine à Mayotte.

L'institut a aussi contribué activement à la détermination du système mondial de coordonnées, dit GGRF (Global Geodetic Reference Frame). Il participe également à l'infrastructure de stations de suivi au sol des satellites de positionnement pour Galileo.

D'ailleurs, l'expertise internationale de l'IGN dans ce domaine a trouvé une reconnaissance concrète dans l'élection d'un directeur de recherche à l'IGN en tant que président de l'Association internationale de géodésie.

Face à un nouveau champ de contraintes - l'enjeu croissant que représente la préservation de la maîtrise des données géographiques qui fondent la décision publique, d'une part, le choix gouvernemental d'étendre largement le champ de la mise à disposition gratuite des données publiques, d'autre part -, l'IGN n'est toutefois pas en mesure d'assumer seul l'effort de production et d'entretien de toutes les données utiles, voire essentielles. Il est dès lors nécessaire de mobiliser toutes les énergies, en particulier celles des autres acteurs qui produisent des données géographiques. Les collectivités, les autres établissements publics, mais aussi de simples citoyens peuvent contribuer, au travers de leur usage ou de façon volontaire, à consolider les données.

L'IGN est donc appelé à mettre à profit son expertise pour optimiser le recours aux différentes capacités d'acquisition, gérer l'agrégation et l'intégration des diverses contributions ainsi que leur standardisation, et assurer un certain niveau de maîtrise de la qualité.

L'IGN a déjà exercé ce rôle de coordinateur technique et de tiers de confiance pour répondre aux besoins de certains ministères, notamment du ministère des armées. Celui-ci s'appuie depuis plusieurs années sur l'institut pour gérer l'approvisionnement de données géographiques de précision, nécessaires au bon fonctionnement des systèmes d'aide au commandement et des systèmes d'armes. Dans ce cadre, l'IGN est chargé d'organiser le recours aux capacités de l'industrie afin de couvrir les vastes zones d'intérêt pour les forces armées en territoire extérieur, de qualifier les données produites par des grands opérateurs - Airbus, Thalès -, ainsi que de produire lui-même les données « socle » sur lesquelles s'appuient les productions industrielles.

Ce rôle de tiers de confiance ne concerne d'ailleurs pas uniquement les domaines régaliens où la maitrise de l'État doit être forte. À mon sens, il est essentiel, pour la puissance publique, de disposer d'une capacité d'expertise indépendante lorsqu'elle confie des travaux complexes à un industriel.

Par exemple, dans le cadre de la stratégie nationale pour le développement des véhicules autonomes, le ministère chargé des transports a mandaté l'IGN pour contribuer à l'élaboration d'un standard pour une cartographie haute définition et dynamique utile aux véhicules autonomes, pour réfléchir à la gouvernance globale des données géolocalisées utilisées par ces véhicules et pour définir les moyens dont l'État devrait se doter pour exercer à terme son rôle de police et de régulation.

C'est pourquoi l'institut s'est engagé dans une transformation profonde de sa mission historique, de son organisation, de son modèle économique et de ses méthodes de travail pour renforcer l'appui direct aux politiques publiques.

Cette feuille de route vise à rééquilibrer l'activité de l'IGN. De diffuseur de données, il a vocation à devenir l'architecte référent de l'ensemble des données géographiques nécessaires à l'exercice des politiques publiques. L'IGN se repositionne ainsi au coeur d'un écosystème de partenaires, afin de garantir la disponibilité et la qualité des données importantes pour l'action publique.

Outre ce rôle de garant de la disponibilité des données géographiques souveraines, l'IGN renforce ses activités de formation et de recherche, sa maîtrise des nouvelles technologies ainsi que sa capacité d'innovation. L'objectif est de maintenir notre expertise et notre savoir-faire de pointe, notamment grâce à notre école nationale des sciences géographiques (ENSG) et à ses unités mixtes de recherche. Soixante ingénieurs sont formés par an : tous trouvent un emploi à la sortie de l'école ; une bonne demi-douzaine d'entre eux entre à l'IGN, les autres intégrant le service public ou privé. L'IGN est partie prenante du futur pôle universitaire Gustave Eiffel à Champs-sur-Marne, qui constitue une opportunité d'associer le monde académique, les acteurs publics et les entreprises pour devenir le laboratoire des villes et des transports du futur. Les différents organismes fondateurs qui regroupent leurs capacités pour constituer cette université d'un nouveau mode finalisent actuellement les statuts en vue d'une mise en place effective au 1er janvier 2020.

Il s'agit pour l'IGN à la fois d'entretenir sa propre expertise au meilleur niveau et de jouer un rôle dans la montée en compétence collective des administrations et de la société civile. Cela permettra à la puissance publique de tirer le meilleur profit des données géographiques et de mener les actions qui sont essentielles à la préservation de sa souveraineté. Cela aidera aussi les entreprises nationales à se positionner face à la concurrence internationale.

En réponse à une mission confiée par le Premier ministre sur les données géographiques souveraines, Mme la députée Valéria Faure-Muntian a formulé au mois de juillet 2018 un certain nombre de recommandations qui confortent le nouveau positionnement de l'IGN et réaffirment la nécessité pour l'État de disposer d'un tel opérateur.

L'IGN est bien un outil qui garantit la possibilité pour la puissance publique de prendre un certain nombre de dispositions en vue de préserver son indépendance et sa souveraineté informationnelle dans le domaine des données géographiques. Il est donc plus que nécessaire de maintenir et de développer au sein de l'IGN des compétences clefs pour dominer les nouvelles technologies et une force d'action suffisante. Le ministère des armées a fait le choix de maintenir des compétences indispensables à la conception et à l'entretien de ses capacités militaires, afin de préserver son indépendance d'action. Nous sommes confrontés à des problématiques similaires.

À l'heure où une forte compétition s'exerce entre les entreprises pour recruter les meilleures compétences dans le domaine du numérique, le fait d'avoir un statut d'établissement public et d'être tenu par un recrutement de fonctionnaires peut parfois poser problème : il n'est qu'à voir les salaires proposés à des spécialistes dans le secteur privé.

Dans le contexte de contraintes qui s'imposent à nous en matière de finances publiques, d'effectifs et d'élargissement de l'open data, l'IGN doit relever le défi de maintenir un centre national d'expertise en appui des politiques publiques. C'est tout l'enjeu des prochaines années et le défi du projet d'établissement que j'essaye de conduire avec mes équipes et l'appui des ministères de tutelle.

M. Gérard Longuet, rapporteur. - Monsieur Bursaux, je vous ai connu dans plusieurs autres vies, notamment à l'Agence de financement des infrastructures de transport de France (l'AFITF).

L'open data n'est-elle pas pour vous une source d'inquiétude, voire de frustration ? Il vous faut en effet obligatoirement partager ces données avec d'autres acteurs nationaux et internationaux, qui, compte tenu de leur puissance financière, technologique et commerciale, exploitent la valeur ajoutée de votre patrimoine propre, ce trésor que vous détenez et dont vous devriez être les seuls à tirer les bénéfices pour les usagers publics comme privés. Comment vivez-vous cette situation ? Le législateur ne devrait-il pas réexaminer les règles du jeu ?

Nous nous heurtons à la question du recrutement chaque fois que le secteur public - secteur de souveraineté par définition - est confronté au marché de l'emploi, qui est souvent international, notamment dans le domaine de la recherche. Le civisme et la passion du service public et de l'action collective sont-ils un ressort suffisant et durable pour les jeunes chercheurs ?

Mme Martine Filleul. - Vous avez souligné la fragilisation de la récolte des données, puisque l'IGN doit désormais travailler avec d'autres acteurs pour collecter les données, par exemple les collectivités territoriales et les citoyens. Comment organisez-vous la protection de l'ensemble et l'agrégation des données au regard de la multiplicité des sources ?

M. Franck Montaugé, président. - Vous avez évoqué votre activité dans le domaine de l'agriculture et de la PAC. Ces données ont une importance que l'on pourrait qualifier de souveraine pour notre pays. Comment sont-elles stockées et protégées ? Sont-elles diffusées dans le monde entier ? Comment faites-vous pour que notre pays en conserve la maîtrise ?

M. Gérard Longuet, rapporteur. - Cela m'amène à prolonger ma question : que vous inspirent certains partenariats avec les Gafam d'autres ministères en charge de missions de service public ? Trouvez-vous cela acceptable ?

M. Daniel Bursaux. - La tendance à l'open data n'est pas nouvelle. Elle a été initiée par le précédent Gouvernement et reprise par l'actuel. La consigne que j'ai reçue est de mettre en open data l'ensemble des données produites par l'IGN seul d'ici au 1er janvier 2022, avec une licence de réutilisation totalement gratuite. Or la vente de données brutes générait des recettes d'une dizaine de millions d'euros - plutôt cinq millions d'euros ces dernières années. Il y a donc un problème de modèle économique. Comme dirigeant de l'établissement, je suis là pour appliquer les consignes - et il est assez logique de mettre en open data les données que nous produisons. Du coup, nous nous orientons vers la production de données extrêmement spécifiques pour les ministères. Cela modifie notre modèle économique : on ne produit plus de la donnée pour la vendre mais on construit des partenariats avec les ministères et les établissements publics, qui nous permettent d'obtenir des ressources pour pouvoir produire ces données très spécifiques. En matière agricole, par exemple, les données du référentiel parcellaire sont en open data. Chacun peut consulter les îlots agricoles du pays, que nous avons redéfinis et repositionnés. Les grands opérateurs que vous avez cités nous achetaient nos données, ce qui constituait une partie de nos recettes. Il y a donc un vrai sujet, politique. Bien sûr, dès lors qu'ils seront taxés, la question sera différente.

M. Gérard Longuet, rapporteur. - Si en plus ils ne payaient pas d'impôts...

M. Daniel Bursaux. - Je ne porte pas de jugement sur les décisions du Gouvernement. Nous mettrons à disposition gratuitement nos données génériques. Quand nous travaillons pour la direction de la sécurité routière ou pour le ministère de l'agriculture, ou encore quand nous travaillons sur la base de données pour les cours d'eau de l'Agence française pour la biodiversité (AFB), il y a une compensation au fait que nos données soient mises à disposition gratuitement. Ce sont les intérêts des ministères qui commandent au degré de publicité qu'ils veulent donner.

M. Franck Montaugé, président. - En somme, vous retrouvez les recettes que vous avez perdues par l'intermédiaire des partenariats ou des contrats passés avec les ministères.

M. Daniel Bursaux. - Oui, en travaillant sur des commandes ministérielles pour des données extrêmement spécifiques, que les ministères sont prêts à payer. Les données que nous produisons pour le ministère des Armées ne sont pas en open data, et font l'objet d'un contrat d'environ 30 millions d'euros par an, dont la moitié nous revient. Nous continuerons à produire des données gratuites, bien sûr, puisque nous touchons une subvention de service public. Mais notre modèle économique évolue vers des données fabriquées à façon.

M. Franck Montaugé, président. - Peut-on aller à jusqu'à penser que ce nouveau modèle économique coûtera plus cher au contribuable ?

M. Daniel Bursaux. - C'est équivalent. Mais nos données serviront davantage en appui direct aux politiques publiques. Notre production s'oriente vers une plus grande satisfaction des besoins des ministères, des collectivités ou des établissements publics. Jusqu'à présent, elle était plutôt définie par l'IGN elle-même... Les ministères nous disent ce dont ils ont besoin, nous fournissent un cahier des charges, et nous répondons à cette commande.

M. Sylvain Latarget, directeur général adjoint de l'IGN. - Il ne faut pas s'en tenir au périmètre strict de l'établissement. Si nous définissons avec un ministère ou un établissement public un jeu de données dont il a besoin, cela peut coûter un peu plus cher sur le périmètre de l'établissement, mais celui-ci va faire des économies dans son fonctionnement. Investir dans les données numériques, souveraines ou non, est souvent bénéfique. Globalement, cela ne va donc pas coûter plus cher.

M. Franck Montaugé, président. - Cette politique publique de la donnée géographique, nous ne sommes pas encore en mesure de l'évaluer. Pourtant, toute politique publique devrait faire l'objet d'une évaluation.

M. Daniel Bursaux. - Nous avons un marché avec le ministère des Armées, et je peux vous dire qu'ils regardent de près la qualité de l'exécution ! Pour l'agriculture, il y avait en 2014 la menace d'une amende de la Commission européenne de plus d'un milliard d'euros. Notre travail pour justifier le versement des aides a permis à la France d'économiser une bonne partie de cette somme. Avec le ministère de la transition écologique, nous travaillons sur la prévention des risques, nous faisons des levées pour délimiter les cours d'eau et faire des schémas de prévisions de crue. Cela permet au ministère d'affiner ses modèles.

M. Gérard Longuet, rapporteur. - Je suppose que vous êtes aussi prestataire de service pour le ministère de l'environnement.

M. Daniel Bursaux. - Oui, et pour celui des transports.

M. Gérard Longuet, rapporteur. - Achetez-vous des informations sur Spot Image ?

M. Daniel Bursaux. - Nous avons deux modes privilégiés d'acquisition des données de base. D'abord, le mode aéroporté. L'IGN dispose de quatre avions, qui couvrent à peu près l'ensemble du territoire tous les trois ans, et prennent des orthophotos, qui sont des images à haute résolution : environ 20 à 25 centimètres, et jusqu'à 5 centimètres s'il y a une commande précise, qui nous permette de le financer.

M. Gérard Longuet, rapporteur. - Vous avez votre propre outil.

M. Daniel Bursaux. - C'est historique.

M. Gérard Longuet, rapporteur. - Je me rappelle en effet que, quand j'étais étudiant, vous aviez des avions Hurel-Dubois à ailes longues,

qui survolaient la France pour photographier le nombre de vaches dans les champs, après les rationnements de la guerre. À présent, ce sont des Beechcraft.

M. Daniel Bursaux. - Ces photos nous permettent de faire directement le travail pour la politique agricole.

M. Gérard Longuet, rapporteur. - Parcelle par parcelle.

M. Daniel Bursaux. - Ilot par îlot. C'est notre moyen d'acquisition historique, qui permet de tomber à des niveaux de précision très forts. Nous utilisons aussi l'image satellitaire.

M. Gérard Longuet, rapporteur. - Là, vous êtes client.

M. Daniel Bursaux. - Oui. Nous utilisons notamment l'image satellitaire pour nos travaux à l'étranger, pour le ministère des Armées. Nous ne sommes d'ailleurs pas directement clients, puisque c'est le ministère qui nous fournit des images à partir desquelles nous travaillons.

M. Gérard Longuet, rapporteur. - Quand vos avions volent, à partir de quel moment la donnée est-elle ouverte ?

M. Daniel Bursaux. - Nos orthophotos ont vocation à être ouvertes d'ici 2022. Plus de la moitié le sont déjà.

M. Gérard Longuet, rapporteur. - C'est du mécénat...

M. Daniel Bursaux. - Pour l'instant, les avions sont le seul outil disponible pour le niveau de résolution dont nous avons besoin.

M. Gérard Longuet, rapporteur. - Et les drones ?

M. Daniel Bursaux. - Ils sont utiles pour photographier des ouvrages linéaires, ou localisés. Mais pour travailler dans un système complètement référencé, c'est plus compliqué. Le satellite a une moins grande résolution : il vole plus haut et les caméras ne sont pas aussi précises - sans parler des nuages. Pour autant, je n'exclus pas que, dans quelques années, avec le progrès des optiques et des satellites, l'image satellitaire finisse par nous permettre de mener quasiment les mêmes travaux. D'ailleurs, il nous est demandé de réfléchir à l'usage de l'image satellitaire pour recaler la politique agricole.

M. Franck Montaugé, président. - En matière agricole, travaillez-vous avec l'Institut national de la recherche agronomique (INRA) ?

M. Daniel Bursaux. - Sur le référentiel, nous travaillons directement avec le ministère de l'Agriculture. Nous travaillons avec l'INRA sur les forêts.

M. Franck Montaugé, président. - Le processus engagé va-t-il simplifier les démarches PAC de déclaration, de suivi et de contrôle ?

M. Daniel Bursaux. - Oui, c'est le but. Nos travaux sont envoyés par l'ASP aux agriculteurs, qui peuvent les corriger. Le travail est donc déjà préparé et simplifié et les contrôles pourront sans doute être plus ciblés à l'avenir.

M. Franck Montaugé, président. - Vous n'avez pas répondu à ma question sur la maîtrise du stockage des données.

M. Sylvain Latarget. - Sur la question de l'open data, plusieurs textes ont été pris, puis consolidés, qui amènent à présent le Gouvernement à décider de l'ouverture complète de nos données en 2022. Un certain nombre de jeux de données de référence ont été définis, qui ont vocation à être diffusées largement. Le référentiel parcellaire graphique en fait partie, tout comme un certain nombre de jeux de données que nous produisons, comme le référentiel à grande échelle, qui comprend les informations topographiques, altimétriques, ortho-photographiques, et les adresses. Il en va de même du plan cadastral informatisé tenu par la Direction générale des finances publiques (DGFIP). Ces données sont diffusées sur data.gouv.fr. Actuellement, nos données sont sous licence, et nous avons un système d'enregistrement et de diffusion. On peut acheter les données ou, si l'on bénéficie de la gratuité - c'est le cas de l'ensemble de de la sphère publique - se déclarer et obtenir un lien de téléchargement.

Nos données sont hébergées sur des serveurs et archivées. Nous rendons disponibles les données topographiques en J+1, c'est-à-dire dans l'état dans lequel la base était la veille. Elles sont archivées tous les trimestres et elles sont stockées en double, pour les reconstituer en cas de problèmes informatiques ou d'attaques malveillantes. L'ensemble est accessible par Internet, à travers l'écosystème du Géoportail, et peut être soit consulté, donc affiché à l'écran, ce qui est toujours possible quand les données ne sont pas confidentielles, soit utilisé en flux, en récupérant l'information dont on a besoin pour l'utiliser dans un système client, soit enfin téléchargé pour installation sur un site distant. Notre meilleure sécurité est que nos données sont recopiées en plusieurs endroits. Elles sont chez quasiment tous les clients qui les ont téléchargées, notamment.

M. Daniel Bursaux. - Nous sommes également en lien permanent avec l'Agence nationale de sécurité des systèmes d'information (ANSSI).

M. Sylvain Latarget. - Nous n'utilisons pas les data center des Gafam : nous sommes sur un cloud d'État, depuis le 1er janvier dernier. Il s'agit d'un site opéré par le ministère de l'Agriculture, qui s'appelle « Oshimae » (Offre de Service d'Hébergement Interministériel Agriculture Écologie). Auparavant, nous utilisions un hébergement privé.

M. Franck Montaugé, président. - Pourquoi ce changement ?

M. Daniel Bursaux. - Le ministère de l'Agriculture, qui souhaitait développer ce site, nous y a vivement encouragés, tout comme la DINSIC (direction interministérielle du numérique et du système d'information et de

communication de l'État). Pour nous, cela présente l'avantage de nous dispenser d'avoir à relancer un appel d'offre tous les six ans. Et être installé sur le réseau interministériel nous rend plus facilement accessibles aux ministères. Pour autant, il n'est pas évident pour le public internet de passer par le site du ministère. Et cela peut créer une surcharge.

M. Sylvain Latarget. - En 2018, par l'infrastructure Géoportail, nous avons diffusé un peu plus de 1000 téraoctets de données... Nous sommes le site gouvernemental qui consomme le plus de bande passante.

M. Gérard Longuet, rapporteur. - L'IGN est-il un EPIC ?

M. Daniel Bursaux. - C'est un EPA, ce qui nous oblige à recruter des fonctionnaires titulaires : nous ne pouvons avoir recours à des contractuels que si nous prouvons qu'il n'y a pas de fonctionnaire compétent pour les fonctions en jeu. Dans les domaines hyperspécialisés, nous avons des difficultés de recrutement : nous ne pouvons pas offrir à des informaticiens les mêmes salaires qu'Airbus... Or nous avons besoin de personnes très compétentes en matière d'intelligence artificielle et de deep learning.

M. Franck Montaugé, président. - N'avez-vous pas recours à la sous-traitance ?

M. Daniel Bursaux. - Si, et nous avons une collaboration avec le Centre d'études et d'expertise sur les risques, l'environnement, la mobilité et l'aménagement (Cerema). Le maintien de la capacité technique est un vrai sujet pour nous.

M. Gérard Longuet, rapporteur. - Avez-vous des exemples d'applications privées issues d'une utilisation judicieuse de vos données ? Les cartes Michelin, peut-être ?

M. Daniel Bursaux. - Michelin a ses propres systèmes de collecte et de cartographie. L'IGN n'est plus seulement le producteur de cartes routières et de randonnée - même si c'est toujours une activité significative, notamment pour les cartes de randonnée, dont nous avons la quasi-exclusivité et dont le marché se maintient bien. Nous avons complètement abandonné la production de cartes urbaines, et la production de cartes routières est également en chute libre.

Nous avons créé il y a quelques années une sorte d'incubateur d'entreprises, hébergeant sur appel à projets des TPE nous ayant présenté des idées qui nous paraissaient intéressantes. L'une d'entre elles s'occupe de cartographie solaire : elle indique l`intérêt à installer du chauffage solaire sur telle ou telle toiture. Elle a pris son autonomie et fait de la cartographie solaire à Nantes et Saint-Mandé. Elle s'appelle In Sun We Trust.

M. Claude Pénicand, délégué à la stratégie de l'IGN. - Cette entreprise s'est placée sur le créneau de l'installation des panneaux solaires en se positionnant sur un critère de confiance, les usagers privés n'ayant pas toujours obtenu les rendements escomptés. Elle ne propose pas d'installation

en propre, mais est en lien avec des installateurs. Elle indique à quel coût l'investissement en panneaux solaires sera rentable ou non. Elle mobilise pour cela des données de précision, que l'IGN lui apporte. Comme notre nom figure sur les simulations, cela inspire confiance au consommateur.

Dans le domaine forestier, une application identifie dans nos données les endroits où la prospection forestière serait la plus intéressante, et propose aux particuliers de mettre à disposition leurs forêts, en se chargeant de trouver un exploitant pour valoriser leurs ressources forestières.

Une société, enfin, travaille sur les risques d'inondations, notamment pour le ministère. Nous avons travaillé avec elle sur les modèles de prévision à partir de modèles numériques de terrain.

M. Franck Montaugé, président. - Intervenez-vous pour Galiléo ?

M. Sylvain Latarget. - Galiléo ne fait pas d'images, il émet des signaux pour faire des calculs de position. Nous avions été associés à sa conception, et participons aujourd'hui au calcul des orbites précises des satellites, ce qui permet, en en temps légèrement différé, des mesures extrêmement fines. Une précision d'un mètre est facile à obtenir pour un GPS. Mais pour un positionnement plus précis, il faut un calcul en temps différé intégrant l'orbite exacte du positionnement du satellite - que nous fournissons gracieusement. Le véhicule autonome, notamment, aura besoin de mieux qu'un mètre de précision pour se positionner. Nous travaillons à un système de PPP (positionnement ponctuel précis) qui permettra, à partir de la position instantanée - à quelques décimètres près - et de la connaissance - quelques minutes voire quelques secondes avant - du positionnement précis, d'interpoler la position où devrait être à peu près le satellite pour obtenir une précision d'une dizaine de centimètres - afin que deux véhicules n'entrent pas en collision !

Nous intervenons comme experts techniques sur les modèles mathématiques, sur les systèmes de référence, sur les processus de calcul et sur le positionnement des points, y compris pour les géomètres. Le réseau ancien de bornes a été complètement dématérialisé et remplacé par des stations qui sont pour certaines opérées par nous mais, pour la grande majorité, sont opérées par des tiers, intégrés dans un réseau global national, ce qui nous permet d'offrir des prestations de qualité et entièrement gratuites.

M. Daniel Bursaux. - L'intégration de données non produites par l'IGN est un vrai changement de pratique, qui est en cours. Nous avons des tiers de confiance : quand une grande métropole ou une région produit des données, nous n'avons pas de raison de penser qu'elles sont de moins bonne qualité que celle de l'IGN. La question est dès lors de voir comment intégrer ces données dans nos bases, et comment vérifier qu'elles correspondent à nos spécifications. Pour les adresses, par exemple, nous avons mis en place un

guichet sur lequel les mairies peuvent procéder directement à des mises à jour : nous n'avons pas de raison de penser qu'elles le font moins bien qu'un agent de l'IGN. La mutualisation, avec des tiers de confiance, évite que la saisie des données soit faite deux ou trois fois. Nous réfléchissons aussi à intégrer des citoyens dans le processus.

M. Franck Montaugé, président. - Merci.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible en ligne sur le site du Sénat.

Audition de Mme Marie-Laure Denis, présidente de la CNIL, de MM. Gwendal Le Grand, secrétaire général adjoint, et Mathias Moulin, Directeur de la Direction de la protection des droits et des sanctions, le 10 juillet 2019

M. Franck Montaugé, président. - Mes chers collègues, notre commission d'enquête poursuit ses travaux avec l'audition de Madame Marie-Laure Denis, présidente de la Commission Nationale de l'Informatique et des Libertés (CNIL). Elle est accompagnée par Messieurs Gwendal Le Grand, secrétaire général adjoint, et Mathias Moulin, Directeur de la Direction de la protection des droits et des sanctions.

Cette audition sera diffusée en direct sur le site internet du Sénat. Elle fera également l'objet d'un compte rendu publié.

Un faux témoignage devant notre commission d'enquête serait passible des peines prévues aux articles 434-13, 434-14 et 434-15 du Code pénal. Je vous invite chacun à tour de rôle à prêter serment de dire toute la vérité, rien que la vérité ; levez la main droite et dites : « je le jure ».

Conformément à la procédure applicable aux commissions d'enquête, Mme Marie-Laure Denis, M. Gwendal Le Grand, et M. Mathias Moulin prêtent successivement serment.

M. Franck Montaugé, président. -.Mes chers collègues, à titre liminaire je souhaite vous rappeler que la CNIL est une autorité administrative indépendante dotée de pouvoirs d'enquête et de sanction. À ce titre, nous aurons bien sûr plusieurs questions importantes à poser à Madame Denis et à ses collaborateurs. Néanmoins, il va de soi qu'aucune de nos questions ne devra les amener à révéler les cibles précises de futures enquêtes de la CNIL ou à fragiliser des enquêtes en cours en révélant des éléments qui porteraient atteinte à l'équité et à l'intégrité de ces procédures.

Madame Denis, vous avez été nommée il y a six mois présidente de la CNIL. Cette autorité administrative indépendante bien connue est en charge, depuis 1978, de la protection des données à caractère personnel. Son champ de compétences est devenu particulièrement vaste en 40 ans, tant les traitements automatisés de données sont courants aujourd'hui. De véritables géants du numérique ont émergé ; par ailleurs, les GAFAM, les plateformes et les usages se sont complexifiés algorithmes, du profilage, du big data, de l'intelligence artificielle, etc.

Le cadre juridique dans lequel le régulateur exerce ses missions a lui aussi profondément évolué avec, en dernier lieu, l'entrée en vigueur le 25 mai 2018 du Règlement Général sur la Protection des Données (RGPD).

Pourriez-vous commencer par nous présenter le cadre général de votre action, vos moyens et les défis que pose cette régulation. Le RGPD a justement été pensé dès l'origine comme un outil de régulation à la hauteur des enjeux de souveraineté numérique, quel bilan dressez-vous de sa première année d'application ?

Mme Marie-Laure Denis, présidente de la CNIL. -. Nous sommes reconnaissants au Sénat d'associer la CNIL à ses travaux sur ce sujet éminemment important. Le foisonnement des innovations a envahi l'ensemble des espaces de la vie quotidienne et publique, mais aussi de la vie privée. Les systèmes d'échanges instantanés bousculent les frontières de ces différents domaines en raison de la vitesse à laquelle circulent les informations.

Dans ce contexte, la souveraineté doit être repensée pour deux raisons.

Tout d'abord, la capacité des États à faire appliquer leurs règles est remise en cause, celles-ci étant plus difficile à ancrer que dans des territoires physiques ; le monde numérique dessine ainsi un vaste territoire au sein duquel les données constituent un élément essentiel par leur collecte, leur croisement, leur enrichissement, leur transfert et leur valorisation. Si certains comparent souvent les données au pétrole de l'économie numérique, je préfère pour ma part utiliser l'image du terreau, plus représentative de leur rôle.

Ensuite, le monde numérique fait interagir plusieurs acteurs qui se comportent différemment des modèles classiques. En nous offrant diverses solutions technologiques, ils ont acquis une puissance inédite sur le plan économique. Cette situation pourrait nous conduire à subir des choix d'organisation sociale, imposés par ces acteurs à notre insu et en dehors de tout cadre démocratique.

L'État, dans toutes ces facettes - expert, stratège, législateur - se trouve donc confronté à plusieurs défis majeurs. L'intervention de la puissance publique doit être repensée autour de leviers forts. Bien que les autorités nationales et européennes disposent de pouvoirs étendus dans le secteur du droit de la concurrence, d'autres cadres doivent être posés dans les domaines de la fiscalité, du droit d'auteur et de la régulation des contenus. Pour ma part, j'aimerais qu'un aspect soit davantage exploré par le législateur, celui de la démultiplication de l'exposition de soi.

Vous m'avez interrogée au sujet du bilan de la CNIL à la suite de l'entrée en vigueur du RGPD. Nous constatons que l'ensemble des publics et des secteurs économiques est concerné par la tendance à vouloir s'approprier ses droits. Ainsi, nous avons relevé plus de huit millions de visiteurs sur notre site internet. Près de 17 000 requêtes électroniques ont été reçues. Notre rubrique questions - réponses a été consultée presque 300 000 fois. Nous avons reçu 200 000 appels téléphoniques.

L'ampleur de ces chiffres démontre à quel point les citoyens recherchent l'information au sujet de leurs droits. Cette tendance va de pair avec la volonté de mieux défendre ses droits en maîtrisant l'utilisation de ses données personnelles. Le nombre de plaintes entre le 25 mai 2018, date de l'entrée en vigueur du RGPD, et le 25 mai 2019, s'élève à 12 500, ce qui dénote une hausse de 42 % par rapport à l'année précédente. Un tiers d'entre elles concerne la diffusion des données personnelles sur internet. Notre bilan au sujet des données personnelles est un enjeu de la souveraineté numérique. La CNIL se doit donc d'être en capacité de répondre aux attentes des citoyens.

Nous partageons généralement bien volontiers nos données privées sur les réseaux sociaux ou les blogs. Or, énormément de personnes s'émeuvent de ce que leurs données soient mises en ligne à leur insu. À l'heure actuelle, les données personnelles dont certaines touchent aux aspects les plus intimes de l'individu, circulent dans des proportions inédites. Le numérique a changé les usages, les pratiques, mais aussi les risques et les enjeux présents dans l'ensemble de la société.

Pour conserver notre souveraineté numérique, nous devons garder comme objectif la préservation de notre autonomie décisionnelle sur le traitement de nos données personnelles, c'est un principe cardinal du RGPD. Outre cet aspect individuel, la protection des données a évidemment une dimension collective : il s'agit de protéger notre contrat social et de défendre notre modèle humaniste et notre conception des droits et libertés.

Le RGPD a instauré un cadre juridique ambitieux et puissant. Il a vocation à s'appliquer à un marché économique de plus de 500 millions de personnes auquel les acteurs du numérique s'intéressent en tant que tel. Il repose sur un cadre juridique novateur qui prévoit, grande nouveauté, une application extraterritoriale même à l'égard des entreprises qui ne disposent pas d'un établissement en Europe dès lors que ce sont les données personnelles d'un Européen qui sont ciblées. L'ensemble du système utilise la notion de risque : les responsabilités varient en fonction du risque représenté par le traitement - volume, sensibilité des données - et les grands acteurs sont donc appelés à être soumis à des obligations particulières.

Le montant des sanctions pécuniaires change d'échelle avec le RGPD : une condamnation peut aller jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires mondial annuel. De plus, elle peut être rendue publique, comme l'a fait la CNIL en janvier dernier contre Google, pour un montant de 50 millions d'euros. Les plaintes engagées en vertu du RGPD peuvent désormais être collectives et c'est sur cette base que la société civile a engagé quelques actions à l'encontre des GAFA.

Un droit nouveau à la portabilité des données est consacré par le RGPD il doit permettre aux petits acteurs économiques de défier plus facilement les grands, en attirant les clients qui peuvent ainsi leur apporter

leurs données, diminuant ainsi le pouvoir de captation des grandes plateformes. À l'occasion hier, d'un colloque organisé à Bruxelles sur la régulation numérique auquel participait le président de l'autorité de la concurrence allemande, j'ai été frappée de constater que le droit à la portabilité des données était évoqué comme un levier d'action essentiel.

En outre, le RGPD a introduit un nouveau modèle de gouvernance de la régulation, jusqu'alors inédit au niveau européen : intégré et décentralisé Ainsi, si un traitement de données concerne des individus dans plusieurs États membres, chaque autorité doit agir de concert avec les autres - c'est un mécanisme de guichet unique - pour adopter une décision applicable dans l'ensemble de l'Union européenne. Pour permettre cette coopération, un nouvel organe européen de régulation a notamment été créé, le Comité Européen de Protection des Données (CEPD).

Par ses lignes directrices, le CEPD garantit la cohérence et assure la pédagogie des principes du droit européen de la protection des données. Le CEPD adopte des décisions structurantes visant à répartir les rôles entre les différentes autorités : il distribue ainsi les rôles dans l'instruction des plaintes de dimension transnationale, et c'est lui qui peut être amené à déterminer quelle autorité sera la chef de file pour une action donnée. Le système mis en place repose donc sur les deux principes essentiels que sont la coopération et la cohérence, permettant de combattre toute volonté d'évitement ou de « forum shopping ».

Bien que le RGPD soit rentré en vigueur il y a plus d'un an, il reste très présent dans les agendas politiques et médiatiques. Au sein de l'Union européenne et au-delà, cette tendance est assez inédite. Le RGPD a su rayonner au niveau mondial en proposant une approche nouvelle. D'autres standards sont à l'oeuvre au niveau mondial, ne l'oublions pas, et une véritable diplomatie de la protection des données mérite d'être engagée pour défendre ces valeurs. Certains États ont mis à jour leurs législations pour se rapprocher de nos standards, comme le Japon, la Corée du Sud, le Bénin, l'Australie. On peut également citer les processus en cours en Tunisie, en Suisse ou le Burkina Faso. D'autres ont adopté, pour la première fois, un cadre comparable au RGPD comme la Californie - dont la loi doit entrer en vigueur en janvier prochain et nourrit même des réflexions pour un texte de portée fédérale ou le Brésil, qui a adopté une telle loi en 2019. Les outils de transfert prévu par le RGPD - et en particulier les décisions d'adéquation par lesquelles la Commission peut les autoriser vers des pays tiers - ont contribué à une élévation internationale générale des standards de protection de la vie privée.

J'insiste : l'Europe ne s'est pas enfermée dans une forteresse avec le RGPD, cadre juridique ouvert qui continue bien sûr à permettre la libre circulation des données. J'ai d'ailleurs été frappée de voir que le G20 organisé à Osaka consacrait un paragraphe entier à la protection des données

et au principe du « data free flow with trust », la libre circulation dans la confiance.

Il est important de défendre nos outils de régulation et nos standards en parallèle aux négociations commerciales internationales - ; la protection des données ne saurait être intégrée au sein des accords commerciaux conclus par l'Union européenne, un consensus existe sur ce point.

L'application effective du nouveau cadre européen de protection des données permettra également de renforcer notre résilience et notre cybersécurité en Europe, et donc d'affronter les dérives liées aux stratégies de désinformation - qui reposent sur l'exploitation des données et le ciblage des individus - ainsi qu'aux menaces portées contre l'intégrité de nos processus électoraux. Dans ce contexte, le RGPD n'apporte qu'une partie des réponses. Toutefois, c'est du succès de son application que dépendra la réussite de ces enjeux.

Il est également question de souveraineté numérique avec l'accès transfrontalier aux données dans le cadre d'enquête de police ou de procédures judiciaires. Nous discutons ainsi en ce moment avec nos homologues de l'impact du Cloud Act. Cette loi américaine adoptée récemment permet aux autorités américaines un accès direct, en dehors des accords de coopération judiciaire, aux données stockées en dehors des États-Unis, et donc y compris en Europe. La commission européenne a présenté une proposition de règlement en matière d'accès aux preuves électroniques actuellement en discussion. Nous devons certes être en mesure d'apporter des réponses concrètes à des problématiques juridiques pour garantir une certaine efficacité aux enquêtes, mais pas au détriment de la protection de la vie privée des individus.

Pour conclure, je tiens à rappeler que la CNIL a vocation à contribuer à une stratégie globale visant à assurer la souveraineté numérique tant au plan national qu'européen. Tout en restant dans le cadre de ses prérogatives réglementaires, elle se tient à la disposition des pouvoirs publics et des citoyens pour atteindre cet objectif. Pour autant, je ne peux que constater à quel point les ressources dont dispose la CNIL sont inadaptées au regard de l'ampleur des enjeux qui se dressent face à elle.

M. Gérard Longuet, rapporteur. - Je vous remercie, et je tiens tout d'abord à saluer l'ensemble de votre équipe et à souligner la qualité du travail accompli au sein de la CNIL. Cette autorité administrative a su s'imposer au fil des années comme un acteur essentiel.

Vous avez évoqué un manque de ressources. Quelles sont vos attentes en la matière ?

Mme Marie-Laure Denis. - La CNIL rassemble 200 agents. Nous serons 215 en fin d'année, ce qui démontre que les pouvoirs publics sont conscients de la nécessité de renforcer les moyens humains. Pour autant,

nous sommes largement en deçà des ressources dont disposent nos homologues européens. Eu égard au nombre d'habitants, nous avons le troisième plus mauvais ratio citoyens/agents de l'Union européenne.

La Grande-Bretagne, qui a une population et un périmètre de régulation comparables, disposera de 900 agents en 2020. Alors que nous avons 20 contrôleurs, la Grande-Bretagne en a 160. Les Britanniques disposent ainsi d'une force de frappe bien plus importante que la nôtre lorsqu'elle est confrontée à une affaire complexe.

De notre côté, nos faibles moyens ne nous permettent pas d'assurer de manière satisfaisante les nouvelles missions confiées par le RGPD. Par exemple, alors même qu'il s'agit d'un enjeu important de cybersécurité, nous recevons sept notifications de failles ou de violations de données par jour - sans pour autant disposer de moyens supplémentaires pour prendre en charge cette nouvelle compétence.

Nous avons démontré notre volonté constante d'accompagner les pouvoirs publics. À ce titre, nous avons rendu 120 avis l'an dernier sur des projets de lois ou décrets et nous avons été auditionnés 30 fois au Parlement. L'accompagnement des entreprises suppose des conseils et des approches spécifiques. Notre présence au niveau européen est essentielle pour porter les valeurs et les points de vue défendus par la France au sein des organes de coopération ou de négociation... Toutes ces missions impliquent de disposer de moyens.

M. Gérard Longuet, rapporteur. - Et par rapport à l'Allemagne ?

Mme Marie-Laure Denis. -L'Allemagne dispose de 700 agents, 250 pour l'autorité fédérale, pour une population de 82 millions d'habitants ; En Pologne, c'est 250 agents pour 37 millions d'habitants soit près de 20 % de plus que la CNIL ! Aux Pays-Bas, 138 agents pour 17 millions d'habitants...

Selon moi, le problème n'est pas le budget, mais bien l'effectif dont dispose la CNIL pour faire face à ses missions, d'autant plus que nous nous devons d'assurer un rôle de pédagogie sur ces sujets auprès du grand public. Il est notamment nécessaire d'envoyer les agents de la CNIL sur le terrain pour faire de l'éducation au numérique, dans les écoles ou les entreprises. Pour mener à bien toutes ces actions, un effectif adapté s'impose.

M. Gérard Longuet, rapporteur. - Vous avez évoqué vos contacts avec les différents acteurs du terrain. Comment les entreprises réagissent-elles face aux obligations découlant du RGPD ? Il me semble que la situation est assez paradoxale : les acteurs les plus puissants sont sans doute les mieux équipés pour répondre à ces obligations. À l'inverse, ceux pour lesquels l'espace numérique est une nouveauté semblent plus en difficulté pour s'adapter à ce cadre.

Comment ressentez-vous les efforts réalisés par les professionnels suite à l'entrée en vigueur du RGPD ? Les organisations professionnelles vous interrogent-elles à ce sujet ?

Par ailleurs, nous avons tous pris l'habitude de cliquer sur « j'accepte » pour la collecte de nos données. Avez-vous des retours d'usagers sur l'évolution des conditions d'octroi du consentement ? N'assistons-nous pas à une forme de standardisation des comportements ?

Mme Marie-Laure Denis. - Notre mission consistant à la fois à accompagner et à sanctionner le cas échéant, cela peut compliquer quelque peu nos rapports avec les entreprises. Celles-ci doivent fournir, c'est vrai, des efforts importants de gouvernance à la suite du RGPD, tant les enjeux juridiques, informatiques, stratégiques voire de réputation sont importants désormais. Pour autant, vous l'avez rappelé, la CNIL a 41 ans. La loi Informatique et Libertés de 1978 portait depuis l'origine des obligations comparables à celles issues du RGPD. Ce règlement n'a donc fait que renforcer ces obligations déjà à la charge des entreprises.

Dans ce cadre nouveau, la CNIL accompagne les entreprises. À cette fin, nous avons mis en place un logiciel en open source, téléchargeable sur notre site. À ce jour, il a été téléchargé 300 000 fois. Initialement disponible dans seulement deux langues, il est actuellement proposé dans dix-neuf langues différentes.

De même, seules les grandes entreprises sont concernées par l'obligation de nommer un délégué à la protection des données. Pour accompagner ce nouveau rôle, nous avons mis en ligne un MOOC (massive open on line courses, c'est-à-dire un cours gratuit en ligne) qui permet de cadrer les missions inhérentes à cette nouvelle fonction.

Notre approche à l'égard des petites entreprises est différente. En effet, nous leur demandons simplement de respecter des obligations de bon sens - registre des traitements, règles de sécurité informatique, etc. Nous avons élaboré un guide à destination des TPE et des PME, et préparons le même type outil pour les collectivités territoriales.

En somme, les retours sont différents en fonction de la taille des entreprises. Dans tous les cas, nous ne devons pas surestimer les coûts induits par le RGPD. Ils sont liés à l'échelle des entreprises.

M. Franck Montaugé. - Si je comprends bien, certaines entreprises n'ont pas du tout été affectées par la mise en place du RGPD.

Mme Marie-Laure Denis. - Je ne voudrais pas minimiser l'impact de cette réglementation parfois perçue comme nouvelle. Pour autant, nous mettons en oeuvre tous les moyens nécessaires afin d'accompagner les entreprises. Bien sûr, nous ne pouvons pas mener un suivi individuel, mais notre site internet regroupe toutes les informations utiles pour se mettre en conformité avec le RGPD.

Concernant les règles de recueil du consentement sur les sites internet, le clic de l'internaute visant à accepter la collecte de ses données doit être relié à la notion de « cookie »s. Ces traceurs ont pour objectif de cibler au mieux l'individu principalement au niveau publicitaire. Le collège de la CNIL a pris ce sujet bras le corps : nous avons décidé de mener un cycle d'auditions au sein de la CNIL avec consultation de l'ensemble des instances professionnelles et des acteurs de la société civile pour rappeler l'état du droit positif en matière de traceurs et élaborer des recommandations claires au sujet des modalités de recueil du consentement de l'internaute. Ce que nous appelons la « fatigue du consentement » est en effet un véritable sujet de réflexion.

M. Gérard Longuet, rapporteur. - La CNIL s'est notamment illustrée par la sanction spectaculaire infligée à Google. Pouvez-vous évoquer cette affaire ?

Mme Marie-Laure Denis. - Cette affaire a été traitée avant que je ne prenne mes fonctions. Elle concernait le sujet spécifique de la création de comptes sur Android. La CNIL, dans sa formation restreinte, à laquelle n'appartient pas la Présidente, a décidé d'une sanction de 50 millions d'euros aux motifs du défaut d'information de l'utilisateur. En effet, pour parvenir à obtenir les informations concernant la collecte et le traitement des données, il fallait effectuer six opérations préalables, ce qui est excessif. Je précise que Google conteste cette sanction, l'entreprise - qui a payé l'amende - a par la suite décidé de déposer un recours encore pendant devant le Conseil d'État.

M. Mathias Moulin, Directeur de la Direction de la protection des droits et des sanctions. -S'agissant du cadre de la sanction infligée à Google, je tiens à préciser qu'elle a été décidée en application du RGPD mais en dehors de la procédure dite du « guichet unique », puisque Google ne disposait pas d'établissement dans l'Union européenne à l'époque de l'action -l'établissement en Irlande n'ayant pas, selon la formation restreinte, de pouvoir d'action sur les traitements de données personnelles. Cette question de compétence a fait l'objet de nombreuses discussions et c'est d'ailleurs l'un des arguments portés par Google dans le cadre de son recours auprès du Conseil d'État.

Nos enquêtes se sont concentrées sur les conditions générales d'utilisation et la politique de confidentialité et nous avons considéré que le consentement ne pouvait pas être valablement recueilli dans ce contexte. Les personnes étaient également insuffisamment ou mal informées, notamment sur les durées de conservation, par conséquent leur consentement n'était pas éclairé.

Au vu de l'ampleur des données traitées, plusieurs millions par minute, l'enjeu en matière de vie privée est essentiel. De ce fait, la formation restreinte de la CNIL s'est prononcée en faveur d'une sanction de 50 millions d'euros, rendue publique.

Je précise que nous avions été saisis par des plaintes collectives portées par les associations La Quadrature du Net, qui rassemblait les réclamations de plus de 10 000 personnes, et None Of Your Business, associations créée par Max Schrems.

Mme Marie-Laure Denis. - A ce jour, nous sommes saisis de sept plaintes collectives sur le fondement du RGPD depuis son entrée en vigueur.

M. Mathias Moulin. -Cette procédure permet de démultiplier notre action.

M. Gérard Longuet, rapporteur. - Madame Denis, vous êtes une juriste éminente et expérimentée. A ce titre, comment appréhendez-vous la coexistence entre le Cloud Act et du RGPD ? Quid du rapport Gauvain ? Pensez-vous qu'il soit possible d'interdire aux entreprises françaises de transmettre des données aux autorités américaines ? Il s'agirait d'une attitude de résistance difficile à tenir...

Le RGPD adopte une approche plus subtile en utilisant le critère de la nationalité de la personne ciblée par l'atteinte à ses données.

Mme Marie-Laure Denis. - L'articulation entre ces différentes dispositions est un sujet très intéressant. Il relève en réalité d'un conflit de lois. Je rappelle que le Cloud Act découle d'une affaire pendante devant la Cour suprême qui avait opposé le gouvernement américain à Microsoft.

Le Cloud Act permet aux autorités américaines, dans le cadre d'une enquête judiciaire, d'exiger des hébergeurs une transmission des données stockées sans passer par les procédures classiques de coopération judiciaire. Les Américains estiment que ce principe accroît l'efficacité des procédures.

Toutefois, les dispositions issues du Cloud Act sont en contradiction directe avec l'article 48 du RGPD qui interdit toute transmission des données aux autorités d'un pays tiers sans un cadre juridique clair.

Le CEPD a adopté ce matin même une position à ce sujet : répondant à une demande d'avis de la commission libertés civiles et justice du Parlement européen, il a réaffirmé la pleine application de l'article 48 du RGPD qui protège les données personnelles contre les transferts ou divulgations non autorisées par le droit de l'Union. En l'absence de traité international, si une demande des autorités américaines visait à obtenir des entreprises européennes la transmission de données sur la base du Cloud Act, elle serait donc illicite au vu du RGPD. Les entreprises ne peuvent se prévaloir pour ce traitement du fondement tiré de l' « intérêt légitime », la seule exception envisageable étant celle destinée à prévenir la survenue d'une menace grave pour l'intérêt vital de la personne concernée.

Dans ce cadre, vous constatez que le RGPD fournit effectivement les moyens d'assurer notre protection - celle des personnes et les intérêts de nos entreprises.- et de préserver notre souveraineté numérique européenne.

La Commission européenne a reçu un mandat pour négocier un traité avec les États-Unis visant à apporter la garantie du respect des droits des personnes. J'ignore quelle sera la forme de ce traité. D'après ce que j'ai entendu, plusieurs hypothèses sont envisageables : peut-être un traité cadre et des accords spécifiques bilatéraux. Dans tous les cas, la position du CEPD est très claire à ce sujet, puisqu'il affirme nettement que l'article 48 du RGPD est pleinement applicable en l'espèce.

Le rapport Gauvain sur la protection des entreprises contre les sanctions américaines a été remis au Premier ministre le 26 juin 2019. Il traite davantage des données non personnelles, c'est-à-dire celles qui ne permettent pas d'identifier des personnes physiques. Il me semble que les sanctions proposées pourraient être appliquées par une autre autorité administrative indépendante que la CNIL. Je n'ai pas d'opinion personnelle à émettre sur ce sujet, si ce n'est que je me réjouis que le RGPD fasse des émules.

M. Franck Montaugé, président. - Le point soulevé par le rapporteur mérite d'être élargi. Les propositions envisagées par le rapport Gauvain pourraient-elles permettre de rétablir l'équilibre des forces dans le contexte du Cloud Act ? Les préconisations du rapport pourraient-elles nous faire gagner en souveraineté ?

De manière plus générale, quelles seraient vos propositions pour trouver des axes d'amélioration au sujet de la protection de nos libertés individuelles ?

Mme Marie-Laure Denis. - Cette initiative est intéressante car elle présente au moins le mérite de traiter un vrai sujet, celui des entreprises françaises confrontées à des législations étrangères. J'ai pu constater, lors de mes déplacements, à quel point les entreprises américaines étaient intéressées par l'affirmation européenne d'une législation extraterritoriale. Lorsque nous allons en Asie, nous ne pouvons qu'observer les modèles concurrents.

Le modèle américain repose avant tout sur la protection des consommateurs. En Europe, nous prenons le parti de protéger les individus en tant que tels, ne négligeons pas les stratégies d'influence.

Vous m'interrogez sur des modifications législatives souhaitables. Très modestement, il me semble qu'en matière de protection des données, la législation a évolué de manière substantielle récemment avec deux décrets, une réforme de la loi Informatique et Libertés et une ordonnance. Laissons le temps aux entreprises d'intégrer ces évolutions avant d'en envisager d'autres.

M. Gwendal Le Grand, secrétaire général adjoint. - La définition des données à caractère personnel retenue par le RGPD dans son article 4 est très large. Il s'agit de « toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une « personne physique

identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ». Son interprétation permet d'englober énormément d'informations détenues par les entreprises.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible en ligne sur le site du Sénat.

Audition de Mme Isabelle de Silva, présidente de l'Autorité de la concurrence, de M. Roch-Olivier Maistre, président du CSA et de M. Sébastien Soriano, président de l'Arcep,
le 10 juillet 2019

M. Franck Montaugé, président. - Mes chers collègues. Notre commission d'enquête consacrée à la souveraineté numérique poursuit ses travaux avec l'audition de Mme Isabelle de Silva, présidente de l'Autorité de la concurrence, M. Roch-Olivier Maistre, président du Conseil Supérieur de l'Audiovisuel (CSA) et M. Sébastien Soriano, président de l'Autorité de Régulation des Communications Électroniques et des Postes (Arcep).

Cette audition sera diffusée en direct sur le site internet du Sénat. Elle fera également l'objet d'un compte rendu publié.

Enfin, je rappelle qu'un faux témoignage devant notre commission d'enquête serait passible des peines prévues aux articles 434-13, 434-14 et 434-15 du Code pénal. Je vous invite chacun à tour de rôle à prêter serment de dire toute la vérité, rien que la vérité ; levez la main droite et dites : « je le jure ».

Conformément à la procédure applicable aux commissions d'enquête, Mme Isabelle de Silva, M. Roch-Olivier Maistre et M. Sébastien Soriano prêtent serment.

M. Franck Montaugé, président. -Nous vous recevons en tant que présidents des autorités administratives indépendantes que vous représentez.

Mme de Silva, vous présidez l'Autorité de la concurrence, autorité transversale qui a la charge de s'assurer du bon fonctionnement de l'ensemble du marché français au regard des pratiques anticoncurrentielles et des concentrations. MM. Maistre et Soriano, vous présidez deux autorités de régulation dites sectorielles. Il s'agit pour M. Maistre du secteur audiovisuel que le CSA à la charge de superviser et pour Monsieur Soriano du secteur des télécoms et des postes avec l'Arcep.

Vos autorités sont toutes les trois confrontées aux géants du numérique et aux difficultés de réguler l'espace numérique. Si certaines questions vous sont propres, d'autres vous sont communes. C'est sur celles-ci que nous aimerions vous entendre dans un premier temps à la lumière de vos expériences respectives.

Estimez-vous que la régulation des acteurs du numérique est aujourd'hui suffisante en France ? Disposez-vous de moyens humains et techniques suffisants pour remplir vos missions dans le monde du numérique ? Faut-il créer un cadre général applicable aux acteurs

systémiques de l'internet et dont l'application serait assurée par un seul régulateur ?

Mme Isabelle de Silva, présidente de l'Autorité de la concurrence. -Nous vivons actuellement dans une période riche en défis pour l'ensemble des régulateurs. Il s'agit pour nous de la même révolution que traversent les entreprises. Face à cela, il me semble que nous disposons des moyens de réponse adaptés pour y faire face. Je me limiterai à évoquer les outils de la concurrence, qui se sont avérés très plastiques et efficaces.

Sur ce sujet, la France se situe à la pointe de ce qui existe. Malgré cela, il reste encore à renforcer ces outils dans le monde du numérique. En début d'année, nous avons pris des mesures conservatoires à l'encontre de Google dans le cadre de la problématique du déréférencement dont avait été victime une PME française. Cet outil s'avère très utile car il permet une intervention rapide pour mettre un terme à des pratiques nuisibles.

Un autre pan d'action important se retrouve au niveau européen. La Commission européenne mène une action très encourageante qui démontre sa volonté d'affirmer avec rigueur la force du droit de la concurrence. J'aimerais notamment évoquer trois affaires concernant Google dans lesquelles la Commission européenne est intervenue.

L'affaire Google Shopping a donné lieu à une sanction de 2,4 milliards d'euros. Dans sa décision, la Commission prend acte de la position dominante de Google dans le marché de la recherche en ligne. La sanction est liée à l'abus dans le changement intempestif des règles du jeu au niveau du volet Google Shopping. Cela rappelle à quel point une entreprise dominante est soumise à des obligations particulières du fait de cette position.

L'affaire Google Adsense s'est conclue par une sanction de 1,25 milliard d'euros en raison de clauses anticoncurrentielles relevées dans les contrats, ce qui aboutissait au maintien de la position dominante de Google dans le marché de la publicité associée à la recherche en ligne.

L'affaire Google Android a enfin débouché sur une sanction de 4,3 milliards d'euros. La Commission a répertorié l'ensemble des actions et clauses contractuelles qui visaient à préserver la position de Google sur les terminaux équipés du système d'exploitation Android.

L'application du droit de la concurrence est un outil qui doit encore être mobilisé. Face aux problématiques qui découlent de l'utilisation des données, notre interprétation de ce droit doit être plus innovante que par le passé. À cet égard, la décision prise par l'équivalent allemand de l'Autorité de la concurrence peut être citée. Elle a abouti à la condamnation de Facebook pour une utilisation disproportionnée des données des utilisateurs, qui excédait ce qui est nécessaire au bon fonctionnement du réseau social. La captation illégitime des données peut donc être sanctionnée, comme nous le démontre cette décision.

Il me semble nécessaire de renforcer les moyens de notre coopération, tant aux niveaux nationaux qu'à l'échelle européenne. Dans cette lutte, nous disposons d'un atout majeur avec le réseau européen de concurrence, lequel permet une action et un traitement coordonnés des affaires par les autorités nationales de régulation et la Commission européenne. La réussite de ces coopérations implique également d'approcher les affaires de manière convergente.

Parmi nos pistes d'amélioration, je citerai le manque de moyens humains pour nos investigations. Au sein de l'Autorité de la concurrence, nous sommes 400 personnes. Ce nombre est insuffisant pour traiter des dossiers éminemment complexes. En Allemagne, les moyens sont 50 % plus importants que les nôtres, et le Royaume-Uni dispose du double de personnes.

Les dossiers sont très délicats, mêlant des sujets d'ordre stratégique ou technique. Ils requièrent des compétences élevées de la part des rapporteurs. Je rappelle également que les entreprises impliquées disposent quant à elles de moyens colossaux et sont accompagnées par des conseils nombreux. Face à cette situation, l'État doit renforcer ses autorités de régulation, en leur octroyant plus de moyens humains et techniques.

Par ailleurs, je tiens à aborder les adaptations législatives récentes. Une directive adoptée en début d'année 2019 tend à renforcer les autorités nationales chargées du droit de la concurrence en leur donnant la possibilité d'utiliser des mesures conservatoires. Les régulateurs pourront décider de ce type de mesures sans même être saisis par une entreprise. Ils pourront ainsi agir sans attendre une saisine, qui parfois n'arrive jamais tant les victimes d'actes anticoncurrentiels craignent de l'engager.

Parmi les évolutions souhaitables, il faudrait renforcer de façon énergique le contrôle des concentrations. Pour que le marché reste concurrentiel, nous devons accroître notre niveau d'exigence actuel. Les acquisitions réalisées par Google et Facebook limitent fortement la concurrence dans le marché du numérique. Ainsi, lorsque Facebook a racheté Instagram et Whatsapp, il a pu contrôler trois ensembles de services très prisés des utilisateurs. À ce jour, il est donc très difficile d'envisager l'émergence d'un concurrent sur ce secteur. Autoriser ces concentrations sans imposer de contreparties a peut-être été une erreur. Il nous faut donc être plus exigeants.

Or, certaines opérations de rachat, notamment par les géants du numérique comme Google - qui a racheté près de 400 entreprises ces dernières années -, restent en dehors du champ d'application du contrôle tel qu'il est actuellement défini. Nous proposons donc de compléter la loi française pour les entreprises du numérique, en abaissant les seuils de chiffre d'affaires impliquant l'obtention d'une autorisation. Parfois, c'est au moment

d'une concentration que le marché se fossilise. Ce serait donc une manière pertinente d'assurer leurs pleins effets aux outils du droit de la concurrence.

Enfin, nous assistons à l'émergence de nouveaux outils de régulation, qui impliquent dans certains cas d'adopter un modèle de régulation ex ante, complémentaire aux outils traditionnels qui interviennent plutôt a posteriori. Serait-il intéressant de disposer de règles dont l'application serait limitée à certains acteurs considérés comme dominants ? Le rapport établi par Jason Furman au Royaume-Uni et celui commandité par Margrethe Vestager pour la Commission européenne ont abordé ces questions ; ils ont émis des propositions en ce sens. De notre côté, nous réfléchissons à l'intérêt que ce type d'outil pourrait avoir dans notre activité.

M. Roch-Olivier Maistre, président du CSA. - Ces débats font écho à l'audition conjointe avec Sharon White, Directrice générale de l'Ofcom, autorité de régulation des médias britannique, organisée hier par Catherine Morin-Desailly. Cela illustre parfaitement à quel point les enjeux du numérique sont présents dans notre réflexion.

Nos diverses discussions démontrent notamment combien la coopération entre les différents régulateurs doit être renforcée. En effet, nous sommes confrontés aux mêmes interlocuteurs et nos actions communes se traduisent par plusieurs travaux. Je citerai l'étude conjointe élaborée par le CSA, l'Hadopi, l'Arcep et l'Autorité de la concurrence à propos des assistants vocaux et des enceintes connectées, ainsi que la note commune sur la régulation par la donnée établie par le CSA, l'Arcep, l'Autorité de la concurrence et d'autres autorités administratives indépendantes.

En tant que régulateur sectoriel, nous sommes pleinement concernés par la transition numérique. En effet, nous assistons au développement de nouveaux opérateurs dotés d'une puissance technologique et financière inédite avec l'irruption des plateformes de type Netflix, Amazon Prime Video ou Disney Fox. À côté de ces plateformes de partage coexistent les réseaux sociaux qui proposent également des contenus médiatiques tels que Facebook, Youtube ou Twitter.

Or, l'irruption de ces acteurs fait apparaître une asymétrie importante au détriment des opérateurs domestiques. Comme l'a signalé un avis rendu par l'Autorité de la concurrence en février 2019, les nouveaux opérateurs échappent totalement aux obligations mises à la charge des opérateurs domestiques. Je rappelle que ces derniers relèvent de la loi de 1986 sur les médias qui leur impose notamment de contribuer au financement du cinéma.

De la même façon, nos modèles d'affaires ont été altérés par cette émergence, notamment sur le terrain publicitaire. En effet, l'essentiel des recettes publicitaires est désormais capté par ces acteurs numériques. Face à cette situation, notre réglementation n'a qu'une portée limitée. Ainsi, l'article 40 de la loi de 1986, qui prohibe la détention de plus de 20 % du capital par

un investisseur non européen dans le secteur audiovisuel, n'a aucun effet sur les acteurs du numérique puisqu'il n'est applicable qu'au secteur hertzien.

L'arrivée de ces nouveaux acteurs impose au régulateur des médias que je préside plusieurs enjeux de natures diverses.

Tout d'abord, un enjeu économique. Nos acteurs nationaux sont frappés de plein fouet par l'essor de ces plateformes. Je citerai à titre d'exemple l'annonce faite hier par Canal + d'un plan de départ de 500 salariés. C'est aussi un enjeu démocratique puisqu'il est directement lié à la question du pluralisme sur notre territoire. Plus encore, il s'agit d'un enjeu culturel. Comment garantir le financement de la création alors même que ces nouveaux acteurs n'y contribuent pas ?

Enfin, le dernier enjeu révèle des problématiques sociétales. Notre modèle français a toujours considéré que les médias portaient une responsabilité forte sur des thématiques comme la protection de la jeunesse, le respect de la dignité de la personne ou la juste représentation de la diversité de la société française. À ce jour, les nouveaux acteurs du numérique ne sont pas soumis à ce cadre.

Ces différents enjeux impliquent tous l'intervention de la puissance publique du fait du rôle quasi éditorial que jouent ces plateformes. Dans ce contexte, la mission des régulateurs peut constituer une partie de la solution. Il ne s'agit pas de limiter l'action des régulateurs à de la production de normes et à de la sanction. Il convient de mettre en place des dispositifs permettant d'orienter les opérateurs privés vers l'objectif d'intérêt général défini par le législateur.

D'ailleurs, je suis frappé de constater à quel point les opinions publiques évoluent partout dans le monde en portant l'idée d'une intensification de la régulation. J'en veux pour preuve les débats menés au sein du camp démocrate aux États-Unis, qui pour certains évoquent même l'idée d'un démantèlement de ces plateformes. Cette tendance se retrouve également en Europe, en Australie et en Nouvelle-Zélande. Tous ces États ont à coeur de rentrer dans un schéma de régulation qui permettrait de combattre les phénomènes de désinformation ou de contenus haineux qui, à terme, nuisent aux processus électoraux.

Ce mouvement général qui concerne tant les populations que les États s'est même étendu à ces plateformes elles-mêmes. Elles ne peuvent donc plus se permettre de l'ignorer tant leur modèle économique repose sur leur acceptation par la société. Je vous renvoie aux déclarations publiques de Mark Zuckerberg appelant à plus de régulation.

Par ailleurs, je note que la régulation a franchi récemment des étapes importantes.

Tout d'abord, l'adoption d'une directive concernant les médias audiovisuels étend le champ de la régulation à ces nouveaux acteurs. Il sera

possible de leur imposer les règles applicables au sein du pays de destination. Par exemple, Netflix pourra être soumis à l'obligation de contribuer au financement du cinéma. Nous veillerons au sein du CSA à ce que les transpositions de cette directive soient harmonisées dans les 27 États.

Ensuite, la loi du 22 décembre 2018 sur la lutte contre la manipulation de l'information impose à ces plateformes l'obligation de coopérer avec le CSA. Dans ce cadre, le texte émet plusieurs recommandations à l'égard de ces acteurs, dont la mise en oeuvre sera contrôlée par le CSA. Il en rendra compte dans un rapport public, selon une approche reposant sur le principe du name and shame.

Enfin, la proposition de loi relative à la lutte contre les contenus haineux sur internet a été adoptée hier à l'Assemblée nationale. Elle étend le champ d'action du CSA puisqu'il pourra désormais sanctionner les plateformes si elles ne déploient pas leurs moyens de modération dans des délais rapides, par le biais d'une amende pouvant aller jusqu'à 4 % du chiffre d'affaires mondial. Cela nous place au même niveau que les sanctions applicables en droit de la concurrence.

Cet ensemble dessine un nouveau schéma de régulation à la française, qui ne sera ni celui statocratique appliqué en Chine, ni celui du laisser-faire américain. Nous tentons de responsabiliser les plateformes elles-mêmes en veillant à ce que les dispositifs légaux soient appliqués. Cela suppose évidemment que l'ensemble des régulateurs se coordonne. Au niveau du CSA, nous avons vocation à travailler étroitement avec l'Arcep, la Cnil, l'Autorité de la concurrence et le CNC (Centre National du Cinéma et de l'image animée).

M. Sébastien Soriano, président de l'ARCEP. - Pour reprendre vos questions et y répondre de manière synthétique avant de les développer, il me semble que la régulation est actuellement insuffisante alors même que ses moyens technologiques sont adaptés. De plus, bien que la régulation des acteurs systémiques soit absolument nécessaire, je ne pense pas qu'il faille mettre en place un régulateur unique.

Je commencerai par m'exprimer sur l'insuffisance de la régulation, en prenant le prisme de l'Arcep. Il me semble que notre situation démontre un échec cuisant de toutes les autorités publiques à créer un véritable jeu concurrentiel entre les plateformes du numérique. Certes ces grands acteurs se comportent entre eux comme des concurrents indirects, mais leurs marchés sont bel et bien différents. Chacun exerce sur son marché un pouvoir économique considérable, inédit à l'échelle de l'humanité. Nous ne sommes pas parvenus à offrir le choix aux utilisateurs. Or, le choix est l'arme absolue qui permet de discipliner les opérateurs en leur insufflant la peur de perdre les consommateurs.

L'absence de cette discipline de marché dans le numérique découle de notre sous-estimation du phénomène. Le numérique s'est développé par

un effet de réseau. L'exemple type est celui du réseau social. Si un utilisateur souhaite se créer un compte, il se tournera naturellement vers le réseau sur lequel se trouvent ses amis, indépendamment de toute considération liée à la qualité, à l'ergonomie ou à l'approche respectueuse de sa vie privée. En réalité, le choix est binaire : aller sur ce réseau ou renoncer à tout réseau.

Ce constat explique beaucoup des symptômes que nous identifions, tels que les conditions générales contestables, les risques de fuite de données ou bien la dépendance des entreprises à l'égard des places de marché d'Amazon ou de la publicité en ligne de Facebook ou Google.

Face à cet échec collectif, nous devons être lucides et nous mobiliser en conséquence. Quelles actions pourrions-nous mettre en oeuvre pour réintroduire du choix ? Au cours de votre introduction, vous avez expliqué que nous étions tous les trois confrontés à ces géants du numérique en tant qu'acteurs de la régulation.

En réalité, l'Arcep ne régule pas les acteurs du numérique ; à l'inverse, elle joue plus un rôle d'accompagnateur en vertu du principe de neutralité. Je suis d'ailleurs le premier à déplorer cette situation. Plusieurs propositions ont visé à élargir notre action, mais à ce jour, elles sont restées sans effet. Mme Morin-Desailly avait déposé un amendement en 2015 sur les moteurs de recherche, M. Lalande a également tenté d'introduire un dispositif de notation des plateformes en 2016. Plus récemment, l'Arcep a mis en évidence le pouvoir des terminaux et des systèmes d'exploitation et nous avons proposé au Gouvernement d'inclure une disposition sur ce sujet dans le projet de loi sur l'audiovisuel.

En tant qu'observateur du numérique, l'Arcep n'hésite pas à apporter sa contribution à la réflexion générale sur le numérique, notamment à l'occasion des états généraux du numérique. Je déplore qu'aucune suite n'ait été donnée pour le moment à ce travail collectif qui regorgeait de pistes intéressantes.

Vous posiez une deuxième question sur les moyens dont disposent les régulateurs. Selon moi, le défi majeur est celui de la transformation de nos outils. La donnée on data est un défi essentiel dans notre action. Nous devons parvenir à l'utiliser au mieux dans notre action. Pour cela, deux pistes majeures doivent être explorées.

Tout d'abord, l'utilisation en tant que supervision, à l'instar de l'Autorité des marchés financiers (AMF) dans le secteur financier et de la Commission de régulation de l'énergie (CRE) dans le secteur de l'énergie. Ces régulateurs recueillent un volume considérable de données au sein desquelles ils réussissent à détecter des signaux faibles permettant d'analyser de manière plus fine le marché. Cette technique est celle qui sera mise en oeuvre dans le cadre de la lutte contre les propos haineux.

Ensuite, la donnée peut être mise au service du consommateur afin de lui donner une information plus éclairée sur le domaine concerné. C'est ce

que nous faisons en communiquant l'ensemble des informations relatives à la couverture du réseau. Ce procédé permet d'enclencher une dynamique positive entre les différents opérateurs.

Je constate que nous sommes en train de dompter les outils techniques dont nous aurons besoin à l'avenir pour réguler ce marché. Reste la question des outils juridiques qui doit être approfondie pour permettre à tous les régulateurs de disposer des compétences adaptées pour mener leur action. Bien entendu, des moyens humains et financiers correspondants à l'ampleur de la tâche sont nécessaires.

Votre troisième question portait sur la nécessité de construire un cadre spécifique pour réguler les acteurs systémiques. Cela me semble éminemment souhaitable. En effet, nos règles actuelles sont d'application horizontale et ont donc tendance à sur-réguler et à accroître la charge supportée par les petits acteurs. Ces derniers ont alors d'autant plus de difficultés à trouver leur place sur le marché. C'est une question qui revient souvent s'agissant du RGPD. Se centrer sur les gros acteurs en les soumettant à des règles de supervision spécifiques permettrait d'améliorer notre système.

Pour autant, les régulateurs doivent aussi savoir adapter leur approche en fonction de la nature des problèmes posés. L'accès d'une PME aux places de marché, le marché de la publicité ou celui du commerce en ligne ne sauraient être traités comme le sont des propos haineux ou des fausses informations sur internet. Certes l'approche systémique est nécessaire, mais avec des réponses différenciées selon les situations.

Sur ce plan, l'Arcep a mené un travail approfondi au sujet des terminaux - les smartphones, les enceintes, les voitures ou les télévisions connectées. Les « acteurs des terminaux » sont en train de prendre le pouvoir alors même que nous semblons aveugles face à ce phénomène. Nous régulons la tuyauterie d'internet, mais nous ne regardons pas les robinets ! Nos tuyaux, dans lesquels les opérateurs investissent beaucoup d'argent, sont aujourd'hui ouverts, mais pas les robinets. Or, lorsque l'utilisateur demande des informations à une enceinte connectée, le choix de la source de recherche des informations est réalisé par le terminal. Ces terminaux joueront un rôle de prescripteur central à l'avenir. On peut se connecter à internet sans un moteur de recherche ou sans un réseau social, mais on ne peut pas se connecter à internet sans un terminal. De ce fait, nous devons leur étendre le principe de neutralité déjà applicable à internet. Cette proposition émane de plusieurs autres autorités de régulation européennes. Nous souhaiterions qu'elle figure dans le projet de loi concernant le secteur audiovisuel.

Enfin, je terminerai avec votre dernière question qui portait sur la mise en place éventuelle d'un régulateur unique. Selon moi, le premier réflexe doit être de prolonger les compétences de chaque autorité - c'est ce

qu'on a vu sur le CSA, mais c'est aussi le cas de l'Autorité de régulation des activités ferroviaires et routières (Arafer) à laquelle le projet de loi d'orientation des mobilités confie de nouvelles missions relatives à l'ouverture des données de transport. Bien entendu, un tel renforcement questionnera notre capacité à disposer d'une force de frappe nécessaire. L'Arcep est tout à fait disposée à engager un processus de partage de compétences avec les autres autorités pour mettre en place un pôle commun.

M. Gérard Longuet, rapporteur. -Mme de Silva, comment réagissez-vous à la réalité capitaliste mondiale qui octroie tout au vainqueur ? Il me semble que nous n'avons pas su prévoir qu'internet pouvait être massif et gratuit. Notre conception le reléguait à une sphère élitiste en raison du coût prohibitif des terminaux. Or, par la suite, le numérique a su se développer sur un principe simple, puisque l'utilisateur bénéficie d'une gratuité apparente pour accéder aux services alors même que c'est lui-même qui sert l'opérateur par le biais de ses données. Ce principe est à l'origine de la naissance du RGPD.

En outre, le développement du numérique a permis aux plus puissants d'acquérir une taille telle qu'ils sont aujourd'hui dans une situation absolument dominante. L'effet de réseau ne fait que consolider leurs richesses dans un contexte où le grand public démontre une véritable addiction à leur égard.

Par ailleurs, le modèle économique de ces géants pose de réels problèmes au regard du droit de la concurrence. En effet, il consiste à financer une activité à perte pour croître puis détruire les opérateurs concurrents en les rachetant. Le phénomène a atteint une telle ampleur que les start-up elles-mêmes se développent en vue d'être rachetées par les Gafa. Pensez-vous que l'idée d'un démantèlement puisse être envisagée ?

M. Roch-Olivier Maistre. - Lorsque vous évoquez les propos haineux tenus sur internet, je m'interroge sur la personne du juge. La qualification de tels propos n'est pas aisée tant elle dépend du contexte et des références. Comment combattre ces dérives tout en ménageant notre liberté d'expression ?

M. Sébastien Soriano. - vous avez proposé l'idée de soumettre les terminaux au principe de la neutralité. Cette idée me convainc totalement. De même, lorsque vous vous exprimez en faveur du maintien des différentes autorités de régulation, je souscris à cette vision. Chacune a su gagner le respect de tous grâce à ses compétences, et toute fusion serait inappropriée. Il convient, en revanche, de renforcer la coopération entre ces autorités, tant les sujets sont liés.

M. Jérôme Bascher. - J'aimerais soumettre une question provocatrice. J'ai, tout comme Gérard Longuet, une attitude libérale qui va de pair avec la conviction qu'une régulation est nécessaire. Les géants du numérique ne réussissent-ils pas à se glisser au sein de vos interstices ? Ne

pensez-vous pas, dans ces conditions, qu'il faille introduire une part de censure dans notre régulation des contenus ?

M. Franck Montaugé, président. - J'aimerais réagir au sujet de la régulation ex ante. Je comprends qu'elle nécessite des moyens et des compétences en matière de traitement de données massives. En dispose-t-on aujourd'hui ? Nous avons abordé certains sujets à caractère technique, comme la localisation des données. Estimez-vous que la localisation des data centers et des clouds en dehors de l'Union européenne pose problème ? Par ailleurs, quel est votre positionnement concernant les moteurs de recherche, qui sont devenus des acteurs souverains du numérique ?

Mme Isabelle De Silva. - Le mécanisme du winner takes all, les effets de réseau et la transformation des modèles d'affaires sont au coeur de la révolution que nous vivons. Ces nouveaux modèles d'affaires ont été financés par un marché qui y a cru. Ainsi, longtemps, Amazon n'a pas été rentable et Netflix ne l'est toujours pas. Il s'agit en réalité d'une stratégie d'un nouveau genre, fondée sur la conquête d'un très grand nombre d'utilisateurs et sur la présence sur différents marchés.

À cet égard, l'exemple d'Amazon est frappant : d'abord libraire en ligne, le site internet a ensuite régulièrement élargi ses activités, jusqu'à la production de contenus audiovisuels...

M. Gérard Longuet, rapporteur. - Et aux lanceurs spatiaux !

Mme Isabelle De Silva. - ...de sorte qu'aujourd'hui, nous ne pouvons savoir où s'arrêtera cette entreprise. Les autorités de la concurrence doivent revoir leurs méthodes, consistant traditionnellement à raisonner par marchés pertinents, car certains marchés que l'on pourrait estimer sans liens vont se trouver connectés par les stratégies de captation de ces utilisateurs. Il nous faut amender notre doctrine sur ce point.

Un autre exemple qui doit nous amener à revoir nos concepts est celui de Facebook. On a longtemps pensé qu'un marché non monétisé n'est pas un marché. Or, les marchés bifaces nous montrent que les choses sont plus complexes : d'un côté, le service est gratuit, mais nous permettons, grâce à l'utilisation de nos données, leur valorisation sur l'autre face du marché, par la publicité en ligne.

Dans ce contexte, la concurrence est-elle impossible ? Je refuse toute attitude pessimiste. Nous avons commis une erreur stratégique en autorisant le rachat d'Instagram et de Whatsapp par Facebook. Tirons les conséquences de cet exemple en imposant des règles strictes pour l'avenir. C'est pourquoi nous réfléchissons, avec le Gouvernement, à la définition de règles spécifiques aux acquisitions menées par des acteurs déjà ultra-dominants. Nous assistons aujourd'hui à une véritable perversion de ce système dans lequel les start-ups elles-mêmes cherchent à se faire racheter par les grandes firmes du numérique plutôt que de devenir elles-mêmes les futurs géants.

Vous soulevez la question du démantèlement. Pour notre part, nous examinons froidement ce sujet. Pour autant, certains estiment que le démantèlement créerait une forme d'Hydre de Lerne. De ce fait, nous devons imaginer d'autres pistes, notamment sur la problématique de l'accès aux données. Nous pourrions ainsi, par exemple, organiser un droit d'accès - pas forcément gratuit - aux données détenues par un moteur de recherche qui permettrait à un nouvel acteur de disposer des moyens pour se développer. Cela peut s'organiser par le droit de la concurrence ou par une régulation ciblée sur l'accès aux données.

Par la suite, nous devons réfléchir à la question de la valeur, lorsque nous sommes confrontés à certaines pratiques. À titre d'exemple, je citerai le cas de Booking prélevant des commissions sur les gains des hôteliers, ou bien d'Apple facturant une commission aux créateurs d'applications. Selon moi, il faut qualifier ce type de phénomène comme de l'abus d'exploitation, notion quelque peu oubliée ces dernières années, durant lesquelles nous nous intéressions davantage aux pratiques discriminatoires. Nous avons d'ailleurs utilisé cette notion il y a quelques mois en sanctionnant pour la première fois depuis dix ans des prix excessifs pratiqués par une entreprise en monopole dans le secteur du traitement des déchets hospitaliers. Nous pourrions utiliser ce même type de raisonnement dans le numérique pour une entreprise en monopole qui changerait du jour au lendemain les commissions qu'elle prélève pour le référencement sur une application devenue incontournable.

Il est également possible d'agir au regard des barrières à l'entrée sur un marché. Actuellement, la Commission se penche sur le cas de Spotify qui entend démontrer que les commissions prélevées par Apple sont illégitimes. La question est également posée au sujet de la place de marché d'Amazon : l'entreprise favorise-t-elle ses propres produits, notamment grâce aux données que les vendeurs utilisant sa place de marché sont contraints de lui transmettre ? Je souhaite également saluer l'avancée que constitue l'adoption du règlement dit « Platform to business » au niveau européen, qui porte précisément sur l'équité des relations commerciales entre les plateformes et les entreprises dont l'accès à la plateforme est une condition sine qua non pour atteindre le consommateur.

Par ailleurs, le traitement de ces sujets doit se faire sur le plan politique, notamment sur le terrain fiscal. Il n'est pas admissible que des revenus générés sur le territoire français n'y soient pas imposés. Une première réponse a été apportée par Mme Vestager, qui a qualifié d'aide d'État le régime fiscal particulier accordé par l'Irlande à Apple, mais c'est une forme de pis-aller au regard d'un système qui favorise l'optimisation fiscale. La taxe Gafa peut constituer une première ébauche, mais ne couvre pas d'autres sujets tels que l'équité de la fiscalité entre les plateformes de commerce en ligne et les distributeurs physiques.

Nos efforts doivent converger vers un objectif de rééquilibrage des réglementations nationales. À défaut, ils conduiraient à favoriser encore plus les Gafa. Dans notre avis du 21 février dernier sur l'audiovisuel et le numérique, nous avons démontré que les acteurs classiques du secteur médiatique étaient désavantagés face aux nouveaux acteurs du numérique. Par exemple, il est interdit de proposer de la publicité ciblée à la télévision, alors qu'il existe une liberté totale sur ce point sur internet. Une action volontaire doit être mise en oeuvre. Au-delà des aspects économiques, il est très grave que des acteurs qui ont pris une importance considérable pour la société ne respectent pas les règles sur la protection des données ou admettent des comportements mettant en cause la sincérité des campagnes électorales. Il est essentiel de faire toute la lumière dans les meilleurs délais sur l'affaire Cambridge Analytica. La question du démantèlement relèvera d'une décision américaine. En revanche, la directive sur le renforcement des autorités de la concurrence permet à une autorité de la concurrence d'enjoindre des mesures structurelles. Ainsi, nous pourrons obliger une entité à céder une partie de son activité lorsqu'elle a commis un abus de position dominante.

Vous soulevez la question de la localisation des data centers. Il est effectivement très compliqué de mener une enquête au sujet d'infractions numériques commises par des entreprises dont les centres de décisions sont aux États-Unis et qui met des moyens colossaux pour se prémunir des enquêtes. La nouvelle directive contient cependant une avancée : si l'entreprise détient des données accessibles sur le territoire européen, nous serons en mesure d'y accéder.

Enfin, je rejoins Sébastien Soriano à propos des états généraux du numérique. Il est effectivement frustrant que ces travaux n'aient pas été accompagnés de suites concrètes alors qu'il est nécessaire de muscler l'action de l'État et des autorités sur le plan du big data, des algorithmes et, plus généralement, des ressources issues de ces nouvelles technologies. Les régulateurs peinent à recruter des experts dans ces secteurs, comme des data scientists, et je souhaite que l'État investisse davantage dans ces domaines.

M. Roch-Olivier Maistre. - Je suis convaincu que nous ne pourrons pas réguler les plateformes de la même manière que les médias traditionnels. Je rappelle que ces derniers se sont vu attribuer des fréquences gratuites par l'État ; en contrepartie ils étaient soumis à plusieurs obligations dont l'application était surveillée par le CSA. Ce modèle ne pourra pas être transposé aux plateformes.

De ce fait, il nous appartient de responsabiliser les plateformes les plus importantes en leur fixant des objectifs clairs à atteindre, dont la mise en oeuvre sera surveillée par un superviseur doté de pouvoirs coercitifs.

La fusion entre le CSA et l'Arcep a pu être évoquée par certains comme une solution envisageable. À cet égard, les propos de Sharon White

sont très intéressants. Lorsqu'elle évoque la fusion opérée en Grande-Bretagne entre plusieurs autorités de régulation, elle ne peut que constater que celle-ci a fait perdre quatre années d'action de régulation au profit de la réorganisation administrative qui en a découlé. Je pense que nous devons donc nous consacrer à d'autres priorités, d'autant plus que le schéma actuel de régulation ne laisse pas d'interstices. J'en terminerai avec l'exemple britannique en citant les débats actuels sur la pertinence de confier à l'Ofcom - bien mieux dotée en ressources humaines, avec plus de 900 personnes, que ne le sont le CSA, qui dispose d'environ 300 personnes et l'Arcep doté de 160 à 180 personnels - la charge de réguler le numérique.

Enfin, la question que vous posez au sujet de l'organe chargé de qualifier les propos tenus sur internet est très intéressante. Effectivement, nous sommes constamment confrontés à une zone grise. Si pour les contenus haineux la tâche est plus aisée, le sujet des fausses informations est bien plus délicat à traiter. C'est la raison pour laquelle nous souhaitons que le CSA tienne un rôle de superviseur, et non pas de juge.

M. Sébastien Soriano. - Je reviens sur la question relative aux terminaux. Leur imposer une neutralité permettrait de confier le pouvoir aux individus et aux entreprises. On peut imaginer des dispositifs de contrôle parental labellisés par l'État plus facilement activables, mais cela découlerait du choix des utilisateurs.

M. Jérôme Bascher. - Est-il possible de sanctionner des abus d'exploitation ?

M. Sébastien Soriano. - Sur le plan économique, les abus d'exploitation émanent d'une entreprise dominante qui met en oeuvre des pratiques dommageables pour les autres acteurs : par exemple, Google Maps qui changerait ses codes. À l'origine, une telle manoeuvre n'a rien d'anticoncurrentiel, mais en raison de sa position sur le marché, elle provoquerait une déstabilisation des autres entreprises. Selon moi, nous devons mettre en place des moyens permettant de prévenir ce type de comportement. Or, en l'état du droit de la concurrence, aucune méthode ne permet de préjuger du rôle des acteurs.

Mme Isabelle De Silva. - Sur ce point également, les terminaux ont pris une importance économique considérable. Je crois qu'il nous faut réprimer tous les comportements d'un acteur puissant qui viseraient à interdire l'accès à un marché d'un acteur donné. La décision prise à propos du système d'exploitation Androïd Google en est l'illustration. Nous avions d'ailleurs été visionnaires dans ce domaine lors de l'affaire visant Orange à propos de la distribution de l'iPhone, en empêchant Orange d'obtenir l'exclusivité, considérant que tous les opérateurs devraient pouvoir le distribuer. Il nous faut être impitoyable sur les comportements du même type que ceux condamnés dans l'affaire Google Androïd.

M. Sébastien Soriano. - Nous devons déterminer si des outils spéciaux sont nécessaires, ou bien si ceux du droit commun de la concurrence suffisent. Isabelle de Silva et moi-même n'avons pas le même point de vue sur cette question. Selon moi, des outils nouveaux doivent être développés pour sortir de l'impasse dans laquelle nous nous trouvons actuellement. C'est un peu ce qui a été décidé lors de l'ouverture du monopole de France Télécom à la concurrence : on a considéré que le pouvoir particulier de cet acteur nécessitait des outils propres. Pour caricaturer, il s'agit d'opposer le droit de la concurrence, qui agit en quelque sorte avec un tribunal traitant des dossiers au cas par cas lorsqu'il en est saisi, à un régulateur ex ante, qui construit un agenda avec des objectifs précis et en vérifie la bonne application en continu.

M. Franck Montaugé, président. - Ce sujet doit-il être corrélé avec la question d'un système d'exploitation souverain ?

M. Sébastien Soriano. - La question des systèmes d'exploitation dépasse les enjeux économiques. Il est très difficile de mettre au point un système entier, à tel point que des acteurs majeurs comme Nokia ou Microsoft ont échoué à le faire.

En revanche, certaines de nos propositions aideraient à la constitution d'un écosystème favorable à l'apparition d'un tel système d'exploitation car nous proposons de favoriser des standards qui permettraient à tout créateur d'application de la rendre utilisable sur tout système d'exploitation, ce qui, en retour, favoriserait l'apparition de nouveaux systèmes d'exploitation.

Concernant les moteurs de recherche, j'aurais la même réponse. Un principe d'ouverture aurait pour effet d'obliger à référencer de la même manière tous les moteurs de recherche et d'empêcher celui qui contrôle le terminal de bloquer l'accès à certaines solutions.

Mme Isabelle de Silva. - Certaines régulations ex ante sont utiles. Je pense notamment aux règles concernant la transparence applicables aux algorithmes. La France a su se montrer très en avance dans ce domaine dans la loi pour une République numérique portée par Axelle Lemaire, qui a confié à la Direction générale de la concurrence, de la consommation et de la répression des fraudes la mission de contrôler certaines règles notamment en matière d'avis en ligne. Une grande partie de ces règles se retrouvent dans le règlement dit « Platform to business ». Nous y avons été favorables dès lors qu'il s'agissait de bien cibler et de proportionner le dispositif à une problématique identifiée, qui est celle des relations commerciales entre les plateformes et les entreprises qui en dépendent pour leur activité économique.

Ce mouvement n'est qu'un début. Nous pouvons d'ores et déjà nous projeter dans la nouvelle génération de règles en matière de protection des données. Le RGPD a introduit des principes de proportionnalité. Pour

autant, du point de vue du consommateur, il en ressort peu de bénéfice. En effet, la plupart des personnes valident systématiquement la collecte de leurs données. Par conséquent, nous menons actuellement une réflexion globale au niveau européen - et Jean Tirole s'est également prononcé en ce sens- visant à faire évoluer la réglementation : il s'agirait de ne soumettre à validation que les collectes qui iraient au-delà du nécessaire. Cet axe de réflexion me paraît intéressant car, sur la protection des données, force est de constater que le consommateur a du mal à faire ses choix - on dit parfois qu'il relève de son libre arbitre de cesser d'utiliser Facebook s'il estime que cette entreprise utilise ses données de façon abusive. Or, et même si le consommateur est de plus en plus informé, cela reste un sujet complexe à appréhender pour les consommateurs et nous sommes encore loin d'une véritable prise de conscience. Ainsi, un tel dispositif permettrait d'atteindre plusieurs objectifs : une restriction de l'utilisation des données et un rééquilibrage de la valeur tirée de l'utilisation des données à des fins publicitaires.

M. Jérôme Bascher. - J'ai lu récemment une critique affirmant que le RGPD avait pour effet une fuite de nos données en dehors de l'Union européenne. Pouvons-nous craindre que notre souveraineté ne soit transférée ailleurs ?

Mme Isabelle De Silva. - C'est un point fondamental : celui des effets induits par nos règles de régulation. On peut voir plus positivement le RGPD en estimant que l'Europe a lancé un mouvement qui est actuellement suivi par plusieurs pays dans le monde - c'est le cas du projet de réglementation en Californie et au Brésil, et ce sujet est au coeur des débats dans la perspective de la prochaine présidentielle américaine. On peut donc considérer que le RGPD essaime à l'international, notamment grâce à l'outil très puissant que constitue le principe d'équivalence - c'est d'ailleurs l'enjeu des discussions qui se déroulent aujourd'hui entre l'Europe et le Japon.

S'agissant de la tentation d'échapper à ces règles, elle est sans doute réelle. Toutefois, dès qu'un Européen est concerné, le RGPD a vocation à s'appliquer. Dès lors, la solution consistant à transférer les données en dehors de l'Union européenne serait totalement inopérante.

M. Sébastien Soriano. - J'aimerais terminer par des propos plus personnels. J'ai eu la chance de participer à des échanges stratégiques avec la Corée du Sud, Taïwan et le Japon. J'ai été accompagné par le sociologue Antonio Casilli, qui a évoqué son travail à propos des fermes à clic présentes dans plusieurs pays comme la Chine ou les Philippines.

Ces entreprises emploient de la main-d'oeuvre très bon marché qui est chargée de cliquer selon les consignes données par le client. Initialement, les grandes marques avaient recours à ce service pour gonfler leur notoriété sur les réseaux sociaux. Peu à peu, leur activité s'est diversifiée, dérivant vers le domaine de la manipulation de l'information.

Je signale l'existence de ces entreprises qui pose la question de l'identité et des objectifs de ceux qui cherchent à propager ce type de contenu. Par exemple, est-ce normal que des milliers d'adresses IP basées en Chine participent aux débats sur la politique européenne ?

Il me semble que ce sujet peut constituer un angle d'intérêt important dans le cadre des travaux menés par votre commission.

M. Franck Montaugé, président. - Ce point m'amène à évoquer deux autres sujets. Ainsi, à propos du traitement des contenus haineux sur internet, seriez-vous opposés à la levée de l'anonymat sur internet ? Il me semble que, quand on affirme quelque chose, il faut être capable de l'assumer.

De plus, ne serait-il pas utile que les internautes puissent disposer d'une vision synthétique des données qu'ils produisent ? Cela permettrait d'améliorer leur culture au sujet d'internet.

M. Sébastien Soriano. - La question relative à la levée de l'anonymat ne relève pas des compétences de l'Arcep, mais en tant qu'observateur, je la relie à celle du pseudonymat. La question que cela pose est de savoir comment découvrir l'identité d'une personne sur internet. De ce fait, une levée du pseudonymat serait lourd de conséquences pour la nature d'internet, d'autant plus qu'il s'agirait parfois de lutter contre des personnes qui n'existent pas. Pour cela, il me semble que d'autres méthodes, plus proportionnées, existent.

Mme Isabelle de Silva. - L'ensemble de la société est en retard au sujet du bon usage d'internet. Or, nous assistons tous à des comportements inacceptables qui impliquent une réaction forte de tous les acteurs sociaux.

À titre personnel, je crois que l'usage des outils numériques est un grand défi posé à nos États et à nos sociétés. Il me semble que l'école est en retard, et la responsabilité est sans doute partagée avec les parents. Parfois, l'école prescrit l'usage d'internet, notamment pour accéder aux devoirs, alors même que cela ne semble pas indispensable : est-ce son rôle ? Il me semble fondamental de mener une réflexion profonde visant à mieux utiliser l'outil numérique.

M. Roch-Olivier Maistre. - Je partage votre vision au sujet de l'éducation aux médias, le CSA déploie d'ailleurs un certain nombre d'actions sur ce sujet. Le statut juridique de ces plateformes date de l'époque de leur création, alors même qu'elles ne disposaient pas de la même puissance économique.

Elles s'abritent derrière le statut d'hébergeur, leur responsabilité doit donc être repensée. Dans les médias classiques, le fait d'avoir un éditeur responsable change la donne sur ce qui est diffusé. On supporte de moins en moins sur internet ce qu'on ne supporte déjà pas depuis longtemps à la télévision, à la radio ou dans la presse.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible en ligne sur le site du Sénat.

Audition de M. Michel Paulin, directeur général d'OVH,
le 11 juillet 2019

M. Franck Montaugé, président. - Notre commission d'enquête poursuit ses travaux avec l'audition de Monsieur Michel Paulin, directeur général de l'entreprise OVH.

Je rappelle pour la forme qu'un faux témoignage devant notre commission d'enquête serait passible des peines prévues aux articles 434-13, 434-14 et 434-15 du Code pénal. Je vous invite à prêter serment de dire toute la vérité, rien que la vérité ; levez la main droite et dites : « je le jure ».

Conformément à la procédure applicable aux commissions d'enquête, M. Paulin prête serment. Vous êtes depuis près d'un an le directeur général d'OVH. Cette entreprise est spécialisée dans les services de cloud. Elle a été fondée en 1999 à Roubaix par Octave Klaba qui en est désormais l'actionnaire majoritaire. Elle est devenue un acteur important du cloud, qui entend se développer partout dans le monde et ainsi défier les grands leaders du secteur que sont Amazon, Microsoft, Google et IBM sans même évoquer les entreprises chinoises. Elle est donc l'une des rares licornes françaises qui tentent de lutter face à ces géants du numérique.

Pourrez-vous nous donner des éléments de comparaison, par exemple en nombre de centres de données, afin que nous puissions nous rendre compte de l'importance de votre activité par rapport à celle de vos concurrents ?

Le fondateur de l'entreprise souligne l'importance de faire héberger ses données en Europe pour éviter qu'elles ne soient soumises à des lois de portée extraterritoriale. Dans une interview publiée l'an dernier, il déclarait ainsi : « il s'agit d'arrêter d'être des bisounours et de prendre conscience que l'Europe est en train de se faire dépouiller de ses données, que les gouvernements perdent la main face à une poignée de grandes entreprises privées. »

Dans le même temps, Monsieur Klaba a également émis un avis réservé sur le projet annoncé par le ministre de l'Économie et des Finances et présenté comme un cloud souverain. Quelles solutions préconisez-vous ? Pouvez-vous nous expliquer en quoi votre entreprise marque un jalon important pour la souveraineté numérique française et européenne ?

M. Michel Paulin, directeur général d'OVH. -Il est clair que l'un des sujets majeurs de la souveraineté est le numérique, tant celui-ci se place désormais au centre des sujets sociétaux, politiques et économiques. Bruno Le Maire a d'ailleurs affirmé qu'il n'y a pas de souveraineté politique sans souveraineté numérique. Selon moi, il est donc essentiel que l'État et l'Union européenne puissent garantir aux citoyens l'effectivité de cette souveraineté.

À titre introductif, je présenterai notre entreprise, OVH. Nous sommes une entreprise française, fondée il y a vingt ans par Octave Klaba. Le siège social est situé à Roubaix. À ce jour, le capital est encore détenu en majorité par la famille Klaba. OVH emploie plus de 2 000 salariés, dont plus de 1 000 à Roubaix. Notre chiffre d'affaires s'élève à plus de 600 millions d'euros, avec une croissance supérieure à 20 %. Nous sommes qualifiés de pure player, ce qui signifie que nous n'exerçons qu'une seule activité, le cloud. Cela nous distingue de la majorité des autres acteurs sur ce marché.

Nous sommes une véritable entreprise industrielle puisque nous produisons nous-mêmes nos serveurs dans un site industriel situé à Croix. Nous achetons les composants et les montons ensuite. À ce jour, nous disposons de 28 centres de données, présents sur quatre continents. En Europe, nous détenons des structures en France et dans la plupart des pays européens comme l'Allemagne, la Pologne ou l'Angleterre. Nous disposons également de centres de données au Canada, aux États-Unis, à Singapour et en Australie. Sur ce marché mondial, avoir une présence internationale est une condition sine qua non pour être en mesure d'accompagner au mieux ses clients.

Sur la période 2016- 2021, nos investissements dans les infrastructures s'élèveront à 1,5 milliard d'euros. Nos serveurs sont construits selon des principes proches de l'open source : ils sont auditables.

Afin de renforcer notre indépendance, nous concevons nous-mêmes nos centres de données et avons également mis au point une technique innovante de refroidissement de nos serveurs à l'eau. Au-delà de ses vertus écologiques, ce processus s'avère bien plus efficace que celui employant l'air. Afin de renforcer encore notre indépendance, nous possédons également notre propre réseau de fibre, ce qui garantit la maîtrise totale du processus pour nos clients.

Comme je l'indiquais, nous ne proposons que du cloud. Dans le top 10 mondial, nous sommes classés à la neuvième place. Nous sommes la seule entreprise européenne qui figure dans ce classement, et la seule à ne proposer que du cloud. Les huit premiers classés sont les géants que vous connaissez tous, américains et chinois. Le dixième est une entreprise japonaise. Sans aides publiques, OVH est devenu le leader européen du cloud.

Nous proposons tous les types de services : public, privé ou hybride, serveurs dédiés et barre métal. Notre philosophie repose sur le principe suivant : « Innovation is freedom », autrement dit, l'innovation doit servir à la liberté et non pas à emprisonner nos clients. Loin d'être anecdotique, cette affirmation se traduit concrètement dans l'ensemble de nos offres, qui s'articulent autour des concepts d'ouverture, de réversibilité et d'accessibilité, et qui reposent souvent sur des logiciels libres, ce qui garantit

à nos clients le respect de leur liberté. Notre parti pris est donc de refuser tout système qui conduirait à emprisonner les citoyens et les entreprises.

Dans le cadre de notre réflexion au sujet de la souveraineté numérique, comment OVH peut-elle apporter des éléments de réponse ? Le numérique se place au coeur de nos préoccupations industrielles, politiques et sociétales. Nous sommes convaincus que ces outils numériques constituent des actifs économiques à part entière. Les données personnelles et celles des entreprises ont une valeur importante. C'est d'ailleurs sur elles que les Gafam ont construit leur puissance. Au-delà de ces acteurs, les données sont stratégiques pour les États et les entreprises dans leur ensemble, comme l'illustrent les effets produits par une utilisation malveillante de ces données.

Le numérique constitue également un enjeu économique. Les données peuvent être utilisées pour attaquer des concurrents sur le marché. Comme l'a justement rappelé le député Gauvain dans son rapport, certains États se sont ainsi dotés d'outils juridiques permettant d'affaiblir les règles relatives à la protection des données. Dans ce contexte, il n'est plus suffisant de conserver les données en Europe pour parvenir à les protéger. En effet, avec le Cloud Act, l'accès aux données est rendu possible, quel que soit leur lieu de stockage.

Selon moi, le Cloud Act est une arme très puissante qui vise directement la souveraineté des États. Son application permet aujourd'hui que certaines entreprises américaines puissent saisir la justice américaine pour qu'elle obtienne ces données. Cette transmission s'opérera sans aucune intervention des juridictions françaises. En ce sens, cela pose un réel problème.

Jusqu'à présent, les questions de protection étaient appréhendées par un prisme strictement technologique - via le cryptage des données, l'installation de pare-feux.... Bien entendu, cette lecture est importante. Pour autant, quand bien même la porte d'une maison serait blindée, si la loi autorise à cambrioler l'intérieur de la maison, la protection de la porte sera inutile. L'enjeu est donc de comprendre l'importance pour les États de se doter d'outils puissants pour résister aux atteintes portées à la souveraineté numérique en Europe. Lorsqu'Octave Klaba évoquait le terme de « bisounours », son propos n'avait rien de défaitiste, car des acteurs comme OVH détiennent des éléments de réponse.

Quels sont les grands enjeux auxquels il faudra faire face ? Le premier enjeu est celui de la transparence. L'État, les collectivités locales et les acteurs économiques doivent être en mesure de comprendre quels sont les risques inhérents à chaque système. Par exemple, les appels d'offre lancés en matière de cloud excluent les solutions situées en zone inondable. Mais certaines entreprises ne posent pas la question de savoir quel est le droit

applicable aux données stockées ! Une plus grande transparence est donc nécessaire afin que chacun puisse prendre sa décision de façon éclairée.

La transparence doit également se traduire dans le cadre des procédures d'appels d'offres. Par exemple, lorsque certaines collectivités territoriales passent un appel d'offres dans le domaine du cloud, elles confient leurs données à des intégrateurs afin qu'ils mettent en oeuvre des solutions. Dans le cadre du comité stratégique de filière, nous estimons qu'il est nécessaire d'indiquer où sont stockées ces données et à quel droit elles seront soumises. À titre personnel, j'ai pu observer que ces intégrateurs les laissaient dans des services de cloud qui ne peuvent être qualifiés de cloud de confiance. Mon propos ne doit pas être interprété comme de l'animosité à l'égard de nos concurrents. Je souhaite seulement qu'il y ait de la transparence sur les conditions de stockage des données, et donc sur le droit applicable.

Au-delà de l'objectif de transparence, je pense que nous devons abandonner toute attitude fataliste. L'exemple d'OVH en témoigne. Sans bénéficier à aucun moment d'argent public, elle a su rester dans la course mondiale au sein d'un domaine économique ultra compétitif. Les concurrents auxquels elle a fait face ont été fortement avantagés dans leurs propres États par le biais des commandes publiques.

Si la préférence nationale est une notion absente de notre droit, c'est une réalité concrète dans les autres États. L'État et les collectivités territoriales doivent comprendre à quel point l'enjeu de ces questions dépasse la seule sphère économique. Choisir un acteur américain ou chinois est lourd de conséquences tant au niveau de la protection des données que pour la viabilité à long terme de la filière numérique en Europe.

Or il existe énormément d'entreprises performantes en Europe. OVH n'est pas un exemple isolé. Il existe des acteurs compétitifs, mais pas encore présents sur l'ensemble de la chaîne du numérique, notamment dans les random access memory (RAM), les puces, le hardware et les systèmes d'exploitation.

En tant qu'entreprise européenne numérique, nous tentons notre chance, mais nous ne pourrons rester seuls dans cet environnement. Nos concurrents bénéficient d'un soutien important de la part de leurs États, qui ont des stratégies en la matière : la Chine a ainsi pour objectif d'être le leader en intelligence artificielle. De même, aux États-Unis, toute la stratégie universitaire de recherche est basée sur un système d'aides, tant privées que publiques. Il me semble que l'État français devrait conclure des accords avec d'autres partenaires. Nous disposons d'ingénieurs parmi les meilleurs au monde, qui sont malheureusement recrutés par ces acteurs étrangers du numérique. Je suis certain que l'Europe détient toutes les capacités pour rivaliser avec eux. L'exemple d'OVH, comme d'autres, n'est pas suffisamment mis en valeur.

Les acteurs économiques doivent également comprendre ces enjeux. Or, quand j'observe que de grandes sociétés publiques passent des accords avec des entreprises américaines, je ne peux que le déplorer. J'imagine bien que la conclusion d'un accord avec Google peut apparaître plus enthousiasmante qu'avec OVH. Pour autant, ce type de situation me semble regrettable dans la mesure où nos solutions sont parfaitement adaptées.

Par ailleurs, j'aimerais rappeler à quel point le cadre juridique mis en place par le RGPD est unique sur le marché mondial. Cet exemple européen inspire certains pays comme le Canada et la Californie. C'est une avancée majeure dans la protection de nos données personnelles. Face à cela, je ne peux que déplorer les stratégies de certains États visant à se doter d'outils comme le Cloud Act. L'Europe doit affirmer une position forte pour protéger toute l'efficacité du RGPD et garantir ainsi aux citoyens que leurs données sont protégées.

Je terminerai en insistant sur l'importance que revêt la réversibilité d'un système : il est indispensable que les entreprises gardent la possibilité de revenir en arrière si elles le souhaitent. Si l'ampleur du coût induit par une telle décision s'avère dissuasive, cette démarche est de fait impossible. Au final, cela alimente la capacité des gros acteurs à préempter les données. Nous pensons que l'intérêt majeur des systèmes de cloud est justement leur capacité à apporter de la flexibilité et de la souplesse aux entreprises. Si ce système aboutit à la mise en place d'un monopole, que reste-t-il de son intérêt ?

Aussi la souveraineté numérique ne peut en aucun cas exister si la notion de réversibilité n'est pas mise en avant : tous les monopoles de fait, américains ou chinois, existent car il n'y a pas d'alternative reposent sur l'irréversibilité. C'est un cercle vicieux duquel il est impossible de sortir.

M. Jérôme Bascher. - Merci beaucoup. Vos propos démontrent à quel point le sujet juridique est majeur. Par le passé, nous restions focalisés sur la localisation physique des données et des infrastructures. Aujourd'hui, il semblerait que les problèmes d'insécurité juridique et de régulation mondiale soient devenus plus prégnants. Qu'en pensez-vous ?

Par ailleurs, l'Union européenne et la France pourraient-elles adopter une attitude de patriotisme économique en valorisant un leader ?

M. Michel Paulin. - Sur le premier point, je suis parfaitement d'accord avec vous. La localisation des données est un enjeu purement technique. Le lieu est choisi pour des raisons d'efficacité. Chez OVH, nous avons des sites en France, en Espagne, en Italie ou en Asie.

En revanche, le droit applicable à ces données dépend de l'acteur hébergeur. S'il est américain, il relève des juridictions américaines. Dans ce cas, quand bien même les données seraient stockées en France, elles seraient soumises à l'application du Cloud Act. Jusqu'à présent, il y avait un échange entre deux juges pour obtenir une transmission de ces données. Avec cette

réforme, l'État américain échappe à cette phase d'entente judiciaire. Cette évolution est effectivement majeure.

De plus, les données ont vocation à circuler. La souveraineté des données apparaît comme un enjeu essentiel pour les États et pour l'Union européenne. Je n'aspire pas à ce que l'ensemble des données soit stocké en Europe. Pour autant, l'État doit avoir conscience des effets attachés à certaines de ses décisions, notamment celles visant à confier à des acteurs étrangers le soin de conserver des données. Nous discutons fréquemment avec des acteurs comme l'Anssi (Agence nationale de la sécurité des systèmes d'information), mais ce dialogue ne revêt pas de réel enjeu tant ce domaine est régulé. À l'inverse, les secteurs bancaires ou médicaux doivent attirer toute notre attention sur ces questions.

Sur le second point que vous avez évoqué, je pense que l'Europe souffre d'un complexe d'infériorité par rapport aux entreprises américaines et chinoises. Trop souvent, elle n'accorde pas aux entreprises européennes toute la reconnaissance qu'elles mériteraient. Or il existe énormément de succès en Europe. Ceux concernant les entreprises américaines semblent davantage médiatisés.

Il me semble également qu'il faudrait rechercher les solutions numériques en Europe, plutôt que d'avoir le réflexe de se tourner vers les entreprises étrangères. Sans parler de mettre en place un patriotisme économique, je constate parfois qu'OVH n'est même pas consultée au cours de certains appels d'offres.

M. Jérôme Bignon. - À titre personnel, je suis un adepte d'OVH, dont je suis client.. En tant qu'élu des Hauts-de-France, je fais preuve d'une certaine solidarité territoriale. De plus, je suis issu d'une tradition familiale de patriotisme industriel. Il me semble que cette attitude a du sens à l'heure actuelle.

Je déplore que beaucoup de citoyens n'aient plus conscience de la nécessité d'être attentifs aux endroits dans lesquels des richesses peuvent se développer. Le succès d'Airbus pourrait être transposé dans le numérique. Il me semble que nous disposons des mêmes compétences que les ingénieurs de la Silicon Valley. Je me demande également si OVH ne pourrait pas agir plus pour être mieux connue du grand public.

Par ailleurs, je rejoins votre approche de la question extraterritoriale. La solution développée dans le Cloud Act est contraire aux fondements de notre droit. C'est un vrai sujet pour lequel nous devons continuer à rechercher des solutions.

La question de la réversibilité est également essentielle. Sans réversibilité, le stockage s'apparente à une confiscation des données. Mais au-delà des problématiques de stockage, il s'agit à mon sens d'un abus de droit. Cette qualification juridique mériterait d'être creusée dans l'optique d'un contentieux.

M. Michel Paulin. - Les entreprises européennes, dont OVH fait partie, de mener une introspection visant à accroître leur capacité à gagner en visibilité. À l'étranger, les aides dont nos concurrents ont pu bénéficier au départ ont fortement participé à leur déploiement. À mon sens, trois facteurs expliquent les différences qui existent entre ces entreprises et les nôtres.

Tout d'abord, les États américains et chinois ont mis en place un écosystème centré sur l'accompagnement des entreprises. Si le système chinois repose sur un État omniprésent, le système d'aide américain est plus décentralisé, mêlant des fonds privés et publics, provenant de l'État, des collectivités locales et des universités... De plus, l'État aide directement les start-ups par le biais des commandes publiques.

Ensuite, le marché européen est très morcelé, en raison de la diversité des langues et des législations. Les entreprises qui veulent s'y implanter doivent réaliser des investissements importants pour un résultat peu rentable comparé à celui escompté sur un marché d'envergure comme le marché chinois.

Enfin, les coûts induits par le marketing en Europe sont considérables. Une stratégie visant à faire croître la notoriété d'une entreprise est plus facile à mettre en oeuvre aux États-Unis qu'en Europe.

Je partage donc votre constat et le regrette tout autant. Pour autant, le nombre de start-ups rachetées sur notre sol par les entreprises américaines démontre bien à quel point les entreprises européennes regorgent de bonnes idées. Il faut donc accompagner leur développement.

M. Franck Montaugé, président. - Vous avez souligné l'intérêt du RGPD. Pensez-vous qu'il puisse être comparé au Cloud Act, ce qui permettrait de rétablir une forme d'équilibre entre l'Union européenne et les États-Unis ? Je rappelle que cela constitue l'une des orientations du rapport Gauvain.

Disposez-vous de serveurs aux États-Unis ? Dans ce cas, comment allez-vous gérer le Cloud Act ?

Vous avez évoqué l'enjeu important de la réversibilité. Lors de nos auditions précédentes, plusieurs personnes se sont prononcées en faveur de l'interopérabilité et de la portabilité des données. Partagez-vous leur opinion ? Je suis conscient que votre secteur d'intervention est différent, pour autant j'ai cru comprendre votre adhésion aux systèmes en open source.

La situation actuelle dans laquelle les données se situent à 80 % dans les centres de données et à 20 % sur les sites de production de données va s'inverser. Comment appréhendez-vous cette évolution ? Eu égard à votre modèle économique centré sur le stockage de données, allez-vous garder la même stratégie de spécialisation, ou développerez-vous d'autres activités liées à la commercialisation de données ?

M. Michel Paulin. - Aux États-Unis, notre filiale est régie par le droit américain. À ce titre, elle respecte scrupuleusement la loi américaine. En revanche, nous avons fait en sorte que seule cette filiale soit soumise au Cloud Act,.et qu'elle ne dispose d'aucun accès aux données situées à l'extérieur des États-Unis : il s'agit d'un bastion isolé. L'accès ne serait tout simplement pas possible d'un point de vue technique : de ce fait, aucun agent américain ne pourra accéder aux données situées en dehors du territoire américain. Cet exemple est totalement unique dans notre activité, puisque l'ensemble des sociétés européennes de notre groupe est soumis aux mêmes règles. Le cas américain est donc à part.

Notre activité n'est pas concernée par les questions d'interopérabilité ou de portabilité. Pour autant, nous mettons en avant la réversibilité du stockage qui est fondamentale à l'heure actuelle. OVH se doit d'offrir à ses clients la possibilité de revenir en arrière - nous travaillons beaucoup avec OpenStack pour garantir cette réversibilité. À leur tour, nos clients offrent aux leurs cette même garantie. À ce titre, nous agissons comme un facilitateur. Sans la réversibilité, le risque est de mettre en place une situation de monopole de fait. Cela conduirait à ne laisser exister que les seules Gafa. Or OVH entend se positionner comme une alternative sérieuse à ces entreprises.

Nous ne souhaitons offrir que des services de cloud. Il nous paraît important de rester focalisés sur ce secteur pour plusieurs raisons. Tout d'abord, c'est un marché qui présente un potentiel de croissance important. Notre objectif est de nous maintenir dans le top 10 des entreprises mondiales du secteur. Ensuite, ce domaine implique de réaliser des investissements massifs dans nos infrastructures et dans la recherche et le développement. Or, face à nos concurrents qui disposent de moyens colossaux, nous devons consacrer toute notre énergie dans ce sens. Se diversifier nous exposerait à un risque de dilution. Nous concentrer sur notre savoir-faire nous permet de conserver notre position d'alternative aux GAFA, et de proposer un cloud de confiance à nos clients.

J'aimerais évoquer l'edge computing. C'est à la fois un sujet technique et un modèle économique. Au niveau du modèle économique, cela ne change pas ce qui existe déjà. Être capable de gérer un centre de données nécessite de l'innovation et des compétences, ce dont nous disposons déjà. À ce titre, nous sommes, avec d'autres, les acteurs les mieux placés pour tenir ce rôle.

Dans ce contexte, l'avenir du cloud réside-t-il dans des gros centres de données interconnectés pour traiter l'ensemble des données ? Je ne le pense pas. Si je prends l'exemple des voitures autonomes, leur mise en place nécessitera énormément de données pour analyser la route et échanger les informations de manière très rapide avec un centre de données local. De nombreuses interrogations restent à résoudre, mais il est clair que ce rééquilibrage aura lieu.

M. Gérard Longuet, rapporteur. - Dans le monde du numérique, la mémoire est interminable. Rien n'est oublié. Dans le secteur de la gestion des données, l'archivage et le stockage sont des domaines très vivants. Dans ce contexte, comment appréhendez-vous cette notion de permanence, qui détient la propriété de ce patrimoine et comment se gère-t-il ?

M. Michel Paulin. - D'un point de vue purement technologique, tout le matériel magnétique a une durée de vie limitée. Les nouvelles technologies reposent désormais sur un matériel en verre qui peut durer des millénaires. Bien entendu, cela interroge sur l'intérêt de conserver des données sur une telle période.

Notre approche est basée sur la volonté de nos clients. Ce sont donc eux qui décident pendant quelle durée ils souhaitent que leurs données soient conservées. En tant qu'hébergeurs, nous ne sommes que des dépositaires et ne regardons jamais leurs données. Cela permet à nos clients de nous confier leurs données en toute confiance. Leurs souhaits sont très variables au sujet de la durée de conservation. En toute hypothèse, nous leur fournissons un service conforme à leurs exigences.

M. Gérard Longuet, rapporteur. - Assurez-vous d'autres prestations liées à l'utilisation des données pour le compte de vos clients ?

M. Michel Paulin. - Non. Les GAFA le font. Ce sont des acteurs qui hébergent et fournissent d'autres services. Ils agissent à la fois comme hébergeurs et comme fournisseur de services - ce qu'on appelle Software as a Service ou Saas. OVH a pris le parti de ne pas se positionner de la sorte. Nous nous limitons à proposer des solutions de cloud à nos clients. De ce fait, aucun de nos salariés ne peut accéder aux données hébergées.

M. Gérard Longuet, rapporteur. - J'imagine que vous consacrez une part d'investissements importante à votre activité.

M. Michel Paulin. - Ces dernières années, nous avons réalisé 1,5 milliard d'investissements, ce qui est effectivement très important. Sur le plan comptable, nos amortissements sont élevés. Nous agissons comme un véritable acteur industriel. Nous concevons et construisons l'ensemble de nos serveurs, après avoir acquis leurs composants qui arrivent dans notre site de Croix.

Ce processus de fabrication interne présente trois avantages : tout d'abord, en évitant toute sous-traitance, nous faisons des économies. Ensuite, nous maîtrisons la qualité de nos serveurs. Enfin, nous nous assurons de la traçabilité de l'ensemble du processus depuis sa conception jusqu'à sa mise en place.

Cette chaîne est entièrement transparente. Le logiciel de robotisation nous appartient pour l'avoir développé en interne. De ce fait, tous nos systèmes peuvent être audités. Cette intégration verticale est assez remarquable dans l'industrie.

M. Gérard Longuet, rapporteur. - Les évolutions technologiques dans votre secteur sont-elles régulières ou risquez-vous d'être frappés par une révolution technologique rendant vos équipements obsolètes ?

M. Michel Paulin. - Tout notre métier repose sur l'innovation. Notre capacité à innover est donc une question de survie. Dans notre domaine, un cycle long ne dure que deux à trois ans. Par conséquent, il faut sans cesse être capable d'anticiper les tendances.

À titre d'exemple, je citerai le procédé de refroidissement par l'eau de notre serveur, très innovant. De même, nous avons déposé beaucoup de brevets qui nous permettent de nous distinguer dans ce secteur.

Pour rester innovants, nous avons conclu des partenariats avec plusieurs start-ups européennes, dont Systran, une société française en pointe sur l'intelligence artificielle appliquée à tout ce qui est audio, notamment pour la capacité à détecter des choses par le langage.

Je pourrais donner d'autres exemples. Ces collaborations démontrent notre conviction qu'à plusieurs, nous pourrons fédérer et démultiplier nos efforts de recherche. L'État et les collectivités territoriales doivent jouer un rôle dans ce contexte. Nous-mêmes fournissons aux start-ups, dans le cadre de notre programme « digital launchpad », des solutions en matière de cloud, de formation et d'assistance parce que nous sommes pleinement conscients de la difficulté qu'il y a à se développer sur ce marché. Nous avons déjà aidé 1 500 start-ups dans ce cadre.

L'ensemble de l'écosystème européen doit développer sa capacité à travailler ensemble pour continuer à innover. Sans cela, il ne sera pas en position de survivre sur ce marché.

M. Gérard Longuet, rapporteur. - J'aimerais savoir si dans le cadre de votre activité professionnelle vous ressentez le souffle de ces géants du numérique.

M. Michel Paulin. - De manière quotidienne. À chacune de nos rencontres avec un client ou une collectivité territoriale, nous sommes comparés à Google. C'est donc une réalité concrète pour nous.

M. Gérard Longuet, rapporteur. - Évoquez-vous le client final ou le vendeur ?

M. Michel Paulin. - Parmi nos clients se retrouvent tous types d'acteurs. L'essentiel de notre chiffre d'affaires se fait à l'étranger. Parmi nos clients en France, on retrouve à la fois des entreprises du CAC 40 comme la Société Générale ou Auchan et de grands intégrateurs comme Capgemini ou Thalès, qui s'adressent au client final. Nous avons aussi des sociétés dites « digital native » qui ont bâti l'ensemble de leur activité autour du cloud.

En réalité, nous menons une compétition permanente avec les entreprises du numérique. Leur puissance de lobbying est particulièrement développée.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible en ligne sur le site du Sénat.

Audition de M. François Villeroy de Galhau, Gouverneur de la Banque de France,
le 11 juillet 2019

M. Franck Montaugé, président. - Notre commission d'enquête poursuit ses travaux avec l'audition de Monsieur François Villeroy de Galhau, gouverneur de la Banque de France.

Je rappelle qu'un faux témoignage devant notre commission d'enquête serait passible des peines prévues aux articles 434-13, 434-14 et 434-15 du Code pénal. Je vous invite à prêter serment de dire toute la vérité, rien que la vérité ; levez la main droite et dites : « je le jure ».

Conformément à la procédure applicable aux commissions d'enquête, M. Villeroy de Galhau prête serment.

M. le Gouverneur, avec la révolution numérique, les entreprises tentent aujourd'hui de concurrencer les États dans l'exercice de leurs missions régaliennes, y compris celle de battre monnaie. Nous le voyons aujourd'hui avec Facebook qui a confirmé son intention de lancer sa propre monnaie, le Libra, dès le début de l'année 2020.

Cette annonce a immédiatement suscité d'intenses réactions, en particulier de la part des régulateurs et des banques centrales concernés en premier lieu par ce projet. Aujourd'hui, les autorités nationales et européennes ne considèrent pas que les cryptoactifs soient de nature à perturber la stabilité de nos systèmes financiers. Le projet de Facebook ne remet-il pas cela en cause ? Nous pouvons imaginer que d'autres géants du numérique américains ou asiatiques choisiraient de développer leur propre cryptomonnaie, ce qui fragiliserait certainement notre système.

Vous défendez également, M. le Gouverneur, la solution de systèmes de paiement européens alors que ce marché est de plus en plus dominé par des acteurs américains ou chinois. En quoi est-ce un enjeu pour notre souveraineté numérique nationale ou européenne ?

Enfin, nous avons beaucoup entendu parler, lors de nos auditions, du risque cyber. Quels sont ces risques dans les domaines financier et bancaire ? Quelles actions la Banque de France a-t-elle entreprises pour protéger le système financier ?

M. François Villeroy de Galhau, Gouverneur de la Banque de France. -C'est une évidence de souligner à quel point votre enquête est primordiale tant le numérique se situe au coeur de notre système financier. Les acteurs du système financier ont été parmi les premiers à devoir opérer leur transition vers le numérique. En effet, l'ampleur des données collectées nécessite un traitement de masse., la donnée étant par ailleurs au coeur des questions que vous avez soulevées, notamment pour les systèmes de

paiement. La capacité des acteurs existants à s'adapter à cette transformation est un enjeu énorme pour leur développement économique.

Parmi les sujets que vous avez cités, vous me permettrez d'esquisser une hiérarchie. Tout d'abord, je relève un certain nombre de points très débattus dans la sphère publique, à l'instar des cryptoactifs, tandis que d'autres sont moins évoqués, mais encore plus importants à court-terme pour la souveraineté de notre pays et de l'Europe, telles la stratégie des paiements et la cybersécurité.

Commençons par le sujet le plus actuel, les cryptoactifs. En réalité, nous plaçons sous ce vocable des réalités très différentes. Derrière le phénomène des cryptoactifs, il y a une technologie prometteuse pour l'avenir : les blockchains. D'ailleurs, la Banque de France fut l'une des premières banques centrales à les expérimenter, avec les banques françaises, pour l'identifiant Single Euro Payments Aera en Espace unique de paiement en euros (SEPA). L'exploitation de cette technologie a permis l'émergence de deux catégories d'actifs : les cryptoactifs et les stable coins (« valeurs stables »).

Au sein de la première catégorie, nous retrouvons les actifs fortement spéculatifs, type bitcoin. Le G20 a estimé que ces instruments ne constituaient pas une menace pour la stabilité de la finance mondiale, en raison de leur volume limité. Pour autant, le G20 a également rappelé que nous devions rester vigilants sur la lutte contre le blanchiment d'argent et de la protection des consommateurs. Les bitcoins sont un placement très risqué, dont personne ne garantit la valeur, et ils doivent donc être réservés aux investisseurs les plus avertis.

La seconde catégorie est illustrée par le lancement du projet Libra par Facebook et ses partenaires. Le terme anglo-saxon pour qualifier le Libra est stable coins, ce que nous pourrions traduire par « valeurs stables ». Cette initiative soulève des questions très différentes pour le régulateur. Le libra, ainsi que tout autre projet de même nature, devront se plier à l'ensemble des règles applicables en matière financière, au niveau national ou international. Le libra est, en outre, encore un projet, qui suscite beaucoup d'interrogations : le libra n'est pas aujourd'hui une réalité pouvant se mettre en place librement. Afin d'analyser cette situation, un groupe de travail a été mis en place au sein du G7 et Bruno Le Maire a confié à Benoît Coeuré le soin d'établir un rapport intermédiaire, pour la réunion du G7 des ministres des finances et des gouverneurs qui se tiendra le 17 juillet, et un rapport définitif, qui sera rendu en octobre 2019.

Jerome Powell, président de la Fed, s'est exprimé hier devant le Congrès américain. Il a estimé que ce projet suscitait de sérieuses interrogations. À mon tour, j'observe effectivement que plus nous étudions le Libra, plus nous partageons cette analyse.

Selon moi, les principales questions concernent d'une part la définition du Libra et de sa valeur, et d'autre part l'usage qui en sera fait.

Le libra se distingue du bitcoin en ce qu'il ne serait pas un actif spéculatif mais posséderait une valeur définie. Reste à savoir par quel moyen. L'intention affichée est de définir la valeur par rapport à un panier de monnaies. À ce jour, nous ignorons quelles seront ces monnaies sous-jacentes. De plus, Facebook laisse entendre que la valeur ne sera pas le résultat de ce panier, mais dépendra des réserves investies par le projet Libra. Au final, ce serait donc la valeur des placements qui déterminerait celle du Libra. Même s'il s'agit de placements assez sûrs, en dépôts bancaires ou en titres obligataires, avec peu de volatilité, cela introduit une incertitude pour ceux qui y souscrivent. Par ailleurs, nous ignorons toujours si les investissements réalisés en Libra pourront être échangés à tout moment contre des monnaies « de plein exercice ».

Quelle est la finalité de ce projet ? Je ne peux que constater à quel point les ambitions affichées sont élevées, et ce à trois niveaux.

Tout d'abord, le Libra serait un moyen de paiement. Un particulier qui entrerait dans le système pourrait ainsi payer ou transférer des fonds en Libra. Au passage, je note la lourdeur et le coût des procédures de paiements transfrontières aujourd'hui, situation à laquelle nous devrions apporter des améliorations. L'utilisation du Libra comme instrument de paiement pose d'autres questions plus directes, notamment celle de la lutte anti-blanchiment. Il est hors de question que ce moyen de paiement se traduise par une régression par rapport à tous les progrès internationaux réalisés dans ce domaine. Je rappelle qu'en l'état des annonces de Facebook, les utilisateurs de Libra seraient anonymes, ce qui n'est pas concevable dans le cadre de la réglementation anti-blanchiment. De même, la question de la protection des données devra être observée de près. Les flux de données associés aux paiements sont très sensibles. Ces données seront-elles revendues ? Le libra satisfera-t-il aux exigences du RGPD ?

Ensuite, nous pouvons nous demander si le Libra ira de pair avec la proposition de services bancaires. Dans le libre blanc présenté lors de l'annonce de la Future création du Libra, il y a en effet une intention affichée d'offrir des moyens de dépôts, des instruments de placement et des crédits. La réglementation est parfaitement claire à ce sujet. Si une entreprise offre des services bancaires, elle doit détenir une licence bancaire. Cette condition est applicable dans l'ensemble des grands États. À défaut, la situation serait totalement illicite.

Enfin, l'ambition la plus forte réside dans l'affirmation selon laquelle le Libra serait une monnaie privée mondiale. Nombre d'expériences de ce type ont connu une fin malheureuse dans le passé. Sur le plan politique et démocratique, ce type d'ambition ne peut que susciter une attitude de méfiance. La mission monétaire a été confiée aux banques centrales par le

législateur et les banques centrales sont comptables de leurs résultats. Je rappelle que la monnaie est un bien public chargé d'assurer trois fonctions : c'est un moyen de paiement, une unité de valeur reconnue par tous et une réserve de valeur. À ce stade, le Libra ne présente aucune de ces trois fonctions.

M. Gérard Longuet, rapporteur. - Comment analysez-vous la démarche de Facebook ? Est-ce une stratégie de communication visant à engager des négociations ou plutôt une provocation qui restera sans effet réel ?

Vous avez évoqué la technologie des blockchains. Pouvez-vous nous expliquer comment elle fonctionne ? Quel est son objectif ?

Je vous rejoins dans votre distinction entre les instruments spéculatifs de type bitcoins et ceux plus stables de type Libra. Malgré tout, les deux posent la question de l'économie du jeton. Aujourd'hui, l'économie numérique présente une apparente gratuité alors même que les données des utilisateurs sont commercialisées. Dans ce contexte, nous pourrions imaginer que les utilisateurs seraient prêts à payer pour utiliser des jetons, plus simples que des cartes de crédit. Qu'en pensez-vous ? Serait-ce utile ? Y aurait-il une régulation à envisager ?

M. Franck Montaugé, président. - J'aimerais aussi que vous reveniez sur les solutions de paiement européen et sur la question de la cybersécurité.

M. Villeroy de Galhau. - Je ne suis pas le plus qualifié pour me prononcer au sujet des intentions de Facebook. Je partage bien volontiers les deux hypothèses que vous avez proposées. Ce projet a aussi une rationalité économique ; il permettrait à Facebook de dépasser son coeur de métier - les réseaux sociaux - domaine qui rencontre aujourd'hui ses limites. Certains évoquent également le fait que ce projet permettrait de collecter davantage de données, qui seraient ensuite monétisées et commercialisées La question reste donc ouverte à ce jour. Dans notre dialogue avec Facebook, nous devrons aborder ces différents points sans faire preuve de naïveté. Ce projet n'est pas seulement guidé par la recherche du bien commun, il répond aussi à des intérêts privés.

Les blockchains sont une technologie de registre distribué qui permet de remplacer certains tiers de confiance, de partager des informations ou de réaliser des transactions dans des conditions beaucoup plus rapides, économiques et sûres.. La sécurité du système repose sur la production d'algorithmes, rémunérée par l'octroi de bitcoins. Dans les blockchains publics, nous ne recourons pas à des bitcoins, mais le principe reste le même. Reste à déterminer quelle est la capacité de cette technologie à supporter un très grand nombre de transactions. En effet, à ce jour, son utilisation reste limitée à des transactions peu nombreuses. Attention, la blockchain n'est pas consubstantielle au libra.

Pour aborder les enjeux de l'économie du jeton, nous devons malheureusement utiliser des termes anglais. Il en existe deux majeurs : le coin que nous traduisons par « unité » et le token, par « jeton ». Selon moi, une meilleure traduction de token pourrait être « certificat ». En réalité, le token est un coin plus un service associé, avec un contenu d'informations. La grande question est donc de savoir si les transactions en jetons peuvent attirer les particuliers et les entreprises à l'avenir. Si je m'en tiens à la fonction paiement, je pense que deux questions majeures se dégagent.

D'une part, l'apparition des jetons, ou certificats, interroge sur nos systèmes de paiement. À ce jour, le système européen de paiement fonctionne bien, par exemple grâce au système TIPS. Pour autant, dès que nous sortons de l'Europe, les systèmes de paiement sont lents, coûteux et parfois indisponibles. C'est le premier défi auquel ces jetons renvoient.

D'autre part, les jetons nous ramènent au débat sur la création d'une monnaie digitale de banque centrale. Jusqu'à présent, la monnaie des banques centrales accessible était le billet de banque. Malgré notre attachement à celui-ci, nous constatons une nette diminution de son usage. Le pays qui se distingue particulièrement à ce niveau en Europe est la Suède. La part des transactions en espèces y est tombée entre 10 et-20 %, contre 60 % en France. De ce fait, la Banque de Suède se penche sur la mise au point d'une e-couronne, une monnaie banque centrale offrant la même garantie aux Suédois que les billets. Or, si on prend le libra, on a le « risque Facebook », l'entreprise peut faire faillite. Le propre d'une monnaie souveraine est au contraire d'avoir la garantie la plus forte qui soit, celle de la banque centrale et de l'autorité publique qui est derrière. Au sein de la zone euro, nous n'en sommes pas à ce stade. Pour autant, s'il y a un attrait pour le Libra, cela pourrait nous convaincre d'approfondir nos réflexions sur ce sujet.

Par ailleurs, j'ai effectivement proposé de mettre en place une stratégie européenne des paiements. Ce sujet est moins hypothétique, c'est aujourd'hui une réalité. Les acteurs financiers sont les opérateurs traditionnels du paiement. Jusqu'à présent, c'était plutôt considéré comme une simple activité d'intendance. Désormais, avec l'entrée de grands acteurs du digital, américains ou chinois, sur ce marché, ce secteur se transforme en profondeur. Ces acteurs peuvent entrer dans la sphère financière via les paiements. Ils ont d'ailleurs commencé à le faire, avec des projets tels que Apple Pay, Ali Pay ou certains services proposés par Amazon. Ils entrent donc par le biais des systèmes de paiement dans ce secteur car les barrières à l'entrée sont peu nombreuses et la régulation, notamment en matière de capitaux, moins exigeante que pour les activités bancaires « pleines ». Cette activité génère en outre deux « trésors » : la récupération de données et la relation clients. Leur intérêt économique certain représente une incitation forte à entrer sur le secteur des paiements.

À l'heure actuelle, l'Europe s'est dotée d'une solution pour les paiements transfrontières instantanés avec le système TIPS, sous l'égide de la

Banque centrale européenne (BCE). Pour autant, je déplore que nous ne disposions pas de grandes entreprises digitales européennes pour proposer des solutions de paiement européennes, alors qu'elles sont encore, en large partie, nationales. Pour rattraper ce retard, le temps nous est compté. À défaut, ce seront encore une fois les grands acteurs internationaux qui domineront ce marché, au détriment des acteurs européens. Selon moi, il ne nous reste qu'un à deux ans, avant qu'il ne soit trop tard pour être présent sur ce marché stratégique crucial. Une stratégie européenne des paiements doit reposer sur une consolidation des schémas nationaux existants, sur l'utilisation de TIPS et, éventuellement, de nouvelles technologies, sur une marque commune de paiements et sur une politique des données bien définie (localisation, protection, accès).

M. Franck Montaugé, président. - Que pouvez-vous nous dire sur la cybersécurité dans le secteur bancaire ?

M. Villeroy de Galhau. - Il s'agit d'un autre enjeu majeur de notre époque et d'une menace déjà existante. Nous incluons la cybersécurité dans nos contrôles et dans notre supervision des établissements financiers : cela fait partie des risques opérationnels. La première ligne de défense face aux cyberattaques réside dans les institutions financières elles-mêmes. Il en est de même pour les banques centrales.

Notre mobilisation est très forte sur ces sujets : investissements, constitution d'équipes spécialisées, schémas de simulation d'attaques en interne.... Je le dis avec prudence mais fierté : si certaines banques centrales étrangères ont été visées par des attaques graves, à l'instar de la Banque centrale du Bangladesh en 2016, il n'y a pas eu à la Banque de France d'attaques cyber ayant eu la moindre conséquence.

Pour autant, cela ne saurait suffire. Il est hors de question que nous relâchions notre vigilance à l'avenir. La menace ne cesse de s'amplifier à une vitesse et dans des proportions plus élevées que nos efforts visant à la contrer. De même, autant les efforts nationaux se sont accrus, autant la coopération entre États reste perfectible. C'est même notre point faible.

La Banque de France a coordonné le premier exercice de simulation de crise en juin 2019, exercice qui a réuni les banques centrales, les autorités financières et des acteurs financiers des pays du G7. Cet exercice de trois jours fut riche d'enseignements. Il s'agissait moins de savoir comment éviter une crise que d'apprendre à la gérer. Nous proposons qu'une telle expérience soit réitérée et pérennisée.

En outre, si nous avons réalisé des progrès en matière de partage d'informations sur les crises, (par exemple sur les modalités de repérage et de déclaration des incidents), nous devons encore progresser sur la catégorisation des incidents. C'est un sujet sensible : le partage des informations ne peut se faire qu'au sein de cercles limités, comme le G7. Pour

partager des informations, nous devons en effet partager un langage commun, notamment sur la gravité des incidents.

Concernant les règles encadrant la sécurité des établissements bancaires et des compagnies d'assurance, leur rédaction mériterait d'être harmonisée et complétée. Depuis la crise financière, nous avons porté toute notre attention sur les risques financiers. Il est temps de nous tourner également vers les risques technologiques qui sont une priorité. Le Comité de Bâle doit pouvoir mener les travaux dans ce domaine.

M. Gérard Longuet, rapporteur. -Deux questions de nature plus prospective : d'une part, comment les banques parviennent-elles à gagner de l'argent avec des taux d'intérêt si bas ? D'autre part, comment est-ce possible d'assurer un service de paiement coûteux pour les opérateurs sans que l'utilisateur paie ce service ?

Face aux établissements financiers qui sont des acteurs naturels de ce marché se trouvent des compétiteurs nouveaux qui ont un contact direct avec des centaines de millions, voire des milliards d'individus. Le coût additionnel de la fonction paiement resterait marginal dans leur activité, tout en créant pour eux une valeur nouvelle. La vente de données générerait pour eux des recettes dont les acteurs traditionnels ne bénéficient pas pour compenser leurs investissements. Cela crée donc un déséquilibre structurel.

M. François Villeroy de Galhau. - Quand nous sommes en dessous de la cible d'inflation de 2 %, objectif inscrit dans le mandat qui nous a été confié, il est de notre devoir d'y répondre, par des politiques monétaires accommodantes. L'inflation tardant à repartir, ces politiques ont été prolongées. Le niveau historiquement bas des taux d'intérêt découle de ce mandat. Malgré tout, je suis attentif aux effets de cette politique sur les banques. Si les établissements bancaires ne relèvent que les conséquences négatives de cette politique, je tiens à en souligner les effets positifs que sont le soutien à la croissance et donc à l'activité des banques d'une part, et la diminution de la charge du risque d'autre part. Il est vrai que si cette politique venait à perdurer, ses effets négatifs prendraient sans doute le dessus sur ses effets positifs. Le débat qui est devant nous est donc celui d'éventuelles mesures d'atténuation des effets des taux bas sur les banques commerciales.

S'agissant des paiements, je tiens à nuancer les positions exprimées. Aujourd'hui, pour les banques et pour les acteurs traditionnels, cette fonction induit le paiement d'une cotisation par titulaire du compte et d'une commission par le commerçant ; De plus, l'activité de paiement rapporte également des profits importants grâce aux comptes de dépôt associés.

Il est possible que les nouveaux acteurs entrant sur ce marché se présentent avec un modèle économique radicalement différent. Ils recherchent avant tout les « trésors » que j'évoquais précédemment, à savoir les données et la relation avec les clients. En cela, la vraie valeur des

paiements est moins la captation des profits attachés à ce service que la captation des données. Cette évolution nous offre un défi à relever. Pour ce faire, je le répète, nous ne disposons que de peu de temps pour développer une politique européenne sur cette activité totalement stratégique. Soit l'Union européenne se mobilise rapidement, soit nous ne serons que des simples consommateurs de services produits par d'autres. J'appelle de mes voeux le développement d'une stratégie européenne des paiements.

M. Franck Montaugé, président. -Le sujet de la souveraineté numérique renvoie naturellement à celui du développement de l'intelligence artificielle ou du deep learning. Considérez-vous que es moyens soient suffisants pour développer des outils en mesure de nous aider à prévenir les crises financières ? Pouvons-nous espérer des progrès dans ce domaine, que ce soit dans la manière d'observer les mouvements du marché ou d'analyser les risques afférents ?

M. Villeroy de Galhau. - C'est une question très importante qui appelle deux niveaux de réponse. Tout d'abord, je pense que la révolution numérique est centrale pour les banques, et ce pour chacune de leurs activités. Une banque qui n'investirait pas massivement dans ces outils serait condamnée à sortir du jeu. Je me réjouis de constater que la quasi-totalité des banques françaises a su prendre la mesure de ce tournant et investir massivement. En effet, pour un acteur installé, il est parfois plus délicat d'opérer une telle transition que de lancer un nouveau système.

Ensuite, je tiens à insister sur la nécessité de porter une attention particulière à l'utilisation des algorithmes. Certes, l'intelligence artificielle peut aider à mieux analyser certaines situations et repérer des anomalies, mais elle ne pourra en aucun cas remplacer le jugement d'un être humain, la gouvernance ou l'analyse des risques. Je ne crois absolument pas qu'un algorithme sera à même de faire seul de la prévision. Il peut constituer un support, mais les données devront malgré tout être analysées par un expert.

Ainsi, les indicateurs délivrent fréquemment des faux négatifs et des faux positifs. Il est très heureux de disposer de ces indicateurs, mais seul un jugement collectif, éclairé par l'expérience et les compétences permettra de les utiliser au mieux. Les autorités publiques ne prétendent pas être omniscientes : elles reçoivent une mission, elles doivent rendre des comptes et elles exercent leur responsabilité de manière transparente. L'analyse doit se faire en ayant pleinement conscience de la responsabilité qu'elle induit. De ce point de vue-là, aucun projet privé ne me semble pouvoir être équivalent aux fonctions des banques centrales.

M. Franck Montaugé, président. - Je constate avec plaisir qu'il reste donc une place pour l'être humain dans ce système.

M. François Villeroy de Galhau. - Beaucoup de ces techniques constituent toutefois de véritables progrès.

M. Gérard Longuet, rapporteur. - Nous allons prochainement recevoir les représentants de Facebook dans notre commission. Nous ne manquerons pas de leur poser les questions ici soulevées.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible en ligne sur le site du Sénat.

Audition de MM. Laurent Giovachini, pour le « Comité souveraineté et sécurité des entreprises françaises » du Medef et Christian Nibourel du MEDEF,
le 17 juillet 2019

M. Franck Montaugé, président. - Notre commission d'enquête poursuit ses travaux avec l'audition de MM. Laurent Giovachini et Christian Nibourel. Monsieur Giovachini, vous présidez la Fédération Syntec, dont est membre le plus important syndicat professionnel du secteur du numérique, le Syntec numérique ; vous êtes également à la tête du comité sécurité et souveraineté économiques des entreprises du Medef. Monsieur Nibourel, vous présidez le groupement des professions de services et la commission mutations technologiques et impacts sociétaux du Medef. Votre audition est diffusée en direct sur le site Internet du Sénat ; elle fera également l'objet d'un compte rendu publié.

Un faux témoignage devant notre commission d'enquête serait passible des peines prévues aux articles 434-13, 434-14 et 434-15 du code pénal. Je vous invite à prêter serment de dire toute la vérité, rien que la vérité, levez la main droite et dites : « Je le jure ».

Conformément à la procédure applicable aux commissions d'enquête, MM. Laurent Giovachini et Christian Nibourel prêtent serment.

M. Franck Montaugé, président. - Une personne auditionnée par notre commission d'enquête a souligné que le monde de l'entreprise avait sa part de responsabilité dans la compétition technologique en cours, et qu'il pouvait contribuer à éviter que la France et l'Europe ne soient réduites à un simple terrain d'opposition entre la Chine et les États-Unis. Il s'agissait d'un appel à davantage de patriotisme économique, afin que les entreprises concourent à la puissance de la France et de l'Europe en conquérant de nouveaux marchés.

La création d'un comité sécurité et souveraineté économiques au sein du Medef semble envoyer un signal en ce sens. Monsieur Giovachini, vous vous êtes d'ailleurs exprimé clairement sur ce point dans une interview, dans laquelle vous déclariez que « pour créer des GAFA européens, il faut que se conjuguent volonté politique et volonté des entreprises. Ces dernières ne peuvent pas s'exonérer de participer à l'effort de reconquête ».

Comment appréhendez-vous la notion de souveraineté numérique et quelle est la situation de notre pays dans ce domaine ? Que faire pour que la France recouvre sa souveraineté dans le monde numérique ?

M. Laurent Giovachini, président du comité souveraineté et sécurité économiques des entreprises françaises du Medef et de la Fédération Syntec. - Nous sommes heureux d'avoir l'opportunité de vous

présenter la position du Medef sur la souveraineté numérique pour le monde économique.

Le Medef représente 170 000 entreprises adhérentes, d'une taille moyenne de quarante-sept salariés, au travers de soixante-dix-huit fédérations sectorielles et d'une centaine de Medef territoriaux. J'exerce, pour ma part, les fonctions de directeur général adjoint de Sopra Steria, entreprise française parmi les leaders européens de la transformation digitale, qui compte plus de 45 000 collaborateurs dans vingt-cinq pays et qui réalise un chiffre d'affaires supérieur à milliards d'euros. Je préside également la fédération Syntec qui regroupe, dans ses syndicats affiliés, des sociétés françaises spécialisées dans les domaines de l'ingénierie, du numérique, du conseil, de la formation professionnelle et de l'événement. Les 80 000 entreprises que nous représentons dans notre branche emploient environ un million de salariés et affichent un chiffre d'affaires total de 120 milliards d'euros. Je suis enfin président du comité souveraineté et sécurité économiques des entreprises du Medef, que Geoffroy Roux de Bézieux a souhaité créer au début de l'année 2019 pour renforcer la mobilisation des entreprises en la matière. De fait, les années passées dans le secteur public, à la délégation générale pour l'armement puis en cabinet auprès du Premier ministre, Lionel Jospin, m'ont permis de développer une expertise des problématiques de souveraineté.

La création d'un tel comité peut paraître à certains contradictoire avec la veine traditionnellement libérale du Medef, mais il convient de ne pas confondre libéralisme et naïveté et de tirer les enseignements de l'insuffisance des règles qui ont accompagné la libéralisation des marchés en Europe. Nous sommes confrontés à un contexte de tensions économiques internationales et de rivalité accrue entre les nations, avec t des conséquences lourdes sur l'activité des entreprises, qui se trouvent au coeur des enjeux de souveraineté économique. Les entreprises doivent, comme l'État, s'engager pour les protéger cette souveraineté économique. À défaut, le tissu économique français et européen pourrait être constitué, à l'avenir, soit de filiales de groupes extra-européens, soit d'entreprises de services de proximité. Si la réponse au défi de la souveraineté économique et numérique relève du politique, les entreprises portent également une responsabilité. De leur engagement dépend la capacité de l'économie française à créer et à développer des activités et des emplois durables.

Il existe une ligne de crête entre l'attractivité de la France et la souveraineté économique : nous devons demeurer un pays attractif, tout en conservant notre souveraineté, entendue comme la capacité de disposer d'une autonomie d'appréciation des situations, de décision et d'action. Le Medef souhaite jouer un rôle de sensibilisation et proposer des recommandations sur les enjeux liés à la souveraineté économique et numérique. Il faut que la France et l'Europe se dotent des outils, notamment juridiques, financiers et technologiques, pour préserver notre compétitivité

et assurer des emplois durables. Nous devons bénéficier d'un cadre réglementaire préservant notre capacité à décider en toute autonomie. Il s'agit d'éviter les situations d'ingérence et de déstabilisation économique, comme les prises de contrôle par des investisseurs étrangers, de lutter contre l'extraterritorialité du droit, notamment américain, l'espionnage économique et industriel et l'action de certains fonds activistes. Le développement d'une culture de la sécurité économique et numérique au sein des entreprises paraît également indispensable.

Notre action vise un double objectif. D'une part, nous devons réinventer et densifier le partenariat entre les entreprises et le secteur public, y compris avec la délégation générale des entreprises, l'Anssi, le SGDSN, les services de renseignement. L'administration a conservé une terminologie pudique avec son service de l'information stratégique et de la sécurité économiques (SISSE), alors que nous osons le terme de souveraineté. D'autre part, il nous revient de mobiliser nos homologues européens, à commencer par la fédération de l'industrie allemande (BDI), car seule sera efficace une action forte et cohérente menée au niveau de l'Union européenne.

M. Christian Nibourel, président du groupement de professions de services et de la commission mutations technologiques et impacts sociaux du Medef. - Outre mes fonctions de président de la commission mutations technologiques et impact sociaux et du groupement des professions de services, je préside l'institut national des sciences appliquées (INSA) de Lyon. Jusqu'au mois de janvier, je présidais également Accenture France Benelux.

Nos adhérents expriment une demande forte de décryptage de l'impact des mutations technologiques sur l'activité des entreprises et sur la transformation de la société, notamment sur les nouvelles formes de travail. Leurs inquiétudes portent également sur l'éthique, sur la protection des données et sur la consommation d'énergie induite par les technologies numériques. Le Medef a créé, pour y répondre, la commission que je préside. L'accélération des transformations numériques oblige les entreprises à travailler différemment. En ce sens, la souveraineté numérique peut être définie comme la capacité des entreprises à s'adapter et à demeurer maîtresses de leur destin et de leur développement économique et social, tout en respectant les valeurs européennes. Cela passera non pas par une copie de ce qui a déjà été fait, mais par notre faculté à innover, notamment dans les domaines de la blockchain, de la cybersécurité, de l'intelligence artificielle, de l'ordinateur quantique et du cloud souverain. Nous devons également remporter la bataille des standards et des normes, essentiels en matière de transparence et d'interopérabilité. Face à l'enjeu numérique, le Medef pousse aussi à une meilleure organisation des entreprises européennes entre elles.

Notre commission a pour mission de faire prendre conscience aux entreprises des bouleversements des modèles économiques et sociaux

induits pas le numérique et de la nécessité qu'elles participent à la construction de la réglementation. La cybersécurité représente un catalyseur fort du développement du numérique, de la sécurité et de la souveraineté : nous devons prendre de l'avance dans ce domaine pour ne pas perdre la bataille de la souveraineté. Nous en avons les moyens.

M. Gérard Longuet, rapporteur. - Le droit européen de la concurrence donne l'impression de favoriser le consommateur au détriment du producteur, en recherchant l'augmentation du pouvoir d'achat par la baisse des prix, par le jeu d'une concurrence forte. Il n'y a qu'à voir le secteur des télécoms... En outre, chaque État membre défend ses consommateurs en abandonnant les producteurs des autres pays européens. Dès lors, l'Union européenne se trouve dans l'incapacité de faire émerger des champions européens. Comment envisageriez-vous un droit de la concurrence plus réaliste ?

L'échec, en France, d'un cloud souverain s'explique par diverses raisons. Si les entreprises préfèrent les meilleures technologies au meilleur prix, elles n'ont pas vocation à financer l'indépendance européenne. Quid cependant de la protection de leurs données ? Quelles sont les conséquences juridiques du Cloud Act ?

Votre commission tente de convaincre les chefs d'entreprise qui n'ont pas encore perçu toute l'importance de la numérisation de leur activité. Certains en sont évidemment conscients, mais beaucoup proposent un service minimum en la matière, estimant que le numérique est avant tout une affaire de spécialistes. Que pensez-vous de l'initiative de notre collègue député Cédric Villani qui recommandait, dans son rapport sur l'intelligence artificielle, que les entreprises soient aidées pour mutualiser leurs données ? Vous semble-t-elle crédible?

Mme Martine Filleul. - Vous avez tous les deux évoqué la nécessité de travailler à l'échelle européenne pour favoriser le travail partenarial. Où en êtes-vous de cette volonté fédérative ? Avez-vous reçu partout le même accueil ?

M. Stéphane Piednoir. - Certains employés des entreprises du Syntec s'inquiètent-ils de l'utilisation des données possédées par ces entreprises à leur sujet ?

M. Franck Montaugé, président. - Êtes-vous favorables à l'extension du règlement général sur la protection des données (RGPD) aux données détenues par les entreprises ?

M. Laurent Giovachini. - Le droit de la concurrence en Europe est un sujet très important. Avec le comité souveraineté et sécurité des entreprises du Medef, nous en avons débattu franchement avec Mme Margrethe Vestager - c'était au moment de la décision de la Commission européenne sur la fusion Alstom-Siemens. Je lui ai dit qu'Airbus, entre ses mains, n'aurait peut-être pas abouti au même résultat...

À titre personnel, je suis favorable à ce qu', à côté de la direction générale concurrence, émerge une préoccupation pour la politique industrielle européenne, non seulement portée politiquement, mais aussi par l'administration bruxelloise. Ceci garantirait un meilleur équilibre dans l'instruction des dossiers. Nous étions les troisièmes interlocuteurs de la commissaire à lui parler de « champions européens » cette semaine-là, après le Premier ministre et Bruno Le Maire ; n'ayons pas peur de défendre cette idée !

Nous avons fait des propositions sur le cadre européen de la concurrence. Dans une Europe qui protège, il faut moderniser les principes et les règles du droit de la concurrence pour favoriser le rapprochement entre les entreprises européennes, renforcer notre système de production autour de champions européens ; rationaliser les règles des aides d'État afin de dynamiser l'investissement et répondre aux grands défis stratégiques - révolution technologique, recherche, innovation, durabilité... ; mettre en place un cadre commun afin de permettre aux États membres d'intervenir dans les secteurs stratégiques dès que des initiatives conduites par des opérateurs de pays tiers ne garantissent pas les règles de réciprocité. Vous avez vu le règlement européen sur le filtrage des investissements étrangers auquel le Parlement européen a donné son feu vert en février dernier. Désormais, il prévoit une obligation d'information mutuelle sur les opérations d'investissement extra-européen dont les États ou leurs entreprises font l'objet.

Nous devons agir pour une réforme en profondeur de l'Organisation mondiale du commerce (OMC) et instaurer des règles internationales pour combattre les pratiques anticoncurrentielles ou hors marché - c'est la notion de level playing field - afin que nos entreprises ne soient pas désavantagées par des règles européennes plus exigeantes que celles auxquelles nos concurrents sont soumis. Nous devons bâtir un agenda de négociations pour progresser sur le régime des échanges mondiaux, la sécurité internationale et la prospérité de l'économie mondiale. J'insiste sur ce nécessaire équilibre à Bruxelles entre la concurrence et la politique industrielle.

M. Gérard Longuet, rapporteur. - Y a-t-il une prise de conscience des entreprises françaises sur le fait qu'avec le Cloud Act, leurs données peuvent être stockées dans des centres de données aux États-Unis ou propriété d'entreprises américaines, et donc susceptibles d'être transférées à la justice américaine pour différentes raisons, parfois surprenantes ?

M. Christian Nibourel. - Il y a une prise de conscience, surtout dans les grandes entreprises, notamment après le RGPD. Nous devons soutenir des solutions juridiques, dont certaines existent déjà au travers de ce règlement. Il faut aussi réduire les risques pour les entreprises, qui ne savent pas toujours que la justice américaine peut aller chercher des données dans ces clouds. Il y a une déconnexion entre la réglementation française et le

Cloud Act. La réponse devra être européenne avec de nouvelles réglementations.

Nous devons être prudents sur un futur RGPD des entreprises et sur la mutualisation des données d'entreprises, certaines données stratégiques sont le savoir-faire, la propriété de l'entreprise - il ne faudrait donc pas les divulguer. Avant de se poser la question de leur mutualisation, il faudrait segmenter les données. Le Health Data Hub va être bientôt créé, on en voit l'intérêt. C'est une solution d'avenir.

Si nous voulons devenir des leaders européens dans un certain nombre de domaines d'innovation, il faut un pilotage de l'innovation de rupture au niveau européen et prendre en compte la composante temps. Les innovations vont très vite. Il faut une vision et une permanence dans nos investissements, tout en étant capable de changer de cap rapidement pour pouvoir répondre aux nouvelles innovations.

Nous pouvons décider, par exemple dans la cybersécurité, avoir perdu la bataille du cloud, mais vouloir gagner la bataille des bases de données réparties, le edge computing.

Ne vaut-il pas mieux investir dans des start-up françaises ou européennes pour en faire des licornes, en travaillant sur des bases de données moins importantes pour entraîner les algorithmes ? Certains ingénieurs travaillent sur des technologies aboutissant aux mêmes résultats avec dix fois moins de données, en changeant la manière de développer les algorithmes. Nous pouvons prendre ce leadership, tout en sachant que, de toute façon, nous ne pourrons pas concurrencer les énormes bases de données. Nous pouvons aussi prendre le leadership d'une blockchain moins consommatrice d'énergie.

Avec le web sémantique, la donnée circule uniquement en fonction du besoin de calcul, mais reste la propriété du producteur. Il faut aller vers ce modèle : nous n'arriverons pas à copier les grands modèles américains, nous sommes trop en retard. Il vaut mieux se concentrer sur les futurs modèles. Actuellement, 80 % des données sont sur le cloud, 20 % sur le device. Demain, nous inverserons ce rapport. Nous avons besoin d'une organisation, d'un pilotage de l'innovation de rupture pour prendre de l'avance et s'affranchir de ces clouds.

M. Laurent Giovachini. - Si nous voulons être présents sur la prochaine vague de la révolution numérique, nous devons le faire à l'échelle européenne.

Nous avons la chance d'avoir en Europe un tissu industriel non négligeable, avec des grandes entreprises comme Thalès, de grandes sociétés de services du numérique - ex-SSII - comme Capgemini, Atos, Sopra Steria, des grands éditeurs de logiciels comme SAP en Allemagne ou Dassault Systèmes en France ; nous ne sommes pas démunis. Nous avons des start-up,

mais, dans 80 % à 90 % des cas, elles sont rachetées pour devenir des sous-ensembles de grands groupes extraeuropéens.

En France, mais probablement aussi en Europe, nous devons faire en sorte que nos impôts, qui paient un appareil de formation qui reste l'un des meilleurs du monde avec des universités et des grandes écoles de qualité, ne conduisent pas à ce que les élèves de ces écoles aillent directement dans des GAFA ou dans des start-up intégrées dans ces entreprises quelques années après leur création... Nous avons des grandes entreprises industrielles, des grands éditeurs de logiciels mais, l'innovation technologique, l'innovation d'usage, qui vient des start-up, est bien souvent captée par des intérêts extra-européens. Il y a vingt ans, les banques américaines et britanniques débauchaient nos polytechniciens pour créer leurs produits structurés. Désormais, ce sont des sociétés comme Palantir Technologies qui captent nos meilleurs cerveaux.

Nous devons proposer des moyens publics et privés, non pour refaire ce qui n'a pas marché, comme le Plan calcul, mais pour que ces jeunes talents aient des débouchés européens. C'est ce qui manque actuellement. C'est une responsabilité partagée de l'État, et des entreprises.

L'Europe a réussi avec le RGPD à créer, sans le vouloir, un instrument à portée extraterritoriale qui défend nos valeurs. C'est donc possible. Certes, cela ennuie les entreprises et cela a un coût. Mais l'avantage, c'est que nos entreprises sont dans le continent où ce règlement a été conçu, elles ont donc un temps d'avance, alors que lorsque nous transposons des normes étrangères, et notamment américaines, nous avons deux temps de retard par rapport à nos concurrents. Nous pouvons être en avance sur les normes mondiales.

M. Gérard Longuet, rapporteur. - Je partage totalement vos orientations, mais il y a des difficultés propres au système européen.

Le marché des capitaux à risque est plus étroit en Europe qu'aux États-Unis pour des raisons structurelles, notamment du fait de la gestion du risque vieillesse. Comment pourrait-on faire basculer ce point rapidement ?

La coopération est difficile entre les entreprises nouvelles, les entreprises existantes et les pouvoirs publics, qui ont un rythme de décision lent, avec des étapes complexes et nécessairement nombreuses. Parfois, cela aboutit à vulgariser une idée, un comble pour l'entreprise qui pensait avoir un avantage sur ses concurrents !

Une start-up ne doit pas être privée de la possibilité d'optimiser son innovation. Si on lui dit qu'elle ne pourra pas vendre à celui qui lui propose le meilleur prix, elle ira ailleurs. Sans parler des solutions, pensez-vous que vos interlocuteurs publics sont conscients du problème ?

M. Laurent Giovachini. - De plus en plus ! Nous devons être conscients que le capitalisme français avait réussi une sorte de tour de force : utiliser l'argent étranger pour construire de grandes entreprises nationales.

M. Gérard Longuet, rapporteur. - Les fonds de pension californiens sont en effet très présents dans les entreprises du CAC 40 !

M. Laurent Giovachini. - Oui, mais les centres de décision restaient en France. Or nous devons être vigilants quant à l'équilibre des pouvoirs entre les conseils d'administration et les assemblées générales. Les choses sont plus compliquées aujourd'hui pour les start-up.

En ce qui concerne la coopération avec les pouvoirs publics, il y a une réelle prise de conscience, mais il faudrait que les mécanismes européens, a minima franco-allemands, soient à la hauteur et que les initiatives étatiques s'inscrivent dans la durée. Les entreprises ont parfois l'impression que chaque nouveau gouvernement, voire chaque nouveau ministre, veut tout réinventer et abandonner ce qui avait été fait précédemment ; certes, les intentions sont bonnes, mais nous avons besoin de stabilité. Devrions-nous aller vers une loi de programmation du numérique, dispositif qui a fonctionné dans le domaine de la défense ? En tout cas, les dispositifs publics doivent dépasser les alternances et les changements de ministre.

Quand je parle de naïveté, je pense aussi au fait que, dans les autres pays - aux États-Unis, en Chine, en Israël -, les start-up ou les licornes placent dans leurs conseils d'administration d'anciens hauts responsables de l'État, souvent issus des services de renseignement, alors que nous, nous mettons d'abord en avant les questions déontologiques ou de pantouflage... Ces restrictions sont légitimes, mais nous devons aussi être conscients de notre environnement et de la manière dont nos concurrents fonctionnent, c'est-à-dire en travaillant de manière étroite avec les services de renseignement de leurs Etats.

M. Christian Nibourel. - Le numérique n'est pas un secteur isolé ; au contraire, il est transversal. Sur le marché européen, la coexistence de vingt-huit législations différentes en termes de fiscalité ou de marché du travail est pénalisante.

Nous avons également tendance à trop raisonner en silo et à ne pas persévérer en matière d'investissements et de priorités. Nous devrions au contraire réfléchir de manière globale. Les innovations de rupture nécessitent un travail collectif entre le monde universitaire, le secteur économique, les start-up, les fonds, etc. C'est cet ensemble qui crée une dynamique. Les Britanniques vont dans ce sens, puisqu'ils sont en train de définir un espace commun de travail sur la cybersécurité. Pour tenir le rythme de l'innovation, nous avons par exemple besoin de doctorants.

Il est vrai que la France ne dispose que de deux fonds spécialisés en cybersécurité, mais la question est plus globale, ce n'est pas une mesure qui

va tout changer, et le monde universitaire n'a pas vraiment fait sa révolution en la matière. Attention, ne prenons pas trois ans pour réfléchir à la question... Ce serait trop tard ! Nous avons besoin de tous ces changements aujourd'hui.

Je le redis, il faut sortir du phénomène de silo, décloisonner, avoir une vision pérenne et globale à même de faire naître les grandes entreprises dont nous avons besoin. Il est vrai aussi que, dans le passé, la commande publique a facilité certaines évolutions.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible en ligne sur le site du Sénat.

Audition de M. Loïc Rivière, Délégué général de Tech in France,
le 17 juillet 2019

M. Franck Montaugé, président. - Mes chers collègues, notre commission d'enquête poursuit ses travaux avec l'audition de M. Loïc Rivière, délégué général de Tech in France. Cette audition est diffusée en direct sur le site internet du Sénat ; elle fera également l'objet d'un compte rendu qui sera publié.

Un faux témoignage devant notre commission d'enquête serait passible des peines prévues aux articles 434-13, 434-14 et 434-15 du code pénal.

Conformément à la procédure applicable aux commissions d'enquête, M. Loïc Rivière prête serment.

M. Franck Montaugé, président. - Créé en 2005 sous le nom d'Association française des éditeurs de logiciels et solutions internet, Tech in France revendique aujourd'hui 400 adhérents dans le secteur du numérique, dont 80 % de PME, mais également des géants du numérique comme Google et Facebook. Vous nous rappellerez rapidement l'état de vos relations avec le Medef.

L'une des personnes auditionnées par notre commission a souligné la très grande responsabilité du monde de l'entreprise dans le fait que la France et l'Europe ne soient pas réduites à un simple terrain d'opposition entre la Chine et les États-Unis dans la compétition technologique qui les oppose. Il s'agissait en fait d'un appel à davantage de patriotisme économique afin que le monde de l'entreprise concoure à la puissance de la France et de l'Europe, en conquérant de nouveaux marchés. Que pensez-vous de cet appel ?

Comment appréhendez-vous la notion de souveraineté numérique et comment appréciez-vous la situation de notre pays?

Le rôle d'une commission d'enquête étant également de savoir si les politiques publiques engagées aujourd'hui vont dans la bonne direction, je vous invite à nous expliquer ce qui, selon vous, reste à faire pour que la France recouvre sa souveraineté dans le monde numérique.

M. Loïc Rivière, délégué général de Tech in France. -Je tiens tout d'abord à souligner que nous représentons aussi des champions nationaux comme Dassault Systèmes, Criteo ou Cegid. Tech in France est membre d'une fédération professionnelle, la fédération des industries électriques, électroniques et de communication (FIEEC), qui est elle-même adhérente du Medef. Nous participons donc régulièrement aux travaux du Medef.

Sur le fond, l'expression « souveraineté numérique » est large et il en existe plusieurs définitions. C'est pourquoi je voudrais circonscrire le sujet.

Dans le domaine numérique, la souveraineté est la capacité de « se gouverner » seul. Pour un individu, il s'agit du contrôle des données personnelles. J'imagine que votre commission d'enquête s'intéresse aussi au fait que la souveraineté numérique peut croiser la notion de souveraineté nationale.

Aucun État n'est strictement souverain. La souveraineté est un objectif, et nous dépendons des autres pour la mettre en oeuvre. Il existe ainsi de nombreux sujets qui font l'objet d'une gouvernance partagée et qui trouvent des réponses par le multilatéralisme. La France s'inscrit d'ailleurs historiquement dans ce mouvement.

Le monde numérique est un monde de communication, donc d'interdépendance, ce qui entraîne d'ailleurs une certaine contradiction avec l'expression « souveraineté numérique ». Je le redis, le numérique, c'est, par définition, la communication, l'interdépendance - on parle d'ailleurs souvent d'effets de réseau. La digitalisation de nos sociétés et de nos économies crée de plus en plus d'interdépendances. Le Président de la République, Emmanuel Macron, déclarait lors de la 72e Assemblée générale des Nations Unies : « Ce qui nous protège, c'est notre souveraineté et l'exercice souverain de nos forces au service du progrès. C'est cela l'indépendance des nations dans l'interdépendance qui est la nôtre ». Nous sommes donc bien dans un contexte d'interdépendance.

Dans le cadre d'un État-nation, se gouverner soi-même et décider seul supposeraient d'être strictement et technologiquement indépendant dans tous les domaines : en matière numérique, cela pourrait signifier disposer de notre propre moteur de recherche, réseau social, système d'exploitation ou plateforme de e-commerce. Or l'intérêt de ces outils est précisément d'être adoptés par tous et de communiquer ensemble - c'est d'ailleurs pour cette raison que les gens les choisissent.

En quoi la souveraineté nationale peut-elle être menacée par le numérique ? Il me semble que votre commission pose très légitimement la question de la maîtrise des intérêts vitaux. Nous ne devons pas confondre ce sujet avec d'autres qui relèvent d'éventuels dysfonctionnements économiques ou de marché : par exemple, la dépendance des acteurs du streaming musical ou du e-commerce envers les plateformes mondiales ne met pas en cause la souveraineté numérique nationale. Il est important de circonscrire ainsi le sujet, car qui trop embrasse mal étreint ! Une acception trop large polluerait le débat et ne nous permettrait pas de nous concentrer sur les sujets les plus pertinents appelant des réponses de politique publique.

Par ailleurs, je voudrais dire que nous devons avoir les moyens de nos ambitions. Dans le domaine militaire, la défense des intérêts nationaux est pensée au-delà du strict cadre territorial et nécessite de disposer d'une capacité de projection et d'intervention. Ainsi, la France va se doter d'un commandement en charge de l'espace. En matière numérique, l'approche est

nécessairement différente ; la dimension territoriale ne s'aborde pas de la même manière. Laisser penser que nous pourrions nous doter demain d'un Google français ou d'un système d'exploitation français ne serait pas réaliste par rapport à nos moyens et nous écarterait du sujet.

En revanche, il existe des questions critiques dans le domaine régalien qui relèvent de nos intérêts vitaux. Le premier aspect concerne la confrontation entre des technologies émergentes et le monopole régalien. Je pense par exemple à l'authentification et à l'identité numériques, à l'essor des cryptomonnaies, aux technologies de surveillance numérique ou d'observation par satellite, à la cybersécurité, au chiffrement, aux biens à double usage, etc. En soi, l'innovation est neutre, mais certaines technologies nouvelles pourraient constituer des menaces si le pouvoir régalien ne s'en emparait pas au bon moment et de manière satisfaisante.

La souveraineté numérique croise aussi les intérêts vitaux du pays lorsque des capacités industrielles peuvent faire l'objet de menaces stratégiques. Il est clair que la France et l'Europe sont loin d'être dans le peloton de tête de ce point de vue, ce qui est problématique en termes stratégiques. Les acteurs sont plutôt américains, ou asiatiques. C'est le cas pour les composants électroniques clés - la France ayant perdu beaucoup de ses actifs dans ce domaine -pour les réseaux - je vous renvoie aux débats actuels sur la 5G -, pour l'offre de cloud ou pour la cybersécurité, domaine dans lequel nous ne disposons pas de pure player de taille mondiale - nos entreprises sont innovantes et performantes, mais elles travaillent uniquement sur des secteurs de niche. De ce fait, au-delà du périmètre stratégique, les entreprises s'équiperont demain de solutions étrangères.

L'une des explications de cette situation est que nous avons délaissé la politique industrielle ; elle nous a pourtant permis de construire des champions, mais pas dans le secteur du numérique à l'exception de Dassault Systèmes ou d'Atos. Contrairement au Nasdaq, le CAC 40 abrite peu d'acteurs de moins de 25 ans. Le ministre de l'économie et des finances, Bruno Le Maire, a raison de mettre en avant le rôle de la politique européenne qui a parfois contrecarré l'émergence de champions nationaux ou européens du fait de l'application des règles de concurrence. Seule une politique industrielle pensée au niveau européen permettrait de répondre aux défis actuels.

Dernier point que je souhaite aborder à ce stade :. toutes les entreprises ont besoin d'un cadre de régulation stable qui ne porte pas atteinte à l'innovation. Il faut aussi que la France s'implique dans la préparation des traités qui concernent le numérique - je pense au Cloud Act ou au projet européen e-evidence - et dans les différents échelons de la gouvernance numérique mondiale. Il est vrai que les Français sont de plus en plus engagés sur ces sujets. Nous devons enfin nous doter d'une cyberdéfense européenne, qui doit être un axe prioritaire de développement

dans lequel nous devons mettre en adéquation les capacités industrielles et nos ambitions de défense.

M. Gérard Longuet, rapporteur. - Dans une interview récente, vous avez évoqué un sujet dont vous n'avez pas parlé pour l'instant : le déficit de profils formés aux nouvelles technologies au-delà des esprits brillants sujets au brain drain. Que vouliez-vous dire ?

Par ailleurs, je suis libéral, mais j'ai été ministre de l'industrie et je regrette que les gouvernements successifs aient supprimé ce ministère en tant que tel. L'époque était certes différente, puisque certains secteurs comme les télécommunications, l'énergie ou les transports vivaient dans le cadre de monopoles. On aurait toutefois pu imaginer que ce ministère survive en tant que lieu de réflexion à la disposition du Gouvernement ; cela aurait peut-être permis de stabiliser les orientations choisies au fil des années... Est-ce que les positions des experts techniques pourraient être mieux intégrées dans le processus de décision de la sphère publique ? Nous avons déjà évoqué cette question au sein de l'Office parlementaire d'évaluation des choix scientifiques et technologiques, dont je suis président.

Enfin, les grands acteurs du cloud sont maintenant mondiaux et nos entreprises privilégient, malgré le Cloud act, leurs solutions. Pensez-vous que nous puissions, dans cette situation, créer un cloud souverain ?

Mme Martine Filleul. - Comme beaucoup des personnes que nous avons auditionnées, vous estimez que la France ne figure pas dans le peloton de tête en matière de sécurité et de souveraineté numériques. Toutefois, pour avoir visité les ateliers de l'imprimerie nationale et rencontré ses cadres, il m'a semblé que la France n'était pas en si mauvaise position sur les questions d'identité. Nous ferions même figure de référence pour un certain nombre de pays. Que pensez-vous de cette petite note d'optimisme ?

M. Franck Montaugé, président. - J'aurais voulu connaître votre position sur la portabilité et l'interopérabilité à la fois des données et des applications. De même, que pensez-vous de l'open source ?

J'aimerais également recueillir votre avis sur le statut des plateformes. Par certains aspects, elles sont extrêmement positives, notamment en termes de création de valeur et de mise en relation ; mais, elles soulèvent des problématiques très lourdes qui nous amènent à nous interroger sur la régulation des contenus. Pensez-vous qu'il soit nécessaire de leur confier le statut d'éditeur plutôt que d'hébergeur, avec toutes les conséquences que cela implique ?

Enfin, vous avez évoqué dans votre liste des points critiques les questions d'identité, de cryptomonnaie, , mais pas celle de la justice. Or je m'interroge aussi sur une forme d'ingérence des plateformes et de certains GAFA dans les questions de justice. Que pouvez-vous nous en dire ?

M. Loïc Rivière. - Le recrutement de profils formés aux nouvelles technologies est l'un des principaux problèmes auxquels sont confrontés les différents acteurs non seulement du secteur producteur de technologie, mais aussi de tous les secteurs en voie de digitalisation. De fait, la très forte pénurie de main-d'oeuvre continue de s'accroître.

Nous travaillons sur cette question dans le cadre du pacte productif que le Président de la République a lancé au mois d'avril dernier. Un groupe de travail, animé par le secrétaire d'État Cédric O, cherche des solutions concrètes à ces problèmes de recrutement dans le secteur de la cybersécurité, qu'il s'agisse de la défense nationale par exemple ou tout simplement des besoins des entreprises. Nos formations sont reconnues et les profils qualifiés sont « chassés » par des acteurs ayant investi en France et disposant d'une attractivité salariale importante. Il s'agit d'un problème à grande échelle et d'une faiblesse de notre écosystème. Nous y travaillons.

Monsieur le rapporteur, on peut effectivement regretter qu'il n'existe pas de structure de pilotage plus pérenne de notre stratégie industrielle. Toutefois, en matière d'innovation, en particulier dans le numérique, ce que l'on prévoit de mettre en place dans dix ans peut se révéler dépassé après seulement deux ans.

Aux États-Unis, par exemple, la Defense Advanced Research Projects Agency, ou DARPA, essentiellement liée à l'environnement militaire, joue un rôle de pilotage des investissements en apportant des soutiens très importants à certaines entreprises innovantes. Comme l'ont souligné beaucoup de rapports, il manque sans doute en France une telle structure de pilotage, qui permettrait d'envisager d'un point de vue stratégique les investissements que la France devrait réaliser au profit des entreprises et secteurs critiques. Si nous comptons beaucoup d'acteurs sur le marché, ils ne sont pas suffisamment puissants. Nous disposons toutefois d'un formidable outil : la BPI.

En ce qui concerne la question du cloud souverain, la dernière expérience menée a laissé un goût amer. Il est essentiel de bien différencier les données relevant du marché de celles, plus sensibles, entrant dans le champ de la souveraineté numérique. En dépit de l'échec des entreprises choisies à l'époque, la problématique reste structurante : il est dans l'intérêt de la France de disposer d'alternatives en matière de cloud.

La question est de savoir où placer le curseur entre un cloud souverain hébergeant uniquement les données sensibles de l'État et un cloud également capable de répondre aux besoins des grands utilisateurs nationaux.

Certains acteurs, comme OVH que vous avez auditionné, ont connu une croissance exceptionnelle. Selon les dires de certains de leurs utilisateurs, qu'il serait intéressant de vérifier, ils ne parviennent pas toujours à répondre à l'intégralité de la demande. Toujours est-il que ces

acteurs ont besoin de grandir à l'échelle européenne pour peser face aux acteurs mondiaux. La problématique du cloud souverain est donc toujours valable mais je pense qu'il faut plutôt faire confiance au marché et soutenir les acteurs français quand ils en ont besoin.

La France dispose de très grands savoir-faire en matière de cybersécurité. Quand j'évoquais le peloton de tête dont nous serions absents, je faisais davantage allusion à notre puissance de marché qu'à notre savoir-faire technologique. Nos pépites sont régulièrement rachetées par des acteurs mondiaux ou par des acteurs nationaux de la défense et de la sécurité qui les intègrent dans leur offre. Malheureusement, ces derniers ne sont pas suffisamment gros pour couvrir l'intégralité de la gamme fonctionnelle de la cybersécurité ni concurrencer les grands offreurs génériques du marché.

La portabilité est un sujet à manier avec précaution. Elle est souvent perçue comme un moyen de « libérer » les énergies et d'ouvrir l'innovation à certaines start-up dans des secteurs où les données sont devenues le nouveau pétrole. Or les données sont souvent enrichies par des algorithmes, par des innovations. Elles peuvent donc embarquer de la propriété intellectuelle, de la valeur propre à l'entreprise. Les pouvoirs publics ne sont d'ailleurs intervenus que par touches successives sur des secteurs relevant soit d'une certaine conception de l'intérêt général, soit d'infrastructures.

Il faut se garder de généraliser et avoir le souci de mener des études d'impact intelligentes. Si l'on organisait la portabilité d'un certain nombre de données, comment pourrait-on s'assurer de ne pas favoriser des acteurs dominants du secteur accusant un retard en termes d'innovation, mais disposant d'un grand pouvoir de marché ? C'est toute la problématique de la régulation en général : il s'agit d'une arme fatale à manier avec précaution. En essayant de briser des situations dominantes ou de monopole, on peut déstabiliser un marché au profit d'autres acteurs que ceux que l'on souhaitait favoriser.

L'interopérabilité est la capacité des systèmes à communiquer entre eux. Les acteurs les plus innovants, pour se protéger de l'appétit des géants, ont tendance à développer des formats fermés. L'interopérabilité relève souvent soit d'un choix industriel de l'entreprise, soit de la régulation face à une rente de situation qui ne crée plus ni valeur ni innovation. Là encore, il faut procéder avec analyse et mesure. Il ne faut pas confondre interopérabilité et open source ou logiciel libre. Ce dernier relève d'un business model particulier, celui de la mutualisation de la recherche-développement en s'appuyant sur une communauté. Par la suite, la distribution sur le marché s'opérera avec des modes de licence open source. La valeur va en quelque sorte se déplacer de la propriété intellectuelle aux services associés.

Ce business model n'a pas fait florès en termes de réussite économique, mais il continue de se développer. On dit de Microsoft qu'elle

est aujourd'hui la première entreprise d'open source dans le monde. En quelques années, nous sommes passés d'un conflit sur la conception de la propriété intellectuelle à l'intégration par le monde propriétaire pour arriver à des modèles mixtes.

Nous comptons quelques réussites nationales et mondiales dans le domaine de l'open source. Je pense notamment à Talend, entreprise aujourd'hui cotée au Nasdaq et dont l'un des fondateurs présidait Tech in France voilà encore peu de temps.

Vous avez également soulevé la question du statut des plateformes. Vous faisiez très probablement allusion à la réouverture de la directive e-commerce et à la remise en cause du statut d'hébergeur. Nous avons toujours plutôt défendu le statut d'hébergeur, afin de garantir la neutralité du net. Il nous semble en effet important de ne pas permettre aux fournisseurs d'accès et aux moteurs de recherche d'éditorialiser internet. Cette irresponsabilité organisée constitue la garantie d'un internet libre et ouvert.

Toutefois, on se rend compte que, sur un certain nombre de sujets, cette irresponsabilité n'est pas forcément tenable - je pense notamment à la proposition de loi de la députée Laetitia Avia sur la cyber-haine. On confie de plus en plus de responsabilités aux hébergeurs, et donc aux plateformes. De facto, cela remet en cause la « pureté » de ce statut. Pour autant, cela ne doit pas forcément déboucher sur un nouveau statut tant les qualités du statut actuel d'hébergeur sont précieuses pour assurer la neutralité d'internet.

Le législateur et les pouvoirs publics confient toujours davantage de responsabilités aux plateformes en matière de régulation des contenus. Dans certains domaines, ces pouvoirs peuvent apparaître exorbitants. Dans le monde ancien, ils auraient sans doute relevé du juge. Il est donc aussi compréhensible que la CNCDH (Commission nationale consultative des droits de l'homme), par exemple, s'inquiète de ce déplacement.

Nous concevons qu'une certaine forme de responsabilisation supplémentaire puisse être imposée, la justice ne pouvant répondre à certaines exigences, notamment en matière de haine.

Toutefois, nous avons critiqué l'alignement de cette proposition de loi sur le périmètre de la loi pour la confiance dans l'économie numérique, laquelle s'appuie sur certaines dispositions du code pénal, notamment la loi de 1881. On se retrouve ainsi avec des éléments relevant davantage de la définition d'une morale publique que de la haine. Or cette proposition de loi n'avait pleinement son sens que circonscrite à son objet initial, à savoir la lutte contre la haine en ligne. In fine, c'est toujours au juge que devra revenir le dernier mot.

M. Franck Montaugé, président. - Quelle est votre position en matière de transparence des algorithmes ?

M. Loïc Rivière. - Là encore, il faut faire preuve de prudence et d'analyse. À partir du moment où un algorithme est connu, il devient « dévoyable ». Or on attend justement d'un algorithme qu'il demeure pertinent. Ceux qui vendent des biens et services sur internet veulent être bien référencés par les moteurs de recherche et s'efforcent donc de connaître l'algorithme, le « secret », pour pouvoir optimiser leur visibilité. Il s'agit d'une « guerre » permanente.

La transparence de l'algorithme suppose ensuite de pouvoir l'interpréter. C'est un peu comme l'open source : il ne suffit pas de connaître un code source, encore faut-il pouvoir l'interpréter, le réécrire et, le cas échéant, le modifier. Il faut donc se méfier de la transparence à tout crin.

En revanche, il va de soi que les citoyens doivent avoir accès, comme le prévoit la loi, aux algorithmes qui mettent en oeuvre des politiques publiques. Je pense, par exemple, au calcul de l'impôt ou à l'orientation des élèves au collège ou dans les études supérieures.

De même, cette information doit être explicitée, car elle n'a de valeur que si elle est compréhensible par tous. L'usage a montré que les algorithmes que je viens d'évoquer n'étaient pas sans défaut. Il faut comprendre qu'un algorithme relève d'une rationalité humaine. Il ne faut pas tomber dans le fantasme d'un monde numérique parfait. Derrière ces algorithmes, il y a une stratégie politique et des objectifs à mettre en oeuvre. Il s'agit, par exemple, d'orienter les collégiens à Paris en assurant la mixité sociale. Un algorithme n'est, par définition, jamais neutre.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible en ligne sur le site du Sénat.

Audition de M. Benoît Tabaka, secrétaire général adjoint de Google France, le 17 juillet 2019

M. Franck Montaugé, président. - Mes chers collègues, notre commission d'enquête poursuit ses travaux avec l'audition d'un représentant de l'entreprise Google : M. Benoît Tabaka, secrétaire général adjoint de Google France.

Cette audition est diffusée en direct sur le site Internet du Sénat. Elle fera également l'objet d'un compte rendu publié.

Un faux témoignage devant notre commission d'enquête serait passible des peines prévues aux articles 434-13, 434-14 et 434-15 du code pénal. Monsieur Tabaka, je vous invite donc à prêter serment de dire toute la vérité, rien que la vérité, levez la main droite et dites : « Je le jure. ».

Conformément à la procédure applicable aux commissions d'enquête, M. Benoît Tabaka prête serment.

M. Franck Montaugé, président. - Je commencerai par une question d'ordre très général : l'entreprise Google veut-elle concurrencer les États en les affaiblissant progressivement comme le suggèrent certains analystes ? De nombreux commentateurs se demandent en effet quels sont l'objectif et l'agenda de Google et de sa maison-mère Alphabet ?

Deux questions plus précises relatives aux données : le Cloud Act permet aux autorités américaines de disposer des données que vous stockez, quel que soit le lieu de stockage. Cela inquiète légitimement les pouvoirs publics français car ce sont à la fois les données personnelles de nombreux citoyens et les données stratégiques des entreprises qui peuvent ainsi être utilisées, sans que leurs propriétaires ne soient seulement informés. Or, de grands groupes vous confient leurs données en utilisant vos solutions logicielles, à l'image d'Airbus Defence and Space ou d'Atos. Pouvez-vous nous assurer que Google ne permet ni ne permettra aux autorités américaines de prendre connaissance des données de nos concitoyens et de nos entreprises ? Comment garantissez-vous la confidentialité des données-clients que vous hébergez et comptez-vous concilier ces obligations avec les règles européennes protégeant les données personnelles (RGPD) ?

M. Benoît Tabaka, secrétaire général adjoint de Google France. - La souveraineté numérique est un sujet qui a émergé depuis ces cinq dernières années. Google est une entreprise créée il y a vingt-et-un ans par deux ingénieurs qui s'étaient fixé comme mission de garantir l'accès à l'information à tous. Ceci a conduit à la mise en service d'un moteur de recherche et d'un outil de messagerie pour rechercher, émettre l'information et publier des contenus, via notamment des plateformes de blog ou de vidéo, comme Youtube. Google est progressivement devenu l'un des principaux acteurs du web, qui a fait disparaître un certain nombre de barrières, en

permettant notamment à de nombreuses PME d'accéder à une audience internationale et de décloisonner leurs réseaux de contacts. Du reste, toute personne, grâce au web, peut à la fois émettre et être le destinataire de l'information.

La souveraineté se définit autour de différents concepts. Le premier est économique : elle définit la capacité de développer des acteurs stratégiques sur son territoire. Dans notre société issue de la révolution numérique, la question de la place des acteurs stratégiques se pose. La France est ainsi en retard en matière de numérisation de son tissu industriel et économique : un commerçant français sera moins prompt que son homologue allemand à faire la démarche d'entrer dans un circuit de transformation numérique. La transformation numérique concerne également les acteurs industriels de plus grande ampleur, comme Airbus et Atos avec lesquels nous travaillons.

Notre objectif, chez Google, est d'accompagner tant les TPE-PME que les grands groupes industriels, grâce à des partenariats stratégiques, et non de nous substituer à eux. À titre d'exemple, nous collaborons avec Orange à la construction de son nouveau câble sous-marin entre la France et les États-Unis, ainsi qu'avec Alcatel pour celle du câble reliant l'Europe et l'Afrique. Nous travaillons également avec Air France sur les technologies d'intelligence artificielle afin d'améliorer sa flotte de fret, ainsi qu'avec Total, pour l'identification de puits de forage, et Carrefour, pour la transformation numérique de ses métiers.

En outre, Google, dont les centres d'intelligence artificielle se trouvent en France, travaille aux côtés des centres de recherche français, comme ceux de l'ENS (École normale supérieure) et de Polytechnique. Notre modèle de recherche est ouvert : avec plus 5 200 publications, nos résultats et un grand nombre de nos bases de données demeurent en libre accès.

En matière de sécurité, qui est l'une des autres composantes de la souveraineté, on a pu entendre, notamment durant vos auditions, que Google refuserait de se soumettre aux lois françaises et de coopérer avec la justice. Je vais être clair avec vous sur ce point : Google applique le droit français et coopère avec la justice française. Pour preuve, nous avons rejoint, au lendemain des attentats terroristes de 2015, le groupe de contact créé sous l'égide du Ministère de l'intérieur et destiné à favoriser l'échange d'informations et de bonnes pratiques entre les acteurs du numérique. Nous travaillons ainsi, en partenariat avec les Pouvoirs publics, tant au niveau national qu'européen, à la détection des contenus terroristes et haineux, ainsi qu'à la transmission, en cas d'urgence, de certaines données. Suite à la promulgation de la loi sur les fausses nouvelles, nous collaborons avec le Conseil supérieur de l'audiovisuel, devenu régulateur des activités numériques. En outre, l'année dernière, Google a répondu favorablement à plus de 11 000 demandes émanant des autorités françaises et nous concernant.

En ce qui concerne l'accès aux données, le Cloud Act, adopté par les États-Unis, visait à redéfinir l'ensemble des régimes spécifiques à l'accès aux données, suite à différentes décisions de jurisprudence. Il s'agit de mettre en place une relation bilatérale qui organise l'accès aux différentes données à la fois des autorités américaines et étrangères. Or, ces dispositions ne sont pas entrées en vigueur, en l'absence de conclusion des accords bilatéraux prévus, notamment entre l'Union européenne et les États-Unis. Le Cloud Act permet d'accéder à un certain nombre de données, à l'instar de ce que permet le droit français en autorisant l'accès aux informations sur nos serveurs. Ainsi, Google ne serait pas uniquement tributaire des seules demandes du gouvernement américain, mais aussi de l'ensemble des gouvernements signataires.

Par défaut, lorsque nous recevons une demande concernant l'un de nos clients, nous renvoyons cette demande à ce dernier. Google n'est qu'un hébergeur de données. Nos services permettent en outre aux entreprises clientes d'appliquer leur propre clef de chiffrement. Ainsi, quand bien même le Cloud Act entrerait en vigueur et obligerait Google à communiquer les données de ses clients, les informations chiffrées ne seraient pas transmises en clair aux autorités qui devraient alors les solliciter directement.

M. Patrick Chaize. - Vous êtes sous serment et ma première question se rapporte aux différentes condamnations dont votre entreprise a fait l'objet. En trois ans, l'entreprise que vous représentez a été condamnée à plus de huit milliards d'euros d'amende pour atteinte aux règles de la concurrence avec les applications AdSense, Android et Shopping. L'Autorité de la concurrence a prononcé des mesures d'urgence en février dernier dans le litige opposant l'entreprise que vous représentez à la société Amadeus sur le marché de la publicité en ligne. En France, l'Autorité de la concurrence n'hésite plus à envisager une régulation asymétrique spécifique pour les géants ayant atteint une taille critique. Certaines voix, notamment de parlementaires américains, réclament le démantèlement des Gafam. Quels arguments leur opposez-vous ? Pourquoi ne pas rendre public votre modèle économique et votre agenda pour répondre aux plus pressantes critiques qui vous sont adressées ?

J'en viens à ma seconde question : la galaxie Google, réunie sous la société mère Alphabet, a, comme les autres grandes entreprises du numérique, une politique d'acquisition très active. Aujourd'hui, certains spécialistes des questions de concurrence considèrent que ces acquisitions sont « prédatrices » en ce qu'elles ont pour objet de tuer la concurrence, et donc l'innovation. Elle aurait également pour conséquence de tuer l'ambition des start-ups qui, au lieu de créer une solution mondiale, souhaiteraient surtout se faire racheter. Les États doivent-ils admettre de telles pratiques et laisser leurs administrations signer des partenariats avec des entreprises régulièrement condamnées ?

Troisièmement, en France, l'Arcep souligne le rôle d'infrastructure essentielle que sont devenus les systèmes d'exploitation des terminaux - Android pour Google et iOS pour Apple. L'autorité propose de les réguler afin d'en garantir l'ouverture et d'éviter qu'une société comme Google ait un pouvoir de vie ou de mort sur une entreprise dont l'activité repose, au moins en partie, sur sa présence au sein du magasin d'application Google Play. Menez-vous un dialogue avec l'Arcep sur ces questions ?

Enfin, des tensions existent, notamment avec un grand équipementier, Huawei, qui pourrait se voir interdire l'utilisation de votre système d'exploitation. Ne craignez-vous pas que cette entreprise ne soit alors conduite à créer son propre système d'exploitation ?

M. Benoît Tabaka.- En ce qui concerne le droit de la concurrence, les décisions de la Commission européenne, qui ont concerné les applications AdSense, Android et Shopping, se sont inscrites dans un temps relativement long - sur près d'une décennie. Au terme de nombreuses discussions avec la Commission européenne, des sanctions ont été prononcées, et que nous avons acquitté les amendes afférentes. Notre appréciation du marché s'avère distincte de celle de la Commission européenne et motive les appels en cours que nous avons faits de ses décisions.

Tout d'abord, de quel marché parle-t-on ? Pour appréhender Google Shopping, la Commission européenne s'est exclusivement focalisée sur le marché des comparateurs de prix. Cependant, nous relevons de notre côté que plus de la majorité des requêtes débutent à partir d'Amazon qui est un site marchand, quitte à solliciter ultérieurement des comparateurs de prix. Nous restons donc en désaccord avec la méthode suivie par la Commission européenne qui a circonscrit son évaluation à des marchés très spécifiques, là où Google considère essentiel d'appréhender le marché plus globalement et de suivre une tout autre dynamique. Ainsi, pour reprendre le cas d'Android, sur lequel la Commission européenne a également rendu une décision, seuls les systèmes d'exploitation Android en dehors de la Chine ont été considérés. Dès lors, le marché mondial des Androids a été segmenté. Le système d'exploitation d'Apple n'a pas été pris en compte dans l'analyse concurrentielle, alors que les consommateurs migrent très facilement d'Android à Apple et vice versa ! La concurrence avec Apple a tout simplement été ignorée dans l'appréciation de la situation de Google !

Deuxième élément de désaccord que l'on retrouve dans les deux décisions relatives à Android et à Shopping : la problématique de l'impact sur le concurrent et le consommateur n'a pas été, selon nous, solidement établie. Ainsi, la distribution concomitante de notre moteur de recherche et de nos autres applications Google Play avec nos Androids n'empêche nullement les constructeurs de préinstaller par défaut d'autres moteurs de recherche, puisqu'il n'y a pas eu de clauses d'exclusivité nous concernant. Nous avions ainsi demandé à la Commission européenne d'aller au-delà de la prise en compte de nos seules pratiques commerciales. Dans sa décision

Shopping, la Commission européenne a avant tout contesté la concomitance du lancement d'un moteur de recherche vertical et d'un nouvel algorithme affectant de nombreux comparateurs de prix.

Le droit de la concurrence est manifestement encore en construction, et je note que sur le dossier Android, d'autres autorités de la concurrence, au Canada, en Australie ou aux États-Unis, ont pu avoir d'autres analyses que celles de la Commission européenne. En tout état de cause, nous avons toujours été à l'écoute des régulateurs et nous ajustons bien sûr nos pratiques et nos contrats en fonction de leurs décisions.

Je ne m'étendrai pas sur le cas Amadeus qui fait actuellement l'objet d'une instruction par l'Autorité de la concurrence. La question posée porte sur la façon dont Google doit notifier la mise en oeuvre d'un certain nombre de ses règles, notamment dans le cadre de la publicité, à ses utilisateurs ? Cette question fait actuellement l'objet d'échanges avec l'Autorité.

M. Patrick Chaize. - Mes questions étaient plus précises : quel argument opposez-vous à ceux qui réclament votre démantèlement et pourquoi ne rendez-vous pas public votre modèle économique ?

M. Benoît Tabaka.- Notre modèle économique est public et repose pour partie, en ce qui concerne notre moteur de recherche, sur la publicité. D'autres modèles économiques coexistent, comme l'abonnement souscrit auprès de Youtube ou la licence sur nos activités de Cloud. L'ensemble de nos éléments financiers sont également publiés trimestriellement et annuellement, conformément à notre statut de société cotée.

La question des types de données que nous utilisons est distincte. Si Internet reste alimenté, pour une large part, par la publicité, le type de modèle publicitaire varie néanmoins selon les acteurs. Ainsi, chez Google, la publicité qui apparaît sur le moteur de recherche est personnalisée en fonction de la requête adressée par l'utilisateur ; elle ne tient pas compte - en tout cas ce ne sont pas les éléments les plus intéressants pour nous - de l'historique des recherches ou des achats de l'internaute. Les données de localisation sont aussi utilisées, qui vont permettre de personnaliser, par exemple, la langue de la publicité.

Au-delà de son activité de moteur de recherche, Google est également une régie publicitaire - ce sont les annonces affichées sur d'autres sites - où les modèles publicitaires résultent, quant à eux, de l'agrégation des données personnelles de l'internaute, voire de son historique de navigation et de cookies, afin d'offrir la publicité la plus personnalisée possible.

M. Patrick Chaize. - Ces modèles publicitaires sont-ils hermétiques l'un par rapport à l'autre ?

M. Benoît Tabaka. - Ce sont deux systèmes totalement différents qui relèvent de deux modes de gestion distincts. Tout système publicitaire est complexe : si la donnée y joue un rôle, son utilisation peut largement différer

selon qu'on se trouve sur le moteur de recherche ou que l'on consulte des sites.

Concernant notre moteur de recherche, les internautes nous indiquent de façon active leurs intérêts, et nous sommes avec les annonceurs en situation transactionnelle : Google ne gagne de l'argent qu'à partir du moment où la personne a cliqué sur le lien qui lui était proposé dans une publicité. Il s'agit ici d'un modèle publicitaire que l'on pourrait qualifier d' « économie de l'intention »

Concernant les annonces sur les sites qui visent à monétiser une audience, il s'agit de capter l'attention de la personne qui se trouve sur le réseau et de la valoriser. Toute une chaîne d'acteurs concourt à ce modèle publicitaire, dont certains vont notamment mixer des bases de données de différents sites internet pour permettre de réaliser un profil publicitaire de l'internaute. Google est ainsi présent comme une régie publicitaire classique : pour 100 euros de revenus publicitaires investis sur un site, une commission de régie représente 30 euros, et 70 euros sont reversés au site internet.

Ce domaine est technique et Google essaie naturellement de faire preuve de pédagogie : par exemple en insérant des icônes spécifiques pour fournir plus d'informations aux internautes qui souhaitent comprendre pourquoi de telles publicités leur sont proposées. Nous avons ainsi demandé à plusieurs associations de travailler avec nous au décryptage complet de la chaîne publicitaire, pour répondre aux attentes des personnes.

M. Patrick Chaize. - Avez-vous confiance quant à l'issue des procédures en cours et des appels que vous avez engagés suite à vos condamnations ?

M. Benoît Tabaka.- Dans tous les cas, une discussion, au niveau européen, sur les critères à la fois de définition du marché numérique et de l'analyse des pratiques, est nécessaire.

Concernant notre politique d'acquisition, Google a acheté des entreprises comme Youtube et Android. C'est là un élément de notre stratégie : Google a continué à investir dans ce marché numérique ultra-compétitif en termes d'innovation. À tout moment, un acteur peut survenir et proposer une innovation disruptive par rapport aux produits de ses concurrents plus anciens. Lorsque Google est arrivé, le marché américain comptait déjà treize moteurs de recherche. C'est notre politique d'innovation qui nous a permis de proposer aux utilisateurs une technologie disruptive et de devenir le leader des moteurs de recherche d'abord aux États-Unis. C'est une démarche de longue haleine : en face de nous se trouvent des entrepreneurs dont certains peuvent suivre une stratégie d'entreprenariat et refuser de vendre leur entreprise à des grands groupes, comme Snapchat vis-à-vis de Facebook. Néanmoins, derrière des entrepreneurs peuvent aussi se trouver des fonds qui ont besoin, à moyen terme, de tirer les bénéfices de leurs investissements. Ceux-là auront une démarche visant à vendre

rapidement leur entreprise afin de permettre aux investissements de ces fonds de poursuivre leur cycle de vie. Nous nous concentrons avant tout sur les acteurs qui participent de notre coeur de mission, à savoir la transmission de l'information.

M. Patrick Chaize. - Votre stratégie vise à acquérir une position dominante. Ne pensez-vous pas qu'on devrait arrêter une telle hémorragie ?

M. Benoît Tabaka. - L'appréciation de la position dominante repose souvent sur la prise en compte statique, à l'instant T, du marché en faisant abstraction de l'ensemble de sa dynamique et de ses acteurs. En outre, lorsque vous débutez une recherche sur internet, soit vous utilisez un moteur de recherche, soit vous vous rendez sur un site dédié, puisque votre recherche tend à être de plus en plus spécialisée.

En termes d'activités, acquérir des entreprises n'implique pas forcément de devenir dominant sur un marché. De nombreux acteurs autres que Youtube font aujourd'hui de la vidéo en ligne. Certains de nos produits, comme le réseau social Google Plus, n'ont pas été compétitifs, faute d'avoir été perçus comme innovants par les utilisateurs. Il ne s'agit nullement d'une hémorragie : aujourd'hui, peu de sociétés françaises ont été rachetées par des grandes entreprises américaines ! Nous n'avons, au final, racheté que trois start-ups en France, tandis que d'autres acteurs emblématiques français, comme Criteo, sont aujourd'hui cotés au Nasdaq.

M. Patrick Chaize. - Quelles sont vos relations avec l'Arcep ?

M. Benoît Tabaka.- A la suite de la publication de son rapport sur les terminaux ouverts, nous avons eu de nombreux échanges avec l'Arcep sur la régulation des systèmes d'exploitation.

Il n'existe pas, en tant que tel, un seul type d'Android puisque celui-ci est, par nature, un logiciel open source. Dès lors, l'ensemble des téléphones Android ne sont pas équipés de la version mère du logiciel. La version que Google met en ligne se retrouve dans nos téléphones ainsi que chez certains constructeurs qui se consacrent avant tout à l'innovation de la partie produit elle-même - hardware - plutôt que de la partie logiciel. L'ensemble des acteurs de l'Android modifient la version initiale de ce logiciel. Il existe aujourd'hui une multiplicité d'Androids présentant, entre eux, une réelle compatibilité au-delà de leurs différences initiales. Plusieurs constructeurs ont d'ailleurs élaboré leur propre système d'exploitation, à l'instar de Xiaomi avec MIUI ou Samsung avec Tizen destiné au marché indien.

M. Patrick Chaize. - Quelle est donc l'origine du problème avec Huawei ?

M. Benoît Tabaka. - Il s'agit avant tout d'un problème géopolitique entre les Gouvernements chinois et américain.

M. Patrick Chaize. - Androd n'est-il pas en définitive un système Open Source contrôlé ?

M. Benoît Tabaka.- Ce n'est pas vraiment le cas. Google met le logiciel en libre accès et chacun des constructeurs va en recevoir les mises à jour, notamment de sécurité, tous les mois. À partir du moment où un gouvernement interdit d'adresser des logiciels à certains acteurs, certes ils ne les recevront plus, mais ceux-ci pourront toujours développer leurs propres patchs de sécurité. L'environnement Android n'est pas contrôlé ; Google dispose de lignes automatiques dans lesquelles sont publiées des pages de sécurité.

M. Pierre Ouzoulias. - Mes questions seront celles d'un historien. Vous êtes aujourd'hui une entité supranationale non étatique, avec une puissance économique et d'influence supérieure à celle de bon nombre d'États, voire prochainement au nôtre. Vous avez pris ce pouvoir d'une façon inédite, c'est-à-dire sans chercher à maîtriser la sphère politique. Votre modèle de domination est donc original. Aujourd'hui, vous investissez énormément dans la formation, via notamment les Google ateliers numériques, où vous offrez, gratuitement, une formation naturellement très conforme à votre vision du monde et à votre modèle économique. Au sommet de votre puissance, considérez-vous toujours utiles les États-nations ? N'avez-vous pas l'impression de participer à leur obsolescence, quitte à produire des conséquences contraires à la diffusion, à terme, de votre modèle ? Si l'on remplace la relation du citoyen à l'État par celle du citoyen à Google, ne permet-on pas l'émergence des formes de prise de domination politique qui peuvent contraindre votre modèle économique ? En d'autres termes, Google a-t-il encore besoin de l'État ?

M. Franck Montaugé, président. - Je compléterai la question tout à fait pertinente de mon collègue en vous interrogeant à mon tour sur un fait que je vous remercie d'éclairer et qui renvoie à la nature de vos relations avec vos utilisateurs. En 2013, Vinton Cerf, qui était « chef évangéliste » de Google, a déclaré que la vie privée pourrait devenir une « anomalie ». Cette phrase me paraît inquiétante ! Au-delà de cette question générale qui touchait au politique et au rapport avec l'État, quelle est la philosophie qui préside aux actions que vous menez et aux formations que vous proposez ?

M. Benoît Tanaka. - Google a besoin des États, en tant qu'entreprise multinationale qui a vocation à appliquer les législations en vigueur dans chacun des pays où elle opère.

Dans les ateliers numériques, nous ne formons pas les gens à une vision du numérique propre à Google. Le principe de ces lieux est donner la capacité de s'informer à un large public, allant des entreprises aux personnes de tout âge et de tout niveau, sur des questions numériques. Il ne s'agit pas de vendre les produits de Google, mais de coopérer avec les acteurs locaux qui vont participer aux formations. Vous trouverez notamment dans ces

ateliers des associations locales, des centres sociaux, des chambres de commerce et d'industrie qui vont utiliser ces ateliers comme des plateformes. À plusieurs reprises, les acteurs du logiciel libre ont été invités et ils ont naturellement pu proposer des alternatives aux produits de Google. Manifestement, l'objectif de ces lieux est d'ouvrir les débats et de sensibiliser les publics. À titre d'exemples, nous aidons les entreprises à mieux utiliser internet ; nous sensibilisons les restaurateurs à répondre aux différents avis qu'ils peuvent susciter sur la toile et dont dépend leur notoriété ; nous assistons les demandeurs d'emplois dans leur démarche de recherche, en partenariat avec des acteurs locaux. Ces ateliers participent ainsi à un mélange d'inclusion numérique au profit du grand public et d'accompagnement du tissu économique.

Google considère l'État comme nécessaire. Loin des zones grises, d'un pseudo « Farweb » ou de l'opposition alléguée entre les règles qui régissent le monde virtuel et le monde réel, Google a décliné sur ses plateformes, de manière très opérationnelle, le contenu de la législation. Nous veillons notamment à ce que les contenus pornographiques ne soient pas accessibles sur YouTube ou que des contenus qui véhiculent de la haine ou qui participent à la désinformation ne soient pas relayés sur nos plateformes. Nous travaillons avec les États et les régulateurs pour entrer dans ce mode d'échange. Toute modification structurelle de produits requiert nécessairement une discussion préalable. Nous aspirons donc à être l'un des acteurs de la régulation étatique, puisque nous sommes voués à y être soumis, sous peine d'être sanctionnés.

Pour autant, les règles actuelles ne sont parfois pas toutes suffisamment claires. Pour preuve, les discussions autour de la protection des données et de la collecte du consentement : si nous avons récemment été sanctionné par la CNIL, je note que la complexité du sujet a récemment motivé l'ouverture par la même CNIL d'une période de douze mois destinée à familiariser les entreprises avec l'interprétation des règles en la matière. Cela démontre bien la difficulté de leur application. Sur un texte aussi fondateur que le RGPD, il faudra attendre plusieurs décisions pour en connaître la juste application.

La phrase de Vinton Cerf, qui est l'un des pères fondateurs de l'internet et assume toujours les fonctions de « chef évangéliste » de Google, est sortie de son contexte et des éléments qui en motivaient la prononciation. Il parlait de sa vie personnelle dans un petit village en Allemagne où la vie privée n'existait pas en raison du contrôle social qui s'y faisait jour. À l'inverse, nous travaillons chez Google pour assurer la vie privée et la protection de l'intégrité physique des données de nos utilisateurs.

M. Franck Montaugé, président. - Auriez-vous des préconisations pour éclairer l'internaute sur l'utilisation de ses données et les conséquences de ses comportements sur internet et ce au-delà du RGPD ?

M. Benoît Tabaka.- En matière de vie privée et de la protection de leurs données personnelles, les gens ne connaissent ni leurs droits ni les moyens dont ils disposent pour les exercer. C'est là un phénomène nouveau, puisqu'il était rare, auparavant, d'évoquer les outils laissés à la disposition des personnes pour gérer l'utilisation de leurs données personnelles. Ainsi, le RGPD contient le droit à la portabilité des données, qui s'étend à toutes les entreprises. Pour traduire concrètement l'existence de ce droit, nous avons renforcé le contrôle donné aux utilisateurs de Google, en leur laissant la possibilité d'avoir accès à l'ensemble des informations disponibles sur leur compte, via un tableau de bord leur permettant d'accéder à leur historique de consultations, tant sur Google que Youtube, et de contrôler la personnalisation de la publicité sur des sites tiers. Au-delà de la transparence, l'outil de contrôle est une réalité. Ainsi, 21 millions d'utilisateurs uniques ont eu recours aux applications disponibles sur la page « Mon compte » en une année, et y ont téléchargé l'équivalent d'un exabyte de données. Google, qui demande à ses utilisateurs, quasiment tous les six mois, de vérifier l'ensemble des informations les concernant, a ainsi mis en ligne les instruments permettant cette vérification.

M. Franck Montaugé, président. - Ne pourrait-on pas préciser aux internautes les données concrètement utilisées dans des algorithmes, pour les profiler et leur envoyer des publicités personnalisées ? C'est le coeur de cette économie de l'attention que vous évoquiez précédemment. Je ne pense pas que ce que vous nous présentez répond à cette demande.

M. Benoît Tabaka.- Ce que je viens d'évoquer s'inscrit en partie dans cette démarche, en ce qui concerne le profil publicitaire. Sur le site YouTube, où vous pouvez bénéficier de recommandations de vidéos, des messages vous indiquent ce qui les a motivées. Nous travaillons actuellement avec le CSA sur la transparence, notamment dans le cadre de la loi sur la désinformation. On demande à Google de fournir sans cesse de nouveaux éléments, n'oublions pas qu'il n'est pourtant que l'un des acteurs de la chaîne.. Au-delà de l'accès aux données, il faut également imaginer les outils qui permettront aux personnes de reprendre le contrôle, de changer de moteurs d'accès - ainsi qu'aux entreprises de changer de Clouds - en assurant le transfert automatique de données d'une plateforme à une autre grâce un standard commun qui est actuellement à l'étude.

M. Patrick Chaize. - Dialoguez-vous actuellement avec l'Arcep ? Par ailleurs, vous considérez-vous propriétaires des données de vos utilisateurs ? Enfin, pourriez-vous accorder l'accès aux algorithmes que vous utilisez aux Autorités de régulation ?

M. Benoît Tabaka. - Nous échangeons très régulièrement avec les services de l'Arcep, en répondant très régulièrement à leurs demandes. Nous venons d'ailleurs de collaborer avec elle à la rédaction du rapport sur l'état de l'internet. Nous répondons systématiquement aux demandes émises par les régulateurs.

Nous ne sommes pas propriétaires des données de nos utilisateurs ; d'où le droit à la portabilité et nos outils qui visent à redonner le contrôle aux utilisateurs sur leurs propres données.

Enfin, les autorités sont en mesure d'accéder aux algorithmes, à l'instar de la Commission européenne lors de son enquête. Nos échanges avec le secrétariat en charge du numérique, notamment à la suite du rapport sur une nouvelle régulation des acteurs du numérique, en s'inspirant de la régulation systémique dans le domaine bancaire, en font foi.

Nos équipes font constamment en sorte que nos algorithmes ne soient pas utilisés à mauvais escient par des personnes extérieures. C'est là une contrainte. Aussi, ne suis-je pas en mesure de préciser l'aboutissement des discussions, qui viennent de débuter, avec les différents régulateurs sur ce point.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible en ligne sur le site du Sénat.

Audition de M. Anton'Maria Battesti, responsable des affaires publiques de Facebook,
le 18 juillet 2019

M. Franck Montaugé, président. - Mes chers collègues, notre commission d'enquête poursuit ses travaux avec l'audition de M. Anton'Maria Battesti, responsable des affaires publiques de Facebook France. Cette audition est diffusée en direct sur le site Internet du Sénat. Elle fera également l'objet d'un compte rendu publié.

Enfin, je rappelle qu'un faux témoignage devant notre commission d'enquête serait passible des peines prévues aux articles 434-13, 434-14 et 434-15 du code pénal. Monsieur Battesti, je vous invite donc à prêter serment de dire toute la vérité, rien que la vérité, levez la main droite et dites : « Je le jure. ».

Conformément à la procédure applicable aux commissions d'enquête, M Anton'Maria Battesti prête serment.

M. Franck Montaugé, président. - Nous connaissons tous les activités de Facebook, réseau social rassemblant près de deux milliards et demis de profils, propriétaire de Whatsapp et d'Instagram, qui tend à assumer de plus en plus de fonctions régaliennes, telles que la prévention en cas de crise avec la fonction Safety Check ou la fourniture d'identité numérique avec Facebook Connect.

C'est pourquoi je vous invite à répondre avant tout aux questions que nous avons à vous poser. Je commencerai par une question d'ordre très général : l'entreprise Facebook veut-elle supplanter les États ?

Je préciserai cette question par les deux exemples les plus récents. Facebook veut s'arroger le pouvoir de battre monnaie en créant le Libra. Quels sont vos arguments pour convaincre les États que le projet ne pose aucun problème au regard de la vie privée, du blanchiment d'argent, de la protection des consommateurs et de la stabilité financière ?

Alors que le Gouvernement français entend légiférer sur la régulation des contenus haineux, Facebook a annoncé sa volonté de mettre en place une « cour suprême indépendante », chargée d'arbitrer les litiges relatifs à la diffusion de contenus pouvant être considérés comme violents ou haineux. Pouvez-vous nous préciser l'articulation de cette solution avec les lois qui pourraient être votées au niveau national ?

Enfin, Mark Zuckerberg a récemment affirmé qu'« il est temps d'actualiser les règles qui régissent Internet afin de définir clairement les responsabilités des personnes, des entreprises et des gouvernements ». Concrètement, quelles solutions l'entreprise Facebook préconise-t-elle ?

M. Anton'Maria Battesti, responsable des affaires publiques de Facebook France. - Avant de répondre à vos questions, permettez-moi de vous présenter rapidement l'entreprise Facebook. En France, environ 36 millions d'utilisateurs utilisent Facebook au moins une fois par mois ; Facebook dispose de 200 salariés en France. Enfin, nous avons réalisé dans ce pays un investissement stratégique via l'ouverture, il y a quelques années, d'un laboratoire d'intelligence artificielle. Il s'agit du seul laboratoire que l'entreprise a ouvert en dehors des États-Unis. Celui-ci est d'ailleurs bien intégré dans l'écosystème français de la recherche, et travaille notamment avec station F. En outre, nous investissons dans la formation ainsi que dans diverses causes sociétales, via la fondation compétence numérique ou à notre fondation de civisme en ligne à laquelle nous avons consacré un million d'euros.

En aucun cas, Facebook n'essaye de supplanter les États. Facebook est un réseau social sur lequel les personnes viennent échanger avec leur famille, défendre une cause qui leur tient à coeur, notamment en s'associant au sein de groupes. Notre réseau est multifacette et a vocation à présenter de nouveaux produits : le market place, le développement de la messagerie. Notre entreprise fournit un service. Certes elle s'est fortement développée dernièrement - nous avons acquis récemment Whatsapp et Instagram -, mais cela reste une entreprise, internationale.

Pour autant, une entreprise n'a-t-elle pas vocation à avoir une responsabilité sociétale ? Vous avez présenté l'outil « Safety check » comme un élément régalien. Je n'irai pas jusque-là. En tout cas, il rend service à la société. Il a été activé pour la première fois en France lors des attentats du Bataclan en 2015. Il existe aujourd'hui un consensus pour dire que nous avons bien fait, car il a permis à beaucoup de personnes se signaler en sécurité dans une situation de crise. D'ailleurs, cet outil est tellement intéressant que l'État est venu nous voir il y a un an, lorsque le ministère de l'Intérieur a arrêté sa propre solution d'alerte - le système d'alerte et d'information des populations (SAIP). Nous avons désormais un partenariat, afin de développer une synergie pragmatique et intelligente entre un service privé et les services de l'État, pour rendre un service à la population. Nous l'avons fait sans hésitation, et je tiens à dire que cela ne coûte pas un euro au contribuable. Il me paraît important de le souligner, car, selon les informations que reçues du ministère de l'Intérieur, lorsque la solution de l'envoi d'un SMS était envisagée, les opérateurs souhaitaient faire payer ce type de solution. Mais, nous avons pris nos responsabilités et nous le faisons de la manière la plus directe possible.

Vous évoquez l'identité numérique. Il ne s'agit pas dans le cas présent de mettre en place une identité officielle comme peut le faire France connect, mais de proposer un service Dans les faits, il est possible d'utiliser ses identifiants Facebook pour se connecter à d'autres sites, sans avoir à recréer un profil. Nous avons considérablement augmenté les contrôles afin

de permettre aux utilisateurs de ne pas partager les données qu'ils ne souhaitent pas partager avec des tiers. Des audits sont également conduits à posteriori. En outre, si vous ne vous êtes pas connectés à un site utilisant vos identifiants Facebook pendant un certain temps - 100 jours il me semble - ce site ne peut plus user de vos données.

En 30 ans, internet a énormément changé. Aujourd'hui, on peut en quelques secondes envoyer à quiconque dans le monde des données, des fichiers, des photos. Ce constat a conduit à nos réflexions sur le Libra. Comment se fait-il qu'avec toute cette technologie, il y ait autant de difficultés pour transférer de l'argent d'un point A vers un point B à l'heure de l'économie et des services mondialisés ? Aujourd'hui, 1,7 milliard de personnes dans le monde sont exclues du système bancaire et sont dépendantes de transferts d'argent de leurs familles d'un pays vers un autre. Elles ont également besoin d'un accès au capital et d'un service monétaire. En utilisant la technologie blockchain, ainsi que d'autres technologies, nous avons annoncé la mise en place de cet outil en partenariat avec 27 autres membres très divers - UBER, Visa, Iliad - dont le nombre est appelé à augmenter. Je tiens immédiatement à préciser qu'il ne s'agit pas de la monnaie de Facebook mais de cette organisation regroupant plusieurs entreprises.

L'association Libra est une association indépendante au sein de laquelle Facebook dispose d'une voix parmi les autres. Elle est basée en Suisse et sera supervisée depuis ce pays. M. Marcus en a expliqué les raisons. Le Libra sera assis sur une « réserve libra », composée de plusieurs devises : le dollar, l'euro, le yen et la livre sterling, des monnaies étatiques. Je tiens à le préciser : sans monnaie étatique, il ne peut pas y avoir de Libra. Cet outil ne représente en rien une substitution de l'État, il ne fonctionnera qu'au sein du réseau Libra, mais il apportera de vraies facilités à des millions de personnes dans le monde. Vous m'interrogez sur la sécurité de cette nouvelle monnaie. Aujourd'hui, l'argent noir représente un réel problème. La cryptomonnaie n'est pas quelque chose de nouveau. Le bitcoin existe depuis plusieurs années. Il est utilisé sur le darkweb, à des fins diverses et variées, pour des bonnes ou de mauvaises raisons. Le Libra est une opportunité de disposer d'un service porté par de grandes entreprises connues et qui utilise la blockchain, une technologie traçable et transparente, contrairement à des paiements en cash ou via d'autres types de services numériques intraçables.

Il n'y aura pas de fusion des bases de données entre Facebook et Libra. Je tiens par ailleurs à souligner que nous lançons cet outil en toute transparence. Nous allons rencontrer les régulateurs, les gouverneurs des banques centrales, les entreprises, les gouvernements. Le G7 s'est saisi de cette question. Il en hors de question d'instaurer cette monnaie sauvagement, ou avant d'avoir obtenu les autorisations nécessaires. En effet, nous entrons dans un secteur où la culture de la régulation est très forte, et nous n'avons aucune raison de ne pas suivre cette régulation. Ce que nous proposons est

l'émergence d'un service de cryptomonnaie stable, globale, portée par des entreprises connues, et qui peut apporter un vrai bénéfice.

Vous avez évoqué, Monsieur le Président, la tribune de Mark Zuckerberg. Si nous devions refaire les règles de l'internet aujourd'hui, les pouvoirs publics auraient sans doute une approche différente. La gestion des contenus doit se faire en fonction de deux éléments : la loi et les conditions générales d'utilisation du service. Les lois sont supérieures aux conditions générales d'utilisation du service, car elles sont l'expression de la volonté générale. Nous avons participé à la mission lancée par le Président de la République et conduite par M. Loutrel. Nous avons largement ouvert Facebook, pour montrer ce que nous faisons en matière de modération et pour réfléchir collectivement à ce qui peut être amélioré. Le rapport de M. Loutrel et de son équipe rendu au mois de mai donne beaucoup de pistes en la matière. Par ailleurs, la proposition de loi de Mme la députée Laëtitia Avia visant à lutter contre la haine sur internet a été votée en première lecture à l'Assemblée nationale. Elle renforce la responsabilité des plateformes.

Le comité de supervision, proposé par Mark Zuckerberg, ne remet pas en cause ce principe. Ce dernier a utilisé l'expression de « cour suprême », pour illustrer l'outil qu'il veut mettre en place. Il vise à répondre à un problème régulièrement soulevé par les pouvoirs publics, parle milieu associatif et par les experts. Aujourd'hui, en cas de désaccord sur la suppression d'un contenu en vertu des conditions d'utilisation du service, la personne concernée peut faire appel de cette décision au sein de l'entreprise. Pour un certain nombre de cas - les plus compliqués -, c'est Mark Zuckerberg, seul, qui décide si le contenu respecte ou non les conditions générales et s'il doit être en conséquent supprimé. Nous proposons de transférer cette décision prise par un seul homme basé aux États-Unis à un groupe d'une quarantaine d'experts internationaux indépendants. Pour nous, cela représente objectivement un progrès. Nous avons organisé plusieurs dizaines de réunions dans de nombreux pays et nous avons notamment présenté cette solution à des experts et associations françaises. Nous avons des retours constructifs, certains très francs, nous permettant de réfléchir à un comité en capacité de fonctionner correctement. Il s'agit d'un outil propre à notre service, utilisé pour régler ses questions internes. Cette « cour suprême » ne viendra donc pas en conflit avec la Cour de cassation, le Conseil d'État, la Cour européenne des droits de l'homme ou la Cour de justice européenne.

M. Stéphane Piednoir. - Le Cloud Act permet aux autorités américaines de disposer des données que vous stockez, quel que soit le lieu de stockage. Cela inquiète légitimement les pouvoirs publics français car c'est tant les données personnelles que les données stratégiques des entreprises qui peuvent ainsi être pillées. Or, Facebook détient des données très précises sur 36 millions d'utilisateurs réguliers français. Pouvez-vous

nous assurer que Facebook ne permet ni ne permettra aux autorités américaines de prendre connaissance des données de nos concitoyens ? Comment comptez-vous concilier ces obligations avec les règles européennes protégeant les données personnelles (RGPD) ?

M. Anton'Maria Battesti. - Le Cloud Act est une réponse à un problème juridique. Le Mutual legal assistance treaty, qui permet la coopération judiciaire internationale, a été rédigé et signé à une époque où le numérique n'existait pas. Aussi, le traitement des demandes de données entre les deux rives de l'Atlantique pouvait prendre des mois. Le Cloud Act vise à remédier à ces difficultés. Je tiens toutefois à préciser qu'il s'appliquera uniquement sur demandes judiciaires. Il ne s'agit nullement d'une porte dérobée permettant à tout à chacun d'avoir accès aux données. Le quatrième amendement de la Constitution américaine continue à s'appliquer, tout comme l'ensemble des garanties apportées par l'État de droit américain. Par ailleurs, l'Union européenne se dote d'un instrument comparable, avec le règlement e-evidence. Le Cloud Act prévoit également la signature d'accords spéciaux entre les États-Unis et les autorités d'un pays afin de faciliter les échanges bilatéraux de données. Le Royaume-Uni a signé un tel accord et des discussions sont en cours avec d'autres pays européens. Notre entreprise multinationale souhaite ne pas avoir à affronter de conflit de droit. Nous ne pouvons qu'encourager de tels processus internationaux, permettant de déployer une nouvelle architecture juridique pour régler ces problèmes. Ce n'est pas à nous de les régler. Nous sommes en effet constamment sollicités pour plus de collaboration, pour transmettre les données nécessaires aux enquêtes. Nous voulons appliquer ces dispositifs avec le plus grand sérieux sur la base de règles édictées par les États. De même, nous mettons un point d'honneur à respecter le RGPD, pour plusieurs raisons : d'une part, les sanctions sont très dissuasives, d'autre part, et au-delà de la sanction légale et politique, l'application du RGPD est essentielle pour conserver la confiance de l'utilisateur.

Mme Catherine Morin-Desailly. - Je vais être très directe : peut-on encore faire confiance à Facebook, sachant que Mark Zuckerberg n'a pas dit la vérité devant le Congrès américain ? Un récent article du New York Times a démontré que Facebook était au courant de l'infiltration des Russes sur les réseaux dès 2014. Pourquoi est-ce que le comité exécutif, alerté, n'a pas pris toutes les mesures utiles pour faire remonter les informations vers les États concernés ? Quelles mesures ont été mises en place par Facebook afin d'empêcher une cyber-préemption du réseau social, qui doit rester partagé et neutre ?

En outre, pourquoi Mark Zuckerberg n'accepte-t-il jamais de se rendre aux convocations parlementaires ? Il n'a ainsi pas donné suite à l'invitation à participer à une audition à Londres lancée par 11 parlements. Or, vous pouvez mesurer l'inquiétude des parlementaires face à l'utilisation des données par Facebook dans l'affaire Cambridge Analytica.

Avec quelles entreprises d'agrégation travaillez-vous ? Une récente décision allemande interdit la collecte et l'agrégation des données pour atteindre un objectif particulier. Comment comptez-vous appliquer cette mesure, et retrouver ainsi la confiance de l'utilisateur ?

Enfin, aux États-Unis, des voix se font entendre - parlementaires, ingénieurs, Chris Hughes, le cofondateur de Facebook - plaidant pour une segmentation de l'entreprise. Nous savons qu'Instagram et Whatsapp sont corrélés à Facebook. Que répondez-vous à ces idées ? Ne serait-ce pas également une façon de retrouver la confiance de l'utilisateur ?

M. Anton'Maria Battesti. - Nous n'avons aucun intérêt à agir d'une façon qui nous ferait perdre la confiance des utilisateurs. De même qu'une compagnie aérienne n'est rien sans passager, Facebook n'est rien sans ses utilisateurs. La question n'est pas de savoir si nous avons fait des erreurs. Nous le savons ; des erreurs ont été faites. Mais des compagnies aériennes connaissent des tragédies aériennes et s'en remettent. Toutes les entreprises sont confrontées à des crises graves, entamant la confiance, et elles doivent y répondre.

Je ne commenterai pas l'article du New York Times ni vos commentaires sur le fait de savoir si Mark Zuckerberg aurait ou non menti.

En 2016, l'élection américaine a montré à quel point les outils que nous avions conçus pouvaient être détournés en période électorale. Qu'avons-nous fait depuis ? Nous avons mis en place des équipes qui travaillent à temps plein contre ces menaces. Nous détectons régulièrement des comportements de manipulation - en période électorale ou hors période électorale - et faisons tomber les pages concernées. Nous avons également rencontré les autorités françaises et mis en place un dispositif spécial pour les élections. Aux États-Unis, le recours aux publicités se fait dans un contexte différent. Nous nous sommes rendus compte lors de l'élection de 2016 que les publicités sur un réseau social pouvaient être utilisées pour cibler des personnes afin d'orienter leurs convictions politiques. Nous avons mis en place des mesures, permettant d'archiver ces publicités, de connaître l'identité des émetteurs ainsi que les montants dépensés. Nous visons un « phénomène vampire » : lorsque vous braquez la lumière sur quelque chose, vous espérez que le phénomène s'arrête. La loi sur la manipulation de l'information a repris ces dispositions pour la France et les a renforcées. Nous avons également pris nos responsabilités et mis en place les mêmes dispositions à l'échelle européenne, en l'absence d'ailleurs d'une réglementation européenne harmonisée en la matière. En tant qu'entreprise privée, nous avons donc dû prendre des mesures relevant sans doute de la sphère publique. Nous ne pouvons qu'inviter les pouvoirs publics européens à régler ces questions.

Face aux « fake news », nous avons également signé des partenariats avec des Fact Checkers - notamment Le Monde et l'AFP. Est-ce que cela

empêchera ces phénomènes de se reproduire ? Personne ne peut le dire, mais nous faisons tout pour que cela n'arrive pas.

Vous regrettez le fait que Mark Zuckerberg ne viennent pas aux convocations parlementaires. Laissez-moi vous rappeler qu'il est venu s'exprimer devant le Congrès américain et le Parlement européen la même année.

Mme Catherine Morin-Desailly. - Le groupe des 11 parlements regroupait également des pays qui n'étaient ni les États-Unis, ni membres de l'Union européenne.

M. Anton'Maria Battesti. - Mark Zuckerberg n'a fait aucune difficulté pour venir s'exprimer devant le Parlement européen, qui représente plus de 500 millions d'individus. Il a répondu aux questions posées par tous les groupes politiques et cette rencontre s'est faite dans un climat collaboratif. Je ne suis pas en capacité de vous dire comment il prend la décision de s'exprimer devant tel ou tel parlement. En revanche, pour l'Union européenne, il l'a fait devant le Parlement européen, et je suis sûr que personne dans cette salle ne remet en cause la légitimité de cette institution.

Vous m'interrogez sur une décision juridique allemande. Je ne dispose pas à cet instant des informations nécessaires pour répondre à cette question technique, car je suis en charge des affaires publiques de Facebook en France. En revanche, je reviendrai vers vous à la suite de cet entretien avec les éléments nécessaires.

Vous évoquez également l'opportunité de scinder Facebook en plusieurs entités. La réponse que je vais vous faire est proche de celle de Nick Clegg. Le droit de la concurrence a pour but d'éviter des abus notamment sur les prix, et permettre aux consommateurs d'avoir accès à des produits divers. Facebook ne doit pas être considéré comme un bloc monolithique. Nous ne sommes pas numéro un pour la messagerie, la vidéo ou encore en place de marché (market place). Lorsqu'on parle de concurrence, il faut regarder le périmètre des activités concernées.

En outre, le droit de la concurrence n'est pas conçu pour sanctionner le succès. Il y a deux milliards et demis d'utilisateurs de Facebook, un milliard d'Instagram et un milliard de Whatsapp. Même si les différents services étaient séparés, ils continueraient à former chacun d'entre eux, des gros blocs. Les problèmes seraient les mêmes. Le droit de la concurrence n'est pas la réponse à tous les problèmes de sûreté.

Mme Catherine Morin-Desailly. - Une séparation des différents services pourrait créer une forme d'émulation et recréer des conditions de confiance. Votre réponse est toujours la même : en l'absence de réglementation, vous rejetez la faute sur le politique, pour les usages, vous renvoyez aux utilisateurs. C'est toujours sous la contrainte que vous prenez des mesures d'autorégulation pour tenter de retrouver la confiance des

utilisateurs. Il faut agir de manière structurelle. Mon homologue britannique traite votre organisation de « gangster ». Je suis étonnée que vous ne travailliez pas avec votre homologue allemand, et que vous ne soyez pas au courant de cette régulation outre-rhin. Je suis frappée par cette absence de collaboration et d'approche stratégique au sein d'une grande entreprise internationale comme la vôtre. En outre, je vous ai adressé un courrier le 13 mars dernier, auquel je n'ai jamais eu de réponse.

M. Anton'Maria Battesti. - Je ne commenterai pas le terme de gangster que vous avez utilisé et vous en laisse la responsabilité. Je travaille en étroite collaboration avec mes homologues des autres pays européens. Cependant, je suis sous serment, et je ne veux pas apporter des propos inexacts ou incomplets. J'assume ne pas être au courant de tous les litiges que connaît Facebook en dehors du territoire français. Toutefois, je me suis engagé à vous apporter une réponse à la suite de cette audition.

Je suis désolé que vous n'ayez pas reçu de réponse à votre courrier du 13 mars dernier. Je vais me rapprocher de mes services.

M. Gérard Longuet, rapporteur. -. Je préside l'office parlementaire des choix techniques et scientifiques, où nous venons d'examiner le rapport de notre collègue député Didier Baichère sur la reconnaissance faciale, qui est un des aspects de la souveraineté numérique.

Vous êtes l'un des principaux investisseurs dans les câbles sous-marins. Dans quel esprit Facebook intervient-il dans ce domaine ? Jusqu'à présent, comme tous les opérateurs du numérique, vous utilisiez les réseaux existants. Quel est l'objectif de cette très forte implication : est-ce dans le but de disposer d'un maillage plus fin ? S'agit-il d'un manque de confiance envers les opérateurs, d'une insuffisance des services fournis ?

M. Anton'Maria Battesti. - Je répondrai également avec prudence. La compréhension que j'ai de cet investissement technologique est qu'il doit permettre - comme pour les investissements dans les centres de données - à notre service de fonctionner plus rapidement et au plus près de l'utilisateur. Nous avons signé un partenariat avec un opérateur - Orange il me semble - afin de déployer ces câbles. Toutefois, je ne connais pas les détails de ces programmes industriels.

M. Gérard Longuet, rapporteur. - Pourrez-vous nous transmettre une note d'orientation ? Ce réseau sera-t-il ouvert aux autres opérateurs ?

M. Anton'Maria Battesti. - Je reviendrai vers vous sur ces points. Il me semble que ce déploiement se fait de manière mutualisée avec d'autres opérateurs en raison des coûts importants.

M. Gérard Longuet, rapporteur. - Facebook a fait retirer de ses pages L'origine du monde de Courbet. Le président de la République va se rendre bientôt à Ornans. Notre collègue député Hervé Novelli, président des

amis de Courbet, a été particulièrement ému par cette censure, alors que Facebook est beaucoup plus laxiste pour d'autres sujets de contrebande.

M. Anton'Maria Battesti. - Laissez-moi tout d'abord vous indiquer que Facebook ne fait preuve d'aucun laxisme vis-à-vis de la contrebande.

Pour le Courbet, j'ai rencontré le plaignant. Cette affaire a été très médiatisée.

M. Gérard Longuet, rapporteur. - Au-delà de cette affaire, se pose la question de la censure et du centre de gravité des valeurs culturelles portées par Facebook.

M. Anton'Maria Battesti. -Je tiens à le réaffirmer devant vous. Ce tableau est autorisé, et de manière générale, la peinture de nu est autorisée. Ce tableau est assez réaliste et il y a eu une erreur de modération sur ce tableau.

M. Gérard Longuet, rapporteur. - Que représentent vos équipes de modération ?

M. Anton'Maria Battesti. - On accuse souvent Facebook de promouvoir des valeurs puritaines américaines. Ce qui n'est pas autorisé est la nudité sur les photos, afin de lutter contre la pornographie, mais aussi pour protéger les adolescents victimes de revenge porn. Or, à partir du moment où toute photo de nudité est interdite, nous disposons d'une arme forte pour lutter contre ces pratiques. Certes, il y a la question de la photo d'art, et nous reconnaissons que cette difficulté n'est pas résolue.

Nous avons 30 000 modérateurs dans le monde. Nous avons investi des milliards d'euros dans ce domaine. Pour vous donner un ordre d'idée, les montants investis dans la modération sont similaires à la capitalisation de Facebook au moment de son entrée en bourse. Par ailleurs, lorsque vous être propriétaire de plusieurs réseaux sociaux, vous pouvez mutualiser cette question. Les modérateurs couvrent l'ensemble du réseau, 24 heures sur 24, dans une centaine de langues.

Ce sont 85 % des utilisateurs de Facebook qui ne sont pas américains. Ce serait donc une erreur de copier-coller le modèle de valeurs américain au reste du monde. La politique de contenus de Facebook met en balance la liberté et la responsabilité, la liberté et la sécurité.

M. Gérard Longuet, rapporteur. - Vos modérateurs sont-ils répartis partout dans le monde ?

M. Anton'Maria Battesti. - En effet. Le quotidien Le Monde a d'ailleurs récemment publié un article sur l'équipe située à Barcelone. Une autre équipe se trouve à Dublin. Je suis également impliqué dans des décisions de licéité de contenus. Enfin, nous avons des experts dédiés à certains contenus, notamment des personnes qui ne surveillent que les contenus à caractère terroriste.

M. Gérard Longuet, rapporteur. - Qu'en est-il de l'interopérabilité entre réseaux sociaux ?

M. Anton'Maria Battesti. - Le RGPD donne le droit à l'utilisateur de pouvoir télécharger l'intégralité de ses données de manière simple et standardisée. C'est la première étape, la portabilité. Mais, une fois cette procédure faite, peut-il facilement mettre ses données ailleurs ? Une initiative industrielle, construite notamment avec Microsoft et Twitter, le Data Transfert project, est en cours. Elle vise à mettre en place les mécanismes techniques nécessaires pour transférer facilement les photos et données d'un site, d'un opérateur vers un autre. C'est également un moyen de disposer d'une concurrence plus forte entre réseaux sociaux. Toutefois, cette interopérabilité pose de nombreux problèmes, par exemple vis-à-vis de la vie privée. Ainsi, mes données Facebook peuvent impliquer d'autres personnes. Si ces dernières sont d'accord pour qu'un tel lien apparaisse sur Facebook, le sont-elles encore pour une utilisation en dehors de notre réseau ?

M. Pierre Ouzoulias. - Vous avez récemment ouvert un laboratoire d'intelligence artificielle à Paris. Vous avez recruté de nombreux chercheurs venant de l'INRIA (institut national de recherche dédié aux sciences du numérique) ou du CNRS (Centre national de la recherche scientifique). Quelle rémunération moyenne annuelle leur versez-vous ?

M. Anton'Maria Battesti. - Je ne suis pas informé du montant des rémunérations versées. En revanche, il est certain qu'il faut être extrêmement attractif dans des domaines aussi compétitifs.

M. Pierre Ouzoulias. - Votre société a mis à profit un internet libre. La faiblesse des règles d'organisation a permis votre expansion. Ce n'est pas un reproche mais un constat. Aujourd'hui, on risque de perdre cette liberté, et les règles d'autorégulation pourraient régir un internet qui ne serait plus libre et vous placeraient en situation de régulateur absolu de tout l'internet. Quelles mesures prenez-vous pour préserver cette liberté dont nous avons besoin ?

M. Anton'Maria Battesti. - Internet a connu une phase d'intense expansion. À l'époque, j'utilisais Netscape sur Windows 98 pour aller sur Yahoo. Cette période est révolue, et de nouveaux produits apparaissent constamment. D'ailleurs, si vous demandez aux jeunes aujourd'hui quel réseau ils utilisent de Facebook en Tik tok, ce dernier a leur préférence. On constate une diversification des usages, notamment chez les jeunes. Il semble que nous arrivons aujourd'hui dans une phase plus institutionnelle, plus régulée de l'internet. Est-ce que cela ne va pas conduire à installer les acteurs déjà présents ?. C'est toute la problématique des barrières à l'entrée d'un secteur.

Il existe ici une contradiction entre les demandes, d'une part, de conserver un internet libre, et d'autre part, de faire preuve de plus de

responsabilité éthique et légale. Dites-nous l'équilibre que vous souhaitez, les responsabilités que vous voulez nous transférer, et nous le ferons sous la responsabilité d'autorités comme le CSA.

En outre, lorsque vous nous demandez de décider de ce qui est légal ou non en 24 heures, c'est un petit transfert de souveraineté. On nous demande de faire quelque chose qui est plutôt du ressort de l'État. Mais dans le même temps, on nous accuse d'avoir trop de pouvoir. La seule façon de sortir de cette contradiction serait un cadre européen. Sinon, nous serons toujours dans l'excès, d'un côté ou de l'autre. De même, face aux barrières à l'entrée, on peut imaginer des règles plus souples pour les start-ups. Attention toutefois à la problématique du franchissement des seuils !

M. Franck Montaugé, président. - Je reviens au projet Libra. Pourquoi devrions-nous vous faire confiance pour la protection nos données financières eu égard aux échecs que vous avez déjà rencontrés dans ce domaine ? M. Marcus a annoncé qu'il n'y aurait pas, « mais pour le moment seulement », de transfert de données entre le Libra et Facebook, sauf consentement de l'usager. Peut-on avoir des garanties sur ce point ?

Êtes-vous favorable à une supervision publique des plateformes, par les États ou des organisations internationales comme l'Union européenne ?

M. Anton'Maria Battesti. - Nous ne sommes pas naïfs. On sait que la pente est raide en matière de confiance, et qu'une fois perdue, il est très difficile de la regagner. De manière générale, la confiance dans les institutions financières est assez faible. Facebook est conscient de l'image générale de ce secteur. David Marcus a présidé Paypal, il a une vraie légitimité en la matière et il a conscience des difficultés.

Il faut changer la méthode. Si vous lancez un produit, puis que vous en discutez après avec les autorités, cela pose problème. Cela a pourtant été la méthode la plus fréquemment utilisée par la Silicon Valley. Je ne remets pas en cause cette période, qui a été caractérisé par un foisonnement d'innovations. Dans le cas présent, nous proposons un renversement de la méthode de travail : cet outil ne sera pas lancé tant que nous n'aurons pas l'accord pour le faire. En matière financière, les barrières à l'entrée sont importantes, et à juste titre, car il y a un risque systémique. On ne pourra pas nous croire sur parole. Aussi, le lancement du Libra se fera sous les auspices de ceux qui ont la légitimité pour nous en donner l'autorisation et pour contrôler ce que nous ferons. C'est seulement dans ces conditions que la confiance pourra s'installer.

Vous m'interrogez sur les données. Mon banquier sait tout de moi. Il sait où je suis allé, à quelle heure, ce que j'ai acheté. Sur les applications bancaires, il est possible de classer ces dépenses par catégorie. Le RGPD nous indique comment développer de nouveaux services. Si nous avons le consentement des usagers, nous pouvons le faire. Le RGPD ne dit à aucun moment que l'on ne peut plus rien faire ! Ce texte s'inscrit dans une logique

de responsabilisation et de sanction. On ne peut rien faire sans l'aval du régulateur. Nous n'avons pas le choix, nous devons demander l'autorisation avant d'agir. D'ailleurs, je ne peux qu'inciter les pouvoirs publics à muscler les régulateurs, à faire en sorte qu'ils soient vraiment en concurrence avec nos entreprises pour attirer les nouveaux talents et recruter les meilleurs. En outre, les serviteurs de l'État peuvent se nourrir d'une expérience du privé.

Nous sommes favorables à une supervision des plateformes. Il faut une régulation complète sur des domaines qui touchent à la vie démocratique telles que les publicités politiques, mais aussi le contrôle des contenus, le transfert de données etc. Faites-le ! Nous nous inscrivons dans une logique de proposition et de dialogue.

Mme Catherine Morin-Desailly. - Dans nos réflexions sur la loi contre la manipulation de l'information, nous nous sommes interrogés sur la rentabilité de la diffusion des fausses nouvelles. Le clic est rémunérateur. Les plateformes bénéficient d'un régime de non-responsabilité et de non-redevabilité. Que pensez-vous de la proposition qui est faite de rouvrir la directive e-commerce, qui n'est plus adaptée ? Cela permettrait de réfléchir à un nouveau statut pour les plateformes, entre hébergeurs et éditeurs, afin de restaurer la confiance et la redevabilité.

M. Anton'Maria Battesti. -La loi pour la lutte contre la manipulation de l'information est nécessaire pour combler les manques identifiés par les pouvoirs publics. Le CSA aura un rôle de supervision de nos obligations de moyens de lutte contre la fausse information. Ce travail a déjà commencé. Ce modèle a vocation à s'étendre à d'autres pays et d'autres sujets.

Mme Catherine Morin-Desailly. - Le Sénat a rejeté cette loi car les solutions proposées ne nous convenaient pas.

M. Anton'Maria Battesti. - Je pense que le Sénat a manqué une opportunité d'améliorer ce texte. Votre institution a toujours été protectrice des libertés publiques. J'ai ainsi toute confiance dans le Sénat pour apporter sa contribution. La directive e-commerce a déjà été remodelée par d'autres textes : la directive copyright, la directive service média audiovisuel. Il faut une approche plus holistique, reposer la question du statut. Je trouve la démarche de la mission Loutrel très intéressante sur ces sujets.

M. Franck Montaugé, président. - Je vous remercie Monsieur pour les éléments de clarification que vous nous avez apportés.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible en ligne sur le site du Sénat.

Audition de MM. Marc Mossé, directeur juridique et affaires publiques de Microsoft Europe et Mathieu Coulaud, directeur juridique de Microsoft France,
le 18 juillet 2019

M. Franck Montaugé, président. – Notre commission d'enquête poursuit ses travaux avec l'audition des représentants de Microsoft. Nous recevons Monsieur Marc Mossé, directeur juridique et des affaires publiques de Microsoft Europe, et Monsieur Mathieu Coulaud, directeur juridique de Microsoft France.

Cette audition sera diffusée en direct sur le site Internet du Sénat. Elle fera également l'objet d'un compte rendu publié.

Enfin, je rappelle pour la forme qu'un faux témoignage devant notre commission d'enquête serait passible des peines prévues aux articles 434-13, 434-14 et 434-15 du code pénal. Je vous invite chacun à tour de rôle à prêter serment de dire toute la vérité, rien que la vérité ; levez la main droite et dites : « je le jure ».

Conformément à la procédure applicable aux commissions d'enquête, MM. Marc Mossé et Mathieu Coulaud prêtent serment.

M. Franck Montaugé, président. – Nous connaissons tous les activités de Microsoft, du moteur de recherche au cloud en passant par les logiciels de bureautique, la messagerie électronique… C'est pourquoi je vous invite avant tout à répondre aux questions que nous avons à vous poser.

Je commencerai par deux questions relatives aux données. Le Cloud Act permet aux autorités américaines d'accéder aux données que vous stockez, quel que soit le lieu de stockage ce qui inquiète légitimement les pouvoirs publics français puisque tant les données personnelles que les données stratégiques des entreprises peuvent ainsi être pillées. Or, de grands groupes vous confient leurs données, en utilisant vos solutions de cloud, à l'image de la SNCF, ou nouent des partenariats commerciaux avec vous comme Thalès ou Qwant.

Pouvez-vous nous assurer que Microsoft ou ses filiales ne permettent pas – et ne permettront pas – aux autorités américaines de prendre connaissance des données de nos concitoyens et de nos entreprises ? Comment comptez-vous concilier ces obligations avec les règles européennes protégeant les données personnelles, avec le RGPD ?

Microsoft a récemment changé de discours sur la protection de la vie privée en faisant de ce sujet un de ses axes stratégiques. Une autorité locale allemande vient pourtant de constater une infraction au RGPD la semaine dernière puisque l'utilisation du logiciel bureautique Microsoft Office 365 dans les écoles du Land de Hesse a été déclarée illégale au regard de la loi

sur la protection des données. Les données personnelles des enfants seraient stockées dans le cloud de Microsoft de façon peu transparente et peu accessible aux autorités américaines. Devons-nous croire les paroles ou les actes ? Cette question est très importante, car Microsoft est également prestataire pour le ministère de l'Éducation nationale en France.

M. Gérard Longuet, rapporteur. – Ce sujet est majeur. Je me réjouis que soient présents ce jour un responsable national et un responsable Europe, ce qui permet d'avoir une vision globale de la question.

M. Marc Mossé, directeur juridique et affaires publiques de Microsoft Europe. – Je vous remercie de nous donner la possibilité de répondre à un certain nombre de questions, souvent posées, parfois complexes, pour lesquelles il est utile d'apporter des précisions et des éléments de contexte.

Pour répondre à la première question relative au Cloud Act, je souhaite effectuer un retour en arrière. Avant l'adoption de cette loi, Microsoft était déjà un acteur important du contentieux autour de l'accès aux données stockées en Europe puisque nous nous sommes opposés à une demande formulée par une autorité de poursuite américaine pour des données hébergées en Irlande. Nous nous y sommes opposés pour deux raisons principales : il nous apparaissait que la demande était formulée d'une part en méconnaissance du droit de la protection des données et de la vie privée alors applicable en Europe, même avant le RGPD, et d'autre part en méconnaissance de la souveraineté de l'État irlandais, étant considéré qu'il existait des procédures de coopération judiciaire internationales pour permettre l'accès à ces données afin de satisfaire les besoins de l'enquête criminelle en question.

Cette affaire nous a conduits devant la justice américaine – puisque nous nous opposions au gouvernement américain – et la Cour d'appel de New York nous avait donné raison, dans un arrêt important. L'affaire a ensuite été portée devant la Cour suprême des États-Unis qui a accepté de l'examiner – ce qui témoigne de l'importance de la question, puisque la Cour suprême choisit d'accepter ou non de traiter telle ou telle affaire. Le Cloud Act est donc intervenu après notre opposition à cette demande d'accès aux données, et après que nous avions fait valoir devant les juridictions américaines nos arguments tirés à la fois de la protection des droits fondamentaux et de la souveraineté des États.

Notre position en la matière n'est donc pas récente, elle était formée bien avant la modification de la législation américaine.

Avant que la Cour suprême ne rende sa décision, une modification du droit américain est intervenue via le Cloud Act qui a eu vocation à régler une partie des questions soulevées par cette affaire. En conséquence, la procédure devant la Cour suprême s'est arrêtée et le Cloud Act a fixé de nouveaux principes.

Le Cloud Act n'a pas modifié les règles d'attribution de juridiction américaine, mais a essayé de régler la question de l'accès à des données stockées en dehors des États-Unis en clarifiant certaines règles. Le Cloud Act aspire à établir une balance équilibrée entre la protection des droits fondamentaux, dont la vie privée, et l'efficacité des enquêtes criminelles et pénales, pour préserver la sécurité. C'est un texte de procédure criminelle. Il n'autorise pas un accès indéfini et indéterminé à l'ensemble des données, mais uniquement dans le cadre d'une poursuite et d'une infraction, pour des données déterminées qui peuvent effectivement être stockées à l'étranger.

Le Cloud Act connaît d'une certaine façon en Europe un texte miroir en cours d'adoption avec le projet de règlement « e-evidence » sur l'accès aux preuves électroniques stockées dans un des 28 autres États membres de l'Union européenne. Le Cloud Act envisage expressément la conclusion d'accords entre les États-Unis et d'autres États pour fixer un cadre et déterminer une balance entre les différents droits lorsqu'il s'agit d'accéder à des données dans le cadre d'une enquête criminelle. L'objectif de ce texte vise à établir un cadre adapté au XXIe siècle, avec des données pouvant être stockées dans différents États et où les enquêtes doivent parfois être menées rapidement, dans le respect des droits et libertés fondamentaux.

En résumé, l'accès aux données via le Cloud Act, ne peut se faire que dans le cadre d'investigations criminelles, pour des données précises et déterminées, et non pour un accès généralisé. Il reste encore à parfaire ce cadre avec l'adoption du règlement européen sur la preuve électronique et un accord éventuel entre les États-Unis et l'Union européenne, puisqu'un mandat de négociation en ce sens a été confié à la Commission….

M. Mathieu Coulaud, directeur juridique de Microsoft France. – … Et ayons bien en tête la hiérarchie des normes américaines. Le Quatrième Amendement de la Constitution des États-Unis a été écrit à la suite du traumatisme des colons américains – les Britanniques ayant le droit d'entrer dans les maisons sans préavis et sans aucun contrôle d'une autorité judiciaire. Le Code de procédure criminelle est donc placé sous l'égide du Quatrième Amendement, et il contient lui-même le Stored Communications Act, qui fixe le régime juridique d'une donnée stockée. C'est ce dernier texte que le Cloud Act est venu amender. Tout ceci correspond à peu près à notre code de procédure pénale ou à notre code pénal. Le Cloud Act intervient donc dans un cadre juridique très déterminé.

M. Marc Mossé. – Nous sommes effectivement dans le cadre d'une procédure sous le contrôle d'une autorité judiciaire indépendante.

Concrètement, si un mandat est demandé, il appartient au juge indépendant de décider ou non de le mettre en œuvre. Le Procureur demandant le « warrant » on mandat devra démontrer qu'il existe de sérieuses présomptions d'une infraction, justifiant que les données visées se trouvent sur le compte ou l'espace de stockage de la personne concernée.

C'est sur ces bases que le juge se déterminera pour délivrer un mandat, et sur la base de ce mandat que nous répondrons, ou non, à la demande.

Le département de la Justice américaine a publié, en avril 2019, un Livre blanc comportant une série de recommandations et principes directeurs permettant d'éclairer la manière de mettre en œuvre ce texte. Une des recommandations vise à demander aux Procureurs fédéraux de s'adresser d'abord directement à l'entreprise dont ils souhaitent obtenir les données, l'intermédiaire technique n'étant sollicité que subsidiairement, si l'enquête l'exige.

M. Franck Montaugé, président. – Qu'en est-il de la communication des avis juridiques internes de nos entreprises ?

M. Marc Mossé. – C'est un excellent exemple, mais le Cloud Act n'est pas spécifiquement en cause sur ce point : c'est, de façon générale, le droit français qui est trop faible, indépendamment de l'évolution de nos pratiques numériques. En effet, les avis des juristes internes des entreprises en France ne bénéficient malheureusement pas du principe de confidentialité, alors que les juristes de la plupart des grands États en bénéficient – soit 18 ou 20 États de l'Union européenne il me semble. Indépendamment du Cloud Act, les documents que vous évoquez sont donc effectivement moins bien protégés en France.

Dans le projet de règlement européen « e-evidence » sur les preuves électroniques que j'évoquais, un article spécifique prévoit que les données protégées par une immunité ou un privilège fassent l'objet de garanties supplémentaires. Dans le droit européen, entre États membres de l'Union européenne, les entreprises françaises seront donc effectivement moins bien protégées que leurs concurrentes d'autres pays de l'Union européenne.

M. Gérard Longuet, rapporteur. – Cette question précise pourrait donc très bien être réglée par le Parlement français…

M. Marc Mossé. – Les rapports suggérant d'instaurer la confidentialité pour les juristes d'entreprise ne manquent pas. Le dernier est celui de Monsieur le député Raphaël Gauvain.

J'en reviens à la procédure de demande de données dans le cadre du Cloud Act. Si le Procureur s'adresse directement à nous, pour les besoins de l'enquête, en demandant l'accès à des données précises, nous nous sommes engagés à informer notre client de cette demande, sauf dans l'hypothèse où cela nous serait expressément interdit, ce qui est prévu dans certaines conditions, elles-mêmes précisément qualifiées – risque pour l'intégrité physique ou la vie d'une personne, intérêt de l'enquête…. Si nous ne pouvons informer notre client, il nous reste la possibilité de considérer que la demande n'est pas fondée, soit parce qu'elle n'est techniquement pas réaliste, soit parce que les données ne sont pas stockées chez nous, soit parce que nous considérons qu'il existe un conflit de loi entre la demande et le droit français – loi protégeant les données en application du RGPD, ou future

« loi de blocage » si par exemple les préconisations du rapport Gauvain étaient retenues.

Nous pourrions alors envisager deux options dans le cadre du Cloud Act. En l'absence d'accord négocié entre les États-Unis et l'Union européenne, comme c'est le cas actuellement, et si nous considérons qu'il existe un vrai risque de conflit de lois, nous pouvons nous y opposer devant le juge américain à travers la procédure de « comity analysis » – principe de courtoisie internationale en Common Lawi – par lequel le juge, pour régler un conflit de lois et mettre en œuvre le droit international, procède à la balance entre un certain nombre de critères : l'intérêt des États-Unis dans l'obtention de ces preuves, les intérêts protégés par les lois de la France, et l'existence de moyens d'obtenir autrement ces preuves dans un délai raisonnable pour le bon déroulement de l'enquête. Aujourd'hui, en l'absence d'executive agreement entre les États-Unis et l'Europe, si la question se posait, nous pourrions fortement envisager de nous opposer à une demande d'accès dès lors que nous serions face à un conflit de lois fort, net et précis.

Concernant le RGPD en particulier, la question s'est posée devant la Cour suprême : Dans un mémoire en intervention déposé par la Commission européenne, cette dernière évoquait l'article 48 du RGPD qui constituait un conflit de lois… même si elle indiquait par ailleurs qu'une exception pouvait exister au titre de l'article 49. Cela affaiblissait quelque peu le conflit de lois constaté, alors que nous avons besoin d'une divergence précise, réelle et conséquente pour convaincre le juge américain…

Si la même question se posait demain et qu'un « executive agreement » avait pu être négocié entre les États-Unis et l'Union européenne, c'est cet accord qui fixerait précisément les règles de communication des preuves électroniques et anticiperait les difficultés, en fixant notamment les critères appliqués par le juge américain. Ce sont ces « executive agreements » qui ont vocation à préciser les règles et à établir la balance entre la protection des droits fondamentaux, dont la protection des données, et les nécessités d'une enquête au titre de la protection de la sécurité publique.

La position de Microsoft devant la Cour suprême – visant à protéger les données stockées en Europe – demeure, même si le cadre a évolué. Nous protégeons les données de nos clients : premièrement en répondant aux autorités qui nous sollicitent qu'il faut demander ces données directement aux clients, deuxièmement en avertissant nos clients si nous sommes saisis d'une telle demande, et troisièmement en envisageant fortement de nous opposer à une telle demande en cas de conflit de loi précis et clair.

M. Franck Montaugé, président. – Merci de ces éclaircissements, mais êtes-vous en mesure de fournir des éléments de preuve de cette manière de procéder ?

M. Marc Mossé. – Nos contrats contiennent de tels éléments, et en pratique nous nous y sommes déjà opposés, en portant l'affaire jusqu'à la Cour suprême !

M. Mathieu Coulaud. – Nos contrats comprennent effectivement une clause stipulant que « Microsoft ne fournit pas : a) un accès direct, indirect, général ou libre aux données clients ; b) les clés de chiffrement utilisées pour sécuriser les données clients ou la possibilité de forcer ce chiffrement ».

Nous reportons donc la responsabilité du dialogue entre l'autorité d'enquête et notre client sur leur relation bipartite. Nous ne souhaitons pas être au milieu de ce dialogue.

Le chiffrement constitue aussi une possibilité : chaque entreprise doit se protéger des cyberattaques, ce qui peut passer par le chiffrement, avec des clés créées pour accéder les données. À un certain niveau de chiffrement, le client est seul maître du déchiffrement et même Microsoft ne peut alors accéder aux données du client.

Il faut bien distinguer les données du client de l'infrastructure. Le Cloud computing offert par Microsoft correspond au stockage informatique, via une infrastructure – ou ferme de serveurs –de données qui appartiennent au client. C'est le client qui définit le degré de chiffrement de ses données...

M. Gérard Longuet, rapporteur. – …C'est lui qui le conçoit ?

M. Mathieu Coulaud. – Tout à fait, en fonction du service qu'il achète, il a la possibilité de prévoir le chiffrement de ses données, dont il détient lui-même les clés, via son responsable de la sécurité informatique. Dans ce cas, nous ne sommes pas en mesure de fournir une donnée déchiffrée – et nous nous engageons contractuellement à ne pas la fournir aux autorités.

M. Franck Montaugé, président. – Concernant ma question portant sur ce qui s'est passé en Allemagne ? Les faits sont-ils avérés ?

M. Marc Mossé. – C'est l'autorité en charge de la protection des données du Land de Hesse qui est à l'origine de ces questions, dont je ne connais pas les détails. Nous avons pour principe d'entrer en dialogue avec le régulateur qui nous interroge. Nous avons mis en œuvre le RGPD, pas simplement en Europe, mais aussi dans le monde entier puisque l'Europe a ainsi fixé un standard international. Nous allons clarifier ces questions et résoudre la difficulté si elle existe.

Au-delà des textes mis en œuvre, la protection des données personnelles est un sujet compliqué et assez nouveau : même si des normes existaient avant le RGPD,, pendant longtemps, personne n'y portait une attention si conséquente. Nous nous sommes engagés très tôt sur la protection de la vie privée, nous étions ainsi les premiers à mettre en œuvre les clauses contractuelles types de la Commission européenne dans les

contrats de cloud qui nous semblaient tout à fait importants. Il est heureux que cette question de protection de la vie privée fasse désormais partie des questionnements quotidiens et de la culture économique.

Différents modèles économiques existent dans le numérique : le nôtre n'est pas fondé sur la publicité. Nous sommes plutôt dans des logiques de « B2B » et de « B2B2C », c'est-à-dire de partenariats et d'écosystèmes. Ces questions se trouvent au cœur de notre modèle et supposent que, par des preuves concrètes, nous puissions inspirer confiance à nos clients.

M. Gérard Longuet, rapporteur. – Vous considérez que votre modèle économique repose sur la vente de prestations et non du patrimoine ou des données de vos clients.

M. Marc Mossé. – Les données de nos clients restent leurs données. Nous n'avons pas vocation à nous les approprier et à en faire le commerce.

Certes nous évoluons dans une économie de données. De nombreuses entreprises traditionnelles vont devenir des entreprises digitales – dans le monde de l'automobile, de la santé ou même de l'agriculture. Un usage des données existe pour apporter des bénéfices – notre outil Skype dispose ainsi d'une fonctionnalité Skype translator de traduction simultanée, à travers l'apprentissage par la machine de données des langues utilisées. Il ne s'agit pas d'écouter les conversations, mais d'utiliser la donnée pour que la machine apprenne et sache traduire. C'est de l'exploitation de la donnée, non pas à des fins de commercialisation de vos données, mais pour améliorer nos produits, créer des fonctionnalités et les sécuriser.

Nous sommes effectivement dans un monde d'usage de la donnée, puisque l'intelligence artificielle suppose de la donnée. C'est une question de souveraineté numérique : pour que l'Europe et la France puissent avancer et accroître leur compétitivité dans cette révolution industrielle portée par le numérique, il faut que les entreprises accèdent à la donnée et utilisent la donnée. Les voitures connectées se développent sur la base de la donnée. Il existe toutefois une différence entre la collecte et l'utilisation de la donnée à des fins pertinentes pour l'utilisateur ou l'industriel qui développe des solutions et l'usage abusif des données.

M. Gérard Longuet, rapporteur. – Est-ce que le critère de distinction n'est pas de savoir qui paie ? Le service que vous évoquez de traduction simultanée est bien payé par l'utilisateur, et quand il l'utilise.

M. Mathieu Coulaud. – Absolument. Notre modèle repose sur un accès pour l'utilisateur à l'infrastructure cloud, avec de l'hébergement pur, puis, selon le contrat souscrit, à des briques logicielles. Le client utilise alors ce qu'il souhaite dans le cloud : c'est ce qu'on appelle le « Software as a Service » – les logiciels Word et Excel de la suite Microsoft Office peuvent ainsi être offert au client dans ce cloud, et utilisés depuis l'ordinateur de notre client. Toutes nos briques logicielles, y compris de « machine learning », fonctionnent de la même manière.

Une distinction doit être faite également entre notre rôle de fourniture d'infrastructures et celui de l'intégrateur. Nous intervenons en amont, en vendant l'infrastructure et éventuellement les briques de logiciel, protégées par le droit d'auteur, tandis que l'intégrateur fait communiquer nos outils avec les outils du client final. Nous nous vivons plutôt comme un fournisseur de propriété intellectuelle.

M. Gérard Longuet, rapporteur. – Quel est le statut de l'intégrateur ?

M. Mathieu Coulaud. – Il a un statut commercial et c'est souvent un partenaire de Microsoft. Il contracte avec le client final pour brancher notre système sur celui du client. Nous avons un écosystème de 10 500 partenaires qui sont les premiers à vendre nos produits et services. Il peut même s'agir d'une filiale, comme Microsoft Services.

M. Franck Montaugé, président. – En 2015, votre entreprise annonçait avoir débloqué une somme conséquente de 70 millions d'euros au service de la French Tech. Quel a été exactement le montant investi ? Dans quelles startups avez-vous investi ? Avez-vous pris des participations, majoritaires ou pas, dans ces entreprises ?

M. Marc Mossé. – Nous avons effectivement annoncé en 2015 cette aide à l'écosystème français. Je ne connais pas le chiffre précis. Nous avons un modèle de support aux startups qui ne passe pas par des prises de participation. Nous les aidons à se développer, à grandir et à accéder à des réseaux de clients nationaux ou internationaux ou à nos partenaires. Avant même cette annonce de 2015, nous avions déjà des programmes autour des startups qui ont permis à certaines de devenir des géants mondiaux, comme Criteo ou Talentsoft.

M. Gérard Longuet, rapporteur. – Comment vivez-vous votre relation avec Criteo ?

M. Marc Mossé. – Le programme IDEES avait été créé pour aider les startups à démarrer et Criteo comme Talentsoft ont intégré ce programme. Ces startups n'y restaient que trois ans au maximum et vivaient ensuite leur vie. C'était une forme d'accélérateur.

Ces mécanismes ne reposent pas sur des prises de participation.

Pour répondre à votre question sur les investissements, nous avons conclu un partenariat avec Station F et avons focalisé nos efforts d'aide aux startups sur la question de l'intelligence artificielle. Les startups que nous aidons dans le cadre de Station F travaillent toutes dans le domaine de l'intelligence artificielle, principal vecteur de développement de l'économie numérique.

À l'origine de ces programmes se trouve notre refus du discours selon lequel la France aurait perdu la bataille du logiciel et ne pourrait se développer dans ce domaine, coincée entre la Chine et les États-Unis. Nous

considérons au contraire que la France est une terre du logiciel : les succès de la Silicon Valley reposent souvent sur un ingénieur français et Microsoft compte de nombreux ingénieurs français. Il existe en effet une école informatique française et une école mathématique française très puissantes. L'INRIA a une réputation mondiale de ce point de vue et nous avons un partenariat avec elle depuis 2006. Nous nous étions battus contre cette idée que nous aurions perdu cette bataille et nous voulions démontrer qu'il existait un écosystème et les talents en France. Je pense que ces programmes ont pu permettre l'éclosion de certains succès.

La France et l'Europe n'ont pas perdu la bataille de l'intelligence artificielle. L'Europe porte des valeurs qui peuvent clairement cadrer un certain nombre d'évolutions sur le respect des droits et libertés, comme avec le RGPD. Une bonne partie de la révolution industrielle repose non pas simplement sur l'économie numérique mais sur le développement de nos grandes entreprises et PME qui peuvent, grâce au numérique, devenir des acteurs de cette économie.

Nous avons développé des actions pour l'intelligence artificielle en France, avec une vingtaine d'écoles à horizon 2021, et avec des partenaires comme Orange ou Capgemini. Dans le cadre du service civique, nous prévoyons de sensibiliser un million de jeunes au numérique. De nombreuses actions peuvent être menées pour ne pas perdre cette bataille du numérique.

M. Gérard Longuet, rapporteur. – Quel niveau de formation visez-vous dans ces écoles ?

M. Marc Mossé. – Les écoles sont sans prérequis. La première est celle d'Issy-les-Moulineaux, avec 24 étudiants. La scolarité comprend 7 mois de scolarité et 12 mois en alternance. Tous les jeunes ont trouvé un emploi, sauf un… qui a créé sa startup. Nous souhaitons implanter des écoles sur les territoires et avons déjà des écoles à Nantes, Castelnau-le-Lez, Biarritz, Lyon… L'objectif est de former des jeunes avec des partenaires, modèle qui peut être dupliqué dans d'autres pays d'Europe.

La nouvelle Présidente de la Commission européenne parlait d'un triplement du programme Erasmus + et des pistes méritent effectivement d'être explorées, notamment pour l'apprentissage, mais aussi pour les salariés déjà en poste dont les métiers vont se transformer. La souveraineté passe aussi par l'importance accordée à la question de la formation qui doit être prioritaire. La transformation digitale constitue une chance pour nos entreprises.

M. Franck Montaugé, président. – Vous détenez un moteur de recherche qui fonctionne, lui, très classiquement dans ce secteur, sur le modèle de l'économie de l'attention, avec des publicités ciblées et l'exploitation des données personnelles. Pensez-vous qu'avec une confiance

accrue à l'égard des internautes, il serait possible de se passer de la publicité ciblée pour concevoir une logique de moteur de recherche différente ?

M. Marc Mossé. – Nous avons conclu un partenariat avec Qwant, moteur de recherche français dont l'approche est celle que vous évoquez. Nous lui fournissons des capacités technologiques – puisque nous lui permettons d'être sur notre Plateforme Azure pour renforcer la capacité de calcul.

Plusieurs modèles existent, qui répondent aux attentes diverses des citoyens. L'intérêt du positionnement de Qwant est de montrer qu'il existe des alternatives. Imaginer d'autres façons de pratiquer la recherche sur Internet constitue une piste intéressante. C'est un écosystème en évolution permanente, la compétition est très forte et il convient de répondre aux aspirations des citoyens.

M. Gérard Longuet, rapporteur. – L'univers numérique a-t-il réfléchi à la possibilité que les utilisateurs paient pour un moteur de recherche ? La gratuité est attractive pour le consommateur, mais comprend effectivement des contreparties. Les citoyens, eux, ont peut-être envie de payer pour accéder à un service avec une économie différente et un classement peut-être plus neutre, ou en tous cas moins tributaire des logiques à l'œuvre chez les autres moteurs de recherches . Un tel modèle vaut pour certaines encyclopédies en ligne. Ce modèle a-t-il du sens ?

M. Marc Mossé. – Votre question ouvre de nombreux champs. Le numérique reflète nos sociétés. Il existe des modèles « freemium » avec un accès d'abord gratuit puis un paiement pour un service d'une autre nature, ou offrant des fonctionnalités complémentaires ou un contenu plus riche. Ce modèle s'impose d'ailleurs progressivement dans la presse avec une approche différenciée.

Au cours des dernières années, la montée en puissance de la dimension citoyenne me paraît aussi très forte : pendant longtemps, les avantages immédiats de la gratuité ont été observés. Pour différentes raisons, liées notamment à la protection des données personnelles ou au pluralisme, les aspirations citoyennes ont ensuite pris de l'importance.

La cybersécurité n'est plus un sujet de spécialistes, d'entreprises ou d'États. Avec la place de la presse ou la lutte contre les fake news, ces questions ont pris une autre dimension. Dans le cadre du Forum de Paris de la paix – qui réfléchit à de nouveaux modes de gouvernance – ceci a abouti à la signature par 66 États, 347 entreprises et 130 ONG et think tank d'un accord pour travailler ensemble sur ces sujets, avec une approche multipartite. La souveraineté des États demeure, mais la manière de mettre en œuvre les attributs de la souveraineté évolue, ainsi que la manière de garantir les droits dans un monde numérique. Le multilatéralisme – en crise à certains égards, peut être complété et renforcé par cette approche.

D'une certaine manière, la souveraineté numérique, c'est la « souveraineté augmentée » grâce au numérique, puisque son cœur – la garantie des droits – peut être renforcé par le numérique et la participation des citoyens.

M. Gérard Longuet, rapporteur. – La citoyenneté repose quand même sur l'impôt qui donne le droit de participer à la collectivité et de la faire fonctionner…

Pourquoi Microsoft n'a-t-il pas, il me semble, réussi dans le système d'exploitation des smartphones alors que ce type de terminal est de plus en plus décisif aujourd'hui ?

Notre commission a découvert que vous étiez un très gros investisseur dans les câbles sous-marins : quel est votre objectif en la matière ?

M. Marc Mossé. – Sur la question relative au système d'exploitation des mobiles, d'autres acteurs ont pris des parts de marché, et la compétition est très vive. Le choix que nous avons effectué, avec des applications fonctionnant sur tous les systèmes d'exploitation, est un mode très interopérable et compatible avec les développements open source. Nous sommes un des principaux contributeurs de Linux et avons acquis GitHub, principale plateforme de développement pour les développeurs open source. La plateforme Azure fonctionne avec de nombreux langages open source.. Face à cette innovation permanente, nous avons su trouver d'autres modèles et une place différente dans un univers conçu autour du cloud et de l'accès à différentes applications, sur les différentes plateformes. L'un des enjeux consiste à donner accès à la puissance de calcul qui permet le développement des applications propres aux entreprises. Le cloud n'est pas seulement du stockage, mais c'est aussi du « Software as a Service » et une « plateforme as a Service », permettant de développer des applications à moindre coûts.

Concernant les câbles sous-marins, la question des infrastructures est aujourd'hui évidemment essentielle. Nous disposons de datacenters partout dans le monde – avec notamment trois datacenters en France – et la question de la circulation et de l'accès à ces données est devenue essentielle.

M. Gérard Longuet, rapporteur. – Vous n'en aviez pas ressenti le besoin jusque-là ?

M. Marc Mossé. – Il s'agit de répondre à notre plan de charge avec la perspective d'offrir le meilleur service. Nous fonctionnons beaucoup avec des partenariats en fonction des caractéristiques des câbles nécessaires. Pour plus de précisions techniques, je vous transmettrai la réponse par écrit.

M. Gérard Longuet, rapporteur. – Les opérateurs télécom ont le sentiment, peut-être caricatural, de construire des autoroutes sur lesquelles vous circulez plus ou moins gratuitement…. Or, vous vous mettez

maintenant à construire vous-mêmes ! C'est honorable mais aurez-vous les mêmes contraintes ?

M. Marc Mossé. – Dans le même cadre juridique, les mêmes règles s'appliquent.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible en ligne sur le site du Sénat.

Audition de MM. Laurent Degré, directeur général, Guillaume de Saint Marc, directeur de l'innovation, Jean-Charles Griviaud, responsable cybersécurité et Bruno Bernard, directeur des affaires publiques, de Cisco France,
le 18 juillet 2019

M. Franck Montaugé, président. - Notre commission d'enquête poursuit ses travaux avec l'audition de représentants de l'entreprise Cisco France : Laurent Degré, directeur général, Guillaume de Saint Marc, directeur de l'innovation, Jean-Charles Griviaud, responsable cyber-sécurité, Bruno Bernard, directeur des affaires publiques, et Pascale Serot, responsable sécurité et défense. Cette audition est diffusée en direct sur le site Internet du Sénat. Elle fera également l'objet d'un compte rendu publié.

Un faux témoignage devant notre commission d'enquête serait passible des peines prévues aux articles 434-13, 434-14 et 434-15 du code pénal. Je vous invite chacun à prêter serment, chacun à votre tour, de dire toute la vérité, rien que la vérité, levez la main droite et dites : « Je le jure ».

Conformément à la procédure applicable aux commissions d'enquête, MM. Laurent Degré, Guillaume de Saint Marc, Jean-Charles Griviaud et Bruno Bernard, et Mme Pascale Serot prêtent serment.

Cisco, même si elle n'est pas désignée dans l'acronyme Gafam, fait partie des grandes entreprises américaines du numérique, en tant que fournisseur d'équipements réseaux pour internet. Nous souhaitons vous interroger sur des sujets sensibles, sur lesquels, peut-être, vous pourrez nous rassurer.

Comme l'avait noté notre collègue Catherine Morin-Desailly dans son rapport intitulé L'Europe au secours de l'Internet, l'affaire Snowden a révélé que la National Security Agency (NSA) aurait pu utiliser des équipements Cisco pour espionner les alliés des États-Unis. Pouvez-vous nous assurer que vos équipements, très présents dans les coeurs de réseaux de nos opérateurs télécoms, sont désormais exempts de tout risque ?

La portée extraterritoriale de lois comme le Patriot Act ou, plus récemment, le Cloud Act représente un sujet d'inquiétude. Êtes-vous en mesure de garantir que les données sensibles qui passent par des serveurs de Cisco en Europe ne peuvent pas être saisies par les autorités américaines ? Cisco France a-t-il déjà donné suite à de telles demandes en dehors des procédures de coopération judiciaire ? Comment conciliez-vous les obligations contradictoires découlant des normes américaines et de la législation européenne du Règlement général sur la protection des données (RGPD) ? Pouvez-vous nous rassurer sur le fait que le gouvernement américain ne peut vous contraindre à faire primer l'intérêt des États-Unis sur celui de la France ou de l'Europe ?

M. Laurent Degré, directeur général de Cisco France. - C'est pour nous un honneur d'être invités en tant que citoyens et représentants d'une entreprise américaine qui contribue à la transformation numérique des entreprises françaises. Nous sommes venus avec des représentants de la cyber-sécurité, de l'innovation et des relations avec le Gouvernement, pour apporter un maximum d'expertise à nos réponses, dans un souci de transparence. Le débat sur la souveraineté numérique apparaît, en effet, aussi important que complexe ; il interroge les notions de territoire et d'application des lois dans un monde numérique fondé sur l'échange de données, en quelques millisecondes, par-delà les frontières. Le numérique représente une source d'innovation, qu'il convient de préserver lorsqu'il s'agit de réfléchir en termes de régulation, de cloisonnement et de sécurité.

Cisco est une société américaine fondée en 1984, dont l'activité initiale consistait à relier les applications connectées des campus universitaires au démarrage de l'Internet. Ont ainsi été créées les fameuses autoroutes de l'information. L'entreprise compte environ 70 000 salariés, dont 26 000 ingénieurs, dans 164 pays et possède 19 000 brevets. Cisco France emploie 650 collaborateurs et travaille avec 1 200 partenaires, auxquels l'entreprise fournit des solutions numériques. Nous disposons également d'un laboratoire de recherche et développement, placé sous la direction de Guillaume de Saint Marc, et d'un trust office chargé de la transparence, du respect des standards et des relations avec l'Agence nationale de la sécurité des systèmes d'information (Anssi) s'agissant de la mise en conformité et de l'autorisation des produits que nous déployons. Nos clients sont des entreprises de toutes tailles, des administrations et des opérateurs télécom - c'est d'ailleurs grâce à ces derniers clients que nous avons développé nos relations avec l'Anssi. La France possède des champions du numérique, des super-calculateurs et de la cyber-sécurité, des acteurs de confiance qui sont nos partenaires. Nous pouvons en être fiers ! De même, l'Anssi représente un modèle pour l'Europe et pour le monde, grâce à la qualité des ingénieurs et de la certification que beaucoup de pays nous envient. La collaboration avec l'Anssi a contribué à faire progresser nos équipes. Enfin, Cisco investit massivement en France pour développer le réseau des start-up, où les talents sont multiples.

Le RGPD représente un élément important de la souveraineté numérique européenne, comme la directive « E-evidence », qui améliorera la transparence. Nous avons mis en place depuis quelques mois une procédure de réponse aux demandes de l'administration américaine qui pourraient intervenir dans le cadre du Cloud Act. À ce jour, cela ne s'est jamais produit. Dans un tel cas, nous regarderons d'abord où se trouvent les données incriminées. Cisco ne fait pas commerce de la donnée, mais la transporte et la sécurise, tandis que nos partenaires installent des solutions applicatives dans le cloud. Dans la majorité des cas, les données se trouvent donc chez le client : nous n'y avons alors pas accès et l'administration américaine devra nouer relation avec ledit client. Lorsque Cisco hébergera les données concernées, la

demande sera traitée au cas par cas après une analyse du type de données et de la pertinence et de la légitimité de la requête. Nos juristes et nos avocats entreront alors dans un dialogue avec l'administration américaine et, le cas échéant, une notification sera envoyée au client.

M. Franck Montaugé, président. - La notification ne sera pas envoyée d'emblée au client ?

M. Laurent Degré. - Si, dès lors que nous n'avons pas d'interdiction de communiquer l'information au client.

M. Gérard Longuet, rapporteur. - Vous êtes à la fois équipementier et hébergeur ?

M. Jean-Charles Griviaud, responsable cyber-sécurité de Cisco France. - Nous fournissons différents types de solutions principalement comme équipementier, ainsi que certains services pouvant se trouver dans le cloud pour lesquels les données nous seront accessibles. Cela dépend de la demande du client.

M. Laurent Degré. - Vous avez évoqué l'affaire Snowden. Sachez d'abord que nous ne développons que des produits standards, nous ne développons jamais une plateforme ou un logiciel spécifique pour un client donné.

M. Jean-Charles Griviaud. - Cisco opère dans 160 pays et développe effectivement les mêmes produits quels que soient la localisation géographique et le client destinataire du service

La confiance est devenue un enjeu majeur pour nos clients, sensibilisés par la médiatisation des faits divers et le travail remarquable réalisé par l'Anssi, avec des conséquences sur le niveau d'exigence attendu des fournisseurs. Nous souhaitons donc être identifié, par nos clients, comme un acteur de confiance. À cet effet, notre stratégie s'appuie sur des doctrines de sécurité qui visent à rendre visibles nos procédures industrielles, de la conception à la réalisation des produits, et à disposer de technologies de protection de ces mêmes produits, notamment des éléments physiques d'identité numérique permettant de vérifier l'authenticité d'un équipement matériel comme d'un logiciel. Nos produits sont construits sur des standards ; Cisco est d'ailleurs un important contributeur de l'open source. En cas de vulnérabilité constatée, nous assurons un traitement transparent selon une procédure centralisée auprès d'une équipe unique. Elle qualifie les mesures de correction nécessaires et communique l'information à l'industrie. Les entreprises et les agences ont, par ailleurs, accès à nos bases de vulnérabilité mises régulièrement à jour.

M. Gérard Longuet, rapporteur. - Qu'est-ce qu'une vulnérabilité ?

M. Jean-Charles Griviaud. - Quand une défaillance peut entraîner un acte de malveillance, il s'agit d'une vulnérabilité.

M. Gérard Longuet, rapporteur. - Ces vulnérabilités sont découvertes au fil du temps ?

M. Jean-Charles Griviaud - Les vulnérabilités nous sont communiquées par différents canaux - par des tests de régression en interne, par des tests réalisés par nos partenaires sur nos équipements ou par nos clients - et sont ensuite traitées et notifiées de façon centralisée par le computer emergency response team (CERT). Notre trust office peut donner, si nécessaire, des explications plus précises, notamment à l'Anssi.

Le troisième pilier de notre stratégie de transparence concerne la vérification par des audits extérieurs et par des programmes internes d'analyse en profondeur des équipements. Cela permet à une agence ou à un client de contrôler si un équipement est architecturé correctement ou si un service correspond à ses attentes. Nous soumettons aussi nos produits aux autorités de certification, soit l'Anssi en France - nous travaillons également avec l'Agence dans le cadre du régime d'autorisation prévu par l'article R. 226-3 du code pénal. Les certifications internationales permettent d'éviter de dupliquer les efforts et de simplifier la gestion. Certains produits, comme nos routeurs ou nos switchs, ne sont pas soumis aux certifications, mais sont utilisés par des opérateurs d'importance vitale dans leurs infrastructures ; nous sommes donc disponibles pour renseigner les clients, ainsi que l'Anssi, sur les modalités de leur fabrication.

M. Franck Montaugé, président. - Vous faites allusion à la norme internationale ISO 27000 ?

M. Jean-Charles Griviaud. - Notamment, car il existe différents types de certification : par entreprise, comme la norme ISO, ou par produits. Notre mission consiste à répondre aux besoins de certification de nos clients.

M. Stéphane Piednoir. - Pourriez-vous nous fournir un éclairage complémentaire sur les structures qui centralisent les vulnérabilités ? Quel est leur niveau de protection ?

En 2015, Cisco a passé un accord avec le gouvernement français, portant notamment sur un investissement de 200 millions de dollars dans des start-up françaises. Quel montant a été réellement investi par votre entreprise ? Avez-vous pris des participations minoritaires ou majoritaires dans ces sociétés ? En janvier, votre groupe a promis un nouvel investissement à hauteur de 61 millions d'euros. Qu'en est-il ?

M. Jean-Charles Griviaud. - Notre point de contact direct, lorsqu'un défaut apparaît, est le centre opérationnel de l'Anssi qui gère les relations avec le CERT. Celui-ci représente, au niveau d'un pays, un guichet unique pour le recensement des vulnérabilités et l'émission de recommandations. C'est un organisme de confiance. Il existe également un CERT européen. Nous souhaitons communiquer sur les vulnérabilités car, en matière de sécurité, le partage des informations fonctionne mieux que l'obscurité.

M. Laurent Degré. - La communication sur ces vulnérabilités s'organise sans aucun favoritisme pour une entreprise ou une administration donnée.

S'agissant des investissements, nous avons lancé un programme pluriannuel pour soutenir les nombreux talents français et stimuler l'innovation dans le secteur numérique. Nous avons ainsi investi au travers de fonds - comme Partech ou Idinvest - qui ont sélectionné les start-up en fonction de critères. Via la Cisco Networking Academy, nous avons également formé, depuis 2015, plus de 180 000 personnes aux métiers du numérique - sans se limiter uniquement aux produits Cisco - dans le cadre des programmes universitaires, des écoles d'ingénieurs, des centres de formation des apprentis (CFA) et des collèges. Il est très important de sensibiliser nos jeunes aux notions de cyber-sécurité et de souveraineté, et aux avantages et inconvénients du numérique. Par ailleurs, nous avons directement investi dans quelques start-up, comme Actility qui intervient dans le secteur des objets connectés. Enfin, nous avons créé une chaire avec l'école Polytechnique dans les domaines de la formation et du développement.

M. Guillaume de Saint Marc, directeur de l'innovation de Cisco France. - Le Lab Cisco a été inauguré en octobre 2015 par Emmanuel Macron, alors ministre de l'économie. Depuis, les investissements ont été maintenus et intensifiés. Avec la Cisco Networking Academy, nous visons un effet quantitatif de formation des personnes à des technologies standards. Le Lab vise davantage un effet qualitatif ; depuis le début de l'année 2019, trois jeunes doctorant en sont sortis, dotés du diplôme de Polytechnique et de l'école d'application Télécom ParisTech. Ces ingénieurs font partie de l'élite mondiale en matière de réseau et nous sommes heureux que l'un d'entre eux ait intégré notre société.

En ce qui concerne les investissements dans les start-up, nous avions reçu, en 2015, le message clair que leur développement constituait un enjeu national. Nous avons investi via des fonds - ceux déjà cités mais aussi le Paris-Saclay Seed Fund, directement, comme dans la société Actility précitée. Nous avons également l'intention d'acquérir la société Sentryo. Pour autant, notre objectif est davantage de collaborer de manière complémentaire avec les start-up que de les racheter : nous pouvons leur proposer l'accès à des opportunités commerciales, tandis qu'elles nous permettent d'augmenter notre portefeuille de produits avec des solutions pointues.

M. Franck Montaugé, président. - Je crois savoir que vous essayez d'innover en appuyant votre développement de la 5G sur le réseau 4G existant avec, notamment, des objectifs de déploiement en zone rurale. Pourriez-vous nous en dire davantage ?

M. Guillaume de Saint Marc. - Le projet auquel vous faites référence a été développé sur le territoire anglais. Il s'agit d'un pilote visant à modéliser le déploiement de la 5G. De fait, la 5G représente probablement la

première technologie mobile cellulaire qui ne sera pas principalement financée et justifiée économiquement par le grand public, mais par la numérisation des entreprises. L'enjeu consiste donc à mettre la 5G à leur service. C'est le sens de l'appel à projets lancé par le gouvernement britannique, que nous avons gagné avec un consortium. En travaillant sur les seuls secteurs du tourisme, de l'agriculture, de l'énergie et des transports, il s'agissait de trouver un modèle économique pour le déploiement de la 5G dans les territoires ruraux. Des expérimentations techniques ont eu lieu et nous attendons les modélisations économiques confiées à des universités. Le projet semble effectivement prometteur, raison pour laquelle nous l'avons présenté au salon Vivatech.

M. Laurent Degré. - S'il était besoin d'évaluer davantage ce type de plateforme, nous le ferions volontiers.

M. Gérard Longuet, rapporteur. - Quel est le pourcentage de votre chiffre d'affaires réalisé dans les différentes régions du monde ? Quels sont, pour vous, les pays leaders ?

M. Laurent Degré. - Schématiquement, 60 % de notre chiffre d'affaires provient de l'Amérique du Nord, où est installée la majorité des équipes d'ingénieurs et de développement ; vient ensuite la zone constituée par l'Europe, le Proche et le Moyen-Orient et la Russie, puis la zone Asie et Pacifique. En Europe, les pays moteurs pour le chiffre d'affaires sont l'Allemagne et la Grande-Bretagne, suivies de la France. Notre pays se situe toutefois en tête en matière d'innovation et de recherche : le Lab français représente près d'un quart des ressources en la matière.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible en ligne sur le site du Sénat.

Audition de M. Weiliang Shi, directeur général de Huawei France,
le 18 juillet 2019

M. Franck Montaugé, président. - Notre commission d'enquête poursuit ses travaux avec l'audition de représentants de l'entreprise Huawei France : MM. Weiliang Shi, directeur général, Benjamin Hecker, directeur juridique et de la protection des données, et Gwenaël Rouillec, directeur de la cybersécurité.

Cette audition est diffusée en direct sur le site Internet du Sénat. Elle fera également l'objet d'un compte rendu publié.

Enfin, je rappelle, pour la forme, qu'un faux témoignage devant notre commission d'enquête serait passible des peines prévues aux articles 434-13, 434-14 et 434-15 du code pénal. Je vous invite donc, à tour de rôle, à prêter serment de dire toute la vérité, rien que la vérité, levez la main droite et dites : « Je le jure.». Conformément à la procédure applicable aux commissions, M. Weiliang Shi prête serment.

M. Franck Montaugé, président. - Monsieur Shi, vous êtes directeur général de la filiale française de Huawei, l'un des géants chinois du numérique avec Baidu, Alibaba, Tencent et Xiaomi. Présente dans les équipements réseaux, mais aussi dans les smartphones ou dans le Cloud, l'entreprise connaît une croissance impressionnante et emploie aujourd'hui nombre de nos concitoyens. Elle est actuellement au coeur de la guerre technologique que se font les États-Unis et la Chine. Notre commission ne pouvait donc faire l'impasse sur votre audition.

Nous devons vous interroger sur des sujets, sur lesquels, peut-être, vous pourrez nous rassurer, alors que nous devrions adopter ce mois-ci définitivement la proposition de loi sur la sécurité des réseaux « 5G » - ce texte, je le rappelle, ne vise aucune entreprise en particulier mais fixe plutôt un cadre général pour garantir la confiance dans la technologie.

La question des liens de votre entreprise avec le Gouvernement chinois ne cesse de défrayer la chronique. Deux points ont particulièrement émergé dans le débat public : qui détient l'entreprise et quel est l'impact de la loi chinoise de 2017 sur le renseignement.

Sur le premier point - qui détient l'entreprise -, dans un article publié en avril dernier, deux chercheurs américains ont montré que la holding de votre entreprise est détenue à 1% par son fondateur Ren Zhengfei et à 99 % par une entité appelée « comité syndical », dont on sait peu de choses. Ces chercheurs en tirent la conclusion selon laquelle, au vu du rôle que jouent les syndicats en Chine, Huawei pourrait être considérée comme contrôlée par l'État - ils parlent au conditionnel. Ils affirment, en revanche, qu'il est clair que Huawei n'est pas détenue par ses salariés, lesquels détiennent seulement ce qui est assimilable à un régime d'intéressement et de participation aux

bénéfices. Pouvez-vous nous éclairer sur ce point important : qui détient le pouvoir de décision in fine dans l'entreprise Huawei ?

Le second point porte sur la loi chinoise sur le renseignement de 2017, qui génère les mêmes inquiétudes que le Cloud Act aux États-Unis. Son article 14 dispose notamment que les services de renseignement chinois peuvent requérir la coopération de tout citoyen chinois et de toute organisation. Êtes-vous en mesure de garantir que les données qui passent par vos équipements et vos serveurs ne seront pas utilisées par le Gouvernement chinois ? Si vous - en tant que personne physique ou en tant que personne morale - recevez une requête d'assistance du Gouvernement chinois, comment pouvez-vous la refuser ? Ces obligations sont-elles compatibles avec les normes européennes telles que le règlement général sur la protection des données (RGPD) ?

M. Weiliang Shi, directeur général de Huawei France. - Nous vous remercions vivement de nous recevoir dans le cadre des travaux de la commission d'enquête sur la souveraineté numérique. C'est avec plaisir que nous avons accueilli votre invitation à participer à cette audition qui sera, je l'espère, l'occasion de faire tomber quelques barrières.

Je débuterai mon propos par une rapide présentation des activités de notre groupe. Comme vous le savez, Huawei est le leader mondial des équipements télécoms et le deuxième fabricant de smartphones. Basé à Shenzhen, le groupe, créé en 1987, compte aujourd'hui près de 190 000 employés dans plus de 170 pays. Huawei est une entreprise 100 % privée, détenue par plus de 96 000 de ses employés et son fondateur, qui ne dispose que de 1,14 % des parts de l'entreprise, selon un modèle coopératif.

S'agissant de la filiale française, Huawei Technologies France est une société par actions simplifiée unipersonnelle inscrite au registre de commerce de Nanterre. En France depuis 2003, Huawei emploie près de 1000 personnes réparties entre différents sites implantés à Boulogne Billancourt, Paris, Nice, Lyon et Grenoble. Les activités sont principalement commerciales, mais nous disposons aussi de centres de recherche et développement spécialisés en design, en traitement de l'image, en mathématiques, en standardisation et en capteurs.

L'ADN de Huawei est la recherche et l'innovation. La première valeur de l'entreprise est le client. Spécialisée dans les nouvelles technologies, notre activité ne peut exister ni se pérenniser sans cybersécurité. C'est pourquoi nous appliquons à tous nos produits et procédures les standards internationaux les plus élevés en matière de sécurité, et imposons à tous nos collaborateurs à travers le monde le respect de règles de sécurité et de conformité extrêmement strictes, dont le RGPD est l'un de nos standards au niveau mondial.

Huawei investit 15 % de son chiffre d'affaires annuel dans la recherche et le développement : en 2018, cela représentait près de 13 milliards d'euros.

La stratégie commerciale de Huawei n'est pas fondée sur des acquisitions d'entreprises. Au contraire, elle est basée sur le développement d'écosystèmes à travers le monde, le transfert de notre savoir-faire et la volonté de nous implanter durablement.

Si nous sommes plus compétitifs, c'est parce que nous permettons à nos clients de faire des économies d'échelle en utilisant des produits très innovants adaptés à leurs besoins. Huawei est un acteur de la souveraineté numérique des pays dans lesquels nos matériels sont installés. Nous développons, en effet, des produits adaptés aux demandes des clients, appliquant les standards de sécurité les plus élevés, respectant les normes de chaque pays dans lesquels ils sont installés. Nous incitons aussi nos clients, publics comme privés, à assurer un niveau de sécurité élevé des matériels et réseaux qu'ils opèrent. J'attire, par ailleurs, votre attention sur le fait que Huawei est l'entreprise dont les matériels ont été le plus testés à travers le monde, tant en matière de certification, que par des tests menés par nos clients.

Contrairement à ce qui a pu être dit ou sous-entendu, Huawei a toujours joué la carte de la transparence et compte bien tenir cette ligne de conduite. Il nous appartient de rassurer les pouvoirs publics sur la qualité et la sécurité de nos matériels, comme de nos services. C'est pourquoi nous avons ouverts plusieurs centres de test, le dernier à Bruxelles, afin de permettre aux agences étatiques et à nos clients de pouvoir vérifier et tester nos codes sources.

En outre, Huawei contribue de manière inclusive et transparente avec tous les acteurs du secteur à l'amélioration des standards internationaux. Huawei collabore en effet activement aux travaux du 3GPP (3rd Generation Partnership Project), et échange régulièrement avec les services de l'Agence nationale des fréquences, de l'Autorité de régulation des communications électroniques et des postes ou encore de l'Agence nationale de la sécurité des systèmes d'information (Anssi) et de la direction générale des entreprises.

Notre volonté est de favoriser l'éclosion d'un écosystème de start-ups françaises qui seront, selon nous, les acteurs de la souveraineté numérique de la France de demain. Contrairement à nombres d'acteurs des nouvelles technologies, notre activité n'est pas fondée sur la cession des données à des fins commerciales. Au contraire, Huawei propose des briques technologiques innovantes qui permettent aux acteurs du numérique de pouvoir les intégrer dans les solutions qu'ils développent eux-mêmes.

Vous l'aurez compris, Huawei est un acteur majeur des nouvelles technologies tant au niveau mondial qu'en France. C'est la raison pour

laquelle nous signerons dans les tous prochains jours l'Appel de Paris pour la confiance et la sécurité dans le cyberespace.

Accompagné de Gwénaël Rouillec, directeur de la cybersécurité, et Benjamin Hecker, directeur juridique et protection des données de Huawei France, je serais heureux de répondre à vos questions. Je vous remercie de votre attention.

M. Benjamin Hecker.- Nous vous remercions de votre question sur la loi de 2017 pour l'analyse de laquelle nous avons missionné plusieurs cabinets d'avocats. Cette loi est liée aux impératifs de sécurité nationale définis par le Gouvernement chinois ; elle a donc vocation à s'appliquer strictement en Chine. À l'inverse du Cloud Act qui présente des effets extraterritoriaux, cette loi s'applique indistinctement à tout individu ou à toute organisation uniquement implantée en Chine, quelle que soit sa nationalité. Il lui est ainsi demandé de collaborer à des enquêtes dont l'objet porte sur des impératifs de sécurité nationale. La demande d'informations sur nos clients français par le Gouvernement, que vous évoquez dans votre question, n'existe donc pas. Elle n'est nullement prévue dans le texte de la loi de 2017, comme nous le confirment d'ailleurs les analyses de ces cabinets d'avocats. Nous nous félicitons également de la récente confirmation, par le premier ministre chinois lui-même, de l'absence d'effet extraterritorial des dispositions de la loi de 2017. Celui-ci a en outre précisé que les individus situés en dehors de la Chine ne devaient pas collaborer à des enquêtes se déroulant en Chine.

M. Weiliang Shi. - Nous n'avons jamais reçu, ni du groupe lui-même ou du gouvernement chinois, de demande de transfert de données. D'ailleurs, nous ne pourrions l'accepter, puisque nous n'appliquons que la loi française.

M. Gérard Longuet, rapporteur. - Je souhaiterais mieux comprendre l'entreprise Huawei qui est un remarquable succès mondial. Quelles sont les parts respectives du chiffre d'affaires de votre groupe réalisées en Chine et à l'international ?

M. Weiliang Shi.- En 2018, le chiffre d'affaires global a atteint 108 milliards de dollars, dont la moitié est issue de nos activités extérieures à la Chine.

M. Gérard Longuet, rapporteur.- Quelle part représente l'Europe dans ce chiffre d'affaires ?

M. Weiliang Shi.- Dans l'organisation de notre groupe, l'Europe est scindée en deux directions régionales distinctes : la première couvre l'Europe de l'Ouest, tandis que la seconde couvre le reste des pays européens, hors Russie ; celle-ci étant considérée comme une région à part entière, à l'instar de la région Pacifique et de la région Afrique.

M. Gérard Longuet, rapporteur.- Vous considérez-vous comme une entreprise d'équipements ou de services qui vend aussi des équipements ? Quelle est la part de services, soit de conception, soit d'hébergement, dans votre chiffre d'affaires ?

M. Weiliang Shi. - Notre modèle économique vise à vendre nos infrastructures matérielles, avec un transfert de savoir-faire. Nos services - d'installation, de formation - s'articulent autour de cette activité.

M. Gérard Longuet, rapporteur. - La première question relative à l'actualité est le fait que vous vendez des téléphones en dehors de la Chine dotés du système d'exploitation Android. Pensez-vous qu'il soit possible d'obtenir, en Europe, voire au-dehors de la Chine, des systèmes d'exploitation qui se libéreraient d'Android ?

M. Weiliang Shi. - Il n'existe, pour l'heure, que deux systèmes d'exploitation : l'iOS et Android. Pour Huawei, s'il n'est pas difficile de créer un troisième système, il est en revanche plus malaisé d'obtenir l'écosystème des applications, qui est la brique clef. La création d'un nouveau système ne permettrait pas nécessairement de se connecter aux applications existantes sur les autres systèmes. Dès lors, un téléphone doté d'un nouveau système et privé des autres applications ne serait acheté par personne !

M. Gérard Longuet, rapporteur.- Pensez-vous possible de survivre au refus d'un équipement iOS ou Android en Europe ?

M. Weiliang Shi.- Tel n'est pas notre souhait. Notre stratégie est avant tout de nous intégrer à des écosystèmes existants. S'il nous était interdit d'utiliser les systèmes d'exploitation existants, alors il nous faudrait en créer un nouveau, tout en veillant à raccorder les applications issues des écosystèmes préexistants.

M. Patrick Chaize. - Nous avons auditionné Google qui affirme que l'accès à son système d'exploitation est libre, même si ses mises à jour, notamment de sécurité, ne le sont pas. Si jamais un durcissement de la situation venait à se produire, resteriez-vous dans cet écosystème ou seriez-vous en mesure d'en créer un autre ?

M. Weiliang Shi.- L'écosystème représente la clef des systèmes d'exploitation. J'affirme également que le système Android est en open source et Huawei est l'un de ses principaux contributeurs. Le problème réside dans l'utilisation des applications, suite à la décision américaine. Or, personne n'achètera un téléphone privé d'applications !

M. Gérard Longuet, rapporteur. - Dans un autre secteur tout à fait différent, nous observons que les grands opérateurs du numérique investissent dans les câbles sous-marins de communications électroniques. À l'inverse, votre entreprise a récemment décidé de céder une partie de son activité à Hengtong, un autre acteur chinois du secteur. Pourquoi avoir procédé à une telle cession ?

M. Weiliang Shi. - Notre stratégie s'est focalisée sur ses trois piliers fondateurs : les connectivités, en particulier les technologies mobiles - de la 2G à la 5G, en passant par la fibre optique et les réseaux télécoms -, le stockage des données et les terminaux. Nous nous sommes donc recentrés.

M. Gérard Longuet, rapporteur. - Vous n'estimez donc pas la propriété des réseaux comme décisifs ?

M. Weiliang Shi.- Tout dépend de la nature des réseaux. Alors que les réseaux télécoms fournissent notre coeur d'activité, le câble sous-marin ne figure plus dans notre stratégie.

M. Gérard Longuet, rapporteur. - Dans votre présentation, vous avez indiqué que Huawei appartenait pour partie à ses 96 000 salariés, soit près de la moitié de ses personnels. Comment fonctionne une telle démocratie économique au sein de votre entreprise ?

M. Franck Montaugé, président. - Qui possède, au final, votre entreprise ?

M. Weiliang Shi. - L'entreprise est détenue à la fois par ses employés et son fondateur, lequel n'en possède qu'1,14 %. Elle est donc à 100 % privée. Le gouvernement chinois ne dispose ainsi d'aucun pouvoir ni d'aucune action dans Huawei.

M. Gérard Longuet, rapporteur.- Le gouvernement chinois, ou les banques chinoises, sont-ils créanciers de l'entreprise ? S'il est vrai que la participation des salariés contribue fortement à la cohésion de la société, elle n'est pas en mesure de soutenir le développement, fortement capitalistique, de vos activités. Comment faîtes-vous pour vous développer en termes de capitaux ?

M. Benjamin Hecker. - Les 96 000 salariés sont regroupés dans une coopérative gérée par un comité élu de 115 représentants qui eux-mêmes s'organisent avec un bureau qui gère l'entité. Aujourd'hui, ce comité est l'organe le plus élevé de la société. Il assure la désignation des membres du conseil d'administration et du conseil de surveillance de Huawei.

M. Gérard Longuet, rapporteur.- Sur le financement de ce secteur aux technologies extrêmement évolutives, l'appel aux capitaux extérieurs est une nécessité. Vos salariés, quand bien même ils seraient nombreux et bien payés, ne peuvent soutenir de tels investissements.

M. Benjamin Hecker. - En effet, la société s'autofinance, en réinvestissant ses revenus dans son développement. Néanmoins, 70 à 80 % des banques qui nous soutiennent sont d'origine non chinoise, parmi lesquelles se trouvent des banques françaises.

M. Franck Montaugé, président.- Compte tenu de l'organisation politique souveraine qui est la vôtre, le Parti communiste chinois est présent

dans chaque entreprise et influence le choix de ses dirigeants qui peuvent par ailleurs être élus. Huawei fait-elle exception par rapport à cette règle ?

M. Weiliang Shi. - La loi chinoise oblige les entreprises à avoir un comité du Parti en son sein. Huawei ne fait pas exception. Celui-ci joue un rôle analogue à celui d'un comité d'entreprise en France et ne prend pas part à la décision stratégique.

M. Gérard Longuet, rapporteur.- Je reviens sur le rôle de l'État chinois. Le département d'État aux États-Unis est un acteur du secteur des hautes technologies, en agissant sous forme d'achats préférentiels ou de subventions. Comme j'ai pu le constater comme ministre de l'industrie ou de la défense, les entreprises françaises savent également se tourner vers l'État pour obtenir des soutiens et des financements. Ma question est importante : Huawei s'efforce-t-elle, comme les autres entreprises américaines ou françaises, de bénéficier des subventions, de ligne de crédits ou d'achats prioritaires de son propre gouvernement ? Ce ne serait pas choquant, puisque les autres pays le font.

M. Weiliang Shi. - Nos produits sont destinés uniquement à l'usage civil et sont ainsi développés selon des standards civils. Ils ne sont donc pas voués à équiper la défense chinoise. Nous participons ainsi à la définition des normes du 3GPP et du GSM Association (GSMA) uniquement pour le secteur civil.

M. Gérard Longuet, rapporteur. - Les pouvoirs publics chinois sont-ils vos clients ?

M. Weiliang Shi. - Ils peuvent l'être, en achetant les serveurs et les capacités de stockage pour leur utilisation, avec les standards civils. Nous ne concevons pas d'équipements spécifiquement destinés aux pouvoirs publics. En outre, nous ne bénéficions d'aucune subvention du gouvernement chinois ou de la banque chinoise.

M. Pierre Ouzoulias. - Sur un plan géostratégique, nous avons l'impression que deux grands blocs se constituent et ce, pour des motifs essentiellement capitalistiques : l'un autour des Gafam, soutenus par le gouvernement américain - qui n'hésite à brandir des menaces de représailles économiques à l'occasion notamment de l'annonce, par Paris, du projet de taxer ces Gafam - et un autre qui rassemble les autres acteurs du numérique. L'Europe semble ainsi être le champ de bataille de ces deux blocs, comme nous ne pouvons que le constater, en raison de la modicité de nos investissements dans la technologie numérique qui nous prive des premiers rôles dans ce secteur. D'ailleurs, nous le regrettons tous collectivement et c'est sans doute l'une des raisons de la constitution de cette commission ! Dans ce conflit qui touche l'Europe, estimez-vous que le RGPD, l'open source et l'interopérabilité, fournissent des moyens de défense contre les Gafam et l'opportunité de proposer aux consommateurs européens un modèle

numérique concurrentiel offrant une sécurité accrue par rapport à ce que proposent les Gafam ?

M. Weiliang Shi. - Personne n'aime la guerre économique et ou numérique pour investir. Nous investissons, notamment en France où, depuis 2003, nous avons créé trois bureaux de recherche, dans le coeur de nos activités, ainsi qu'un Open Lab qui permet de travailler avec nos clients et partenaires en faveur de l'innovation. Nous allons ainsi poursuivre nos investissements, comme l'a annoncé notre président Ken Hu, à hauteur de 35 millions de dollars dans cet Open Lab.

M. Benjamin Hecker. - Il est sans doute opportun de changer de modèle et d'assurer une plus grande protection des données. De ce fait, Huawei a décidé d'appliquer les règles du RGDP et d'en faire un standard au niveau mondial. Nous appliquons donc les programmes de conformité indistinctement dans nos différentes filiales. Nous pensons que le RGPD, à l'instar de la loi de 1978, est un formidable levier pour protéger les consommateurs et leurs données, dans leur transit à travers des réseaux ou des applications. La protection des données dépasse la simple obligation légale pour participer à la responsabilité sociale de l'entreprise, au même titre que les problématiques éthiques. Huawei est principalement un fournisseur d'équipements. Il importe donc que leur niveau de sécurité assure la protection des données de nos clients. En ce sens, nous avons mis en place des procédures très strictes de développement, autour notamment de la notion de « privacy by design » qui vous est familière. Cette dernière, qui est l'un des éléments du RGPD, permet, dès la réflexion à l'origine de la conception d'un équipement, de prendre en compte la problématique de la protection des données et de l'intégrer à ce stade. C'est pour nous une chance, en tant qu'entreprise chinoise implantée dans différents pays et notamment en Europe.

M. Gérard Longuet, rapporteur.- Je suis votre raisonnement. Quel type de certifications mettez-vous en oeuvre pour épauler cette démarche ?

Gwenaël Rouillec, directeur de la cybersécurité. - Tous nos produits, en grande partie, sont certifiés « critères communs. » Si nous appliquons déjà toutes les normes européennes, nous avons, avec l'Anssi, engagé des démarches en vue d'obtenir des certifications de sécurité de premier niveau (CSPN) pour les produits 5G qui vont arriver demain. Sur l'open source, qui est utilisée par Huawei dans la conception de ses produits, dans un souci de transparence et de conformité, la finalité demeure nos clients, au-delà des fournisseurs que nous choisissons.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible en ligne sur le site du Sénat.

Audition de M. Christophe Castaner, ministre de l'intérieur,
le 2 septembre 2019

M. Franck Montaugé, président. - Notre commission d'enquête poursuit ses travaux avec l'audition de M. Christophe Castaner, ministre de l'intérieur. Cette audition sera diffusée en direct sur le site Internet du Sénat et elle fera l'objet d'un compte rendu publié.

Je rappelle qu'un faux témoignage devant notre commission d'enquête serait passible des peines prévues aux articles 434-13, 434-14 et 434-15 du code pénal.

Conformément à la procédure applicable aux commissions d'enquête, M. Christophe Castaner prête serment.

Monsieur le ministre, vous êtes à la tête d'un important ministère régalien, l'Intérieur, qui doit répondre aux défis que représente la révolution des technologies numériques pour notre souveraineté et pour l'intégrité de notre ordre juridique face à des menaces nouvelles.

Votre ministère a publié en juillet dernier un bilan de *L'état de la menace liée au numérique en 2019* et cette feuille de route liste la souveraineté numérique parmi les défis stratégiques identifiés. Peut-être pourrez-vous, à titre liminaire, nous exposer l'état de ces menaces ainsi que les réponses que votre ministère contribue y apporte.

La souveraineté à l'ère du numérique pose également le problème de la liberté de conscience et de choix du citoyen, en matière électorale notamment. Le scandale de Cambridge Analytica a révélé la manière dont le vote de certains citoyens américains a été manipulé lors des dernières élections présidentielles. Il serait utile que vous nous présentiez les dispositions prises par votre ministère et le Gouvernement pour éviter de telles dérives, tout en garantissant le choix le plus libre possible du citoyen électeur.

Les modèles économiques des grands acteurs du numérique passent aujourd'hui par la mise en oeuvre de stratégies d'évitement, ce qui leur permet d'échapper aux contraintes traditionnelles de notre ordre juridique. Obtenir, par exemple, la coopération de grandes plateformes situées à l'étranger n'est pas toujours aisé : quelles difficultés vos services d'enquête rencontrent-ils, et quelles solutions nous sont offertes ? Pensez-vous qu'une évolution du statut des plateformes serait de nature à redonner force d'intervention à l'État au titre de l'intérêt général et de la protection de nos concitoyens ?

M. Christophe Castaner, ministre. - J'ai pris l'engagement de dire toute la vérité, eu égard à la connaissance que nous avons aujourd'hui en la matière. Or, sur ce sujet, la connaissance d'aujourd'hui n'est jamais celle de demain, ni celle d'après-demain. Ce sujet absolument majeur concerne

l'ensemble des ministères : il importe d'être extrêmement vigilant et armé. Vous avez rappelé la fonction régalienne du ministère de l'intérieur, mais presque tous les ministères doivent contribuer à traiter de la question de la souveraineté numérique, ainsi que les collectivités locales et les acteurs publics.

Il faut agir à deux niveaux : tout d'abord, il faut agir sur la conscience. L'intérêt de votre commission d'enquête est d'attirer l'attention sur l'importance de ce sujet en soulignant combien il convient d'être vigilant dans les comportements. Le rapport de 2019 sur la cybermenace pose au préalable la question essentielle de la prévention - il faut avoir conscience du risque. Il faut aussi agir sur la question de la transversalité, avec l'ensemble des autres ministères, dont celui de la défense notamment, et sur celle de la modestie, car la question de la souveraineté numérique relève non pas d'un ministère, mais de la France, qui vit dans un enclos numérique mondial. Compte tenu de tous les enjeux, la France est-elle suffisamment protégée ?

J'apporterai enfin des éléments de réponse à votre question très précise concernant l'attitude des grandes plateformes numériques.

La question de la souveraineté numérique est au coeur des préoccupations du ministère de l'intérieur. Nous aurons beau nous armer de multiples façons, si nous ne sommes pas en capacité de résister à des cyberattaques, c'est tout l'édifice qui tombera. Je l'ai vécu il y a quelques jours avec la préparation du sommet du G7. Nous savions que les cyberattaques étaient l'une des menaces majeures dont nous aurions pu faire les frais. Nous le savons, certains de nos adversaires n'hésitent pas à choisir des moments sensibles ou médiatiques pour attaquer un pays comme la France. Il est donc indispensable que l'ensemble du Gouvernement s'engage sur cette question. J'insiste sur le lien qui existe entre le ministère de l'intérieur et celui de la défense sur la question de la cyberdéfense, sans oublier le travail engagé par le secrétariat d'État au numérique.

Comme je l'ai dit dans mon propos liminaire, il s'agit à la fois d'une question pédagogique et d'une question de travail collectif - c'est ce que j'appelle l'« hygiène cyber ».

Aujourd'hui, il est indispensable que les particuliers, les entreprises, les administrations aient cette hygiène cyber. Nous sommes entrés dans l'ère du numérique par les usages, mais pas forcément par la protection. Les remparts existent, mais ils sont fragiles. C'est de notre capacité à adopter les bonnes pratiques et à ne pas ouvrir nous-mêmes de brèches que dépend notre cybersécurité. Un constat s'impose, le numérique est présent partout : il structure nos échanges, nos déplacements, nos services publics ; il intervient dans toutes les étapes de notre vie et de notre quotidien ; on en est aujourd'hui dépendant. De plus, l'actualité le montre régulièrement, des pans entiers de notre économie s'appuient sur le numérique. Tant le secteur privé que le secteur public sont touchés. Le numérique est un outil

formidable qui offre des opportunités extraordinaires, mais si l'on pèche par naïveté, on néglige les risques nouveaux qui y sont associés.

Quand on regarde le seul sujet de la délinquance classique, on voit bien comment les méthodes et le profil des auteurs ont évolué. Par le piratage des données, les mails d'hameçonnage ou d'usurpation d'identité, des champs entiers de criminalité se développent grâce au numérique. L'information est devenue une source d'enjeux et, en parallèle, une source de conflits. La manipulation de l'information peut battre son plein sur internet et peut alimenter des théories totalement délirantes, qui deviennent des vérités pour certains par le biais d'algorithmes. Ceux-ci vont vous envoyer des informations en lien avec ce que vous pensez et non pas ce que vous cherchez. On voit aujourd'hui comment on peut créer un univers qui va vous influencer et, de fait, comment certains vont manipuler l'information pour interférer dans la vie d'un pays, voire, comme vous l'avez relevé, dans le bon déroulement des élections. Notre économie et nos services publics sont, eux aussi, exposés. Il nous faut donc parvenir à construire des remparts.

Nous avons vécu des cyberattaques majeures sur des services publics : un système hospitalier a été attaqué, avec des conséquences extrêmement graves, mais des attaques contre des gares, des moyens logistiques, voire des moyens de production d'énergie peuvent bloquer un pays et donc menacer sa souveraineté.

C'est pourquoi le ministère de l'intérieur agit depuis plusieurs années pour lutter contre la cybercriminalité, les arnaques et les escroqueries en ligne. À cet égard, la plateforme de signalement Percev@l a été créée pour les victimes d'usages frauduleux de leur carte bancaire. L'idée est simple : d'un côté, pouvoir signaler rapidement et facilement afin de limiter le préjudice et, de l'autre, regrouper les éléments d'information et les moyens pour avoir une enquête unique pour des infractions similaires. L'équipement nécessaire pour procéder à une cyberattaque est très différent de celui dont on avait besoin pour braquer une banque.

Par ailleurs, nous avons mis l'accent sur la formation. Aujourd'hui, 80 % de nos policiers et de nos gendarmes sont sensibilisés aux enjeux cyber. Nous formons aussi des enquêteurs spécialisés dans le domaine du numérique. À cet égard, je citerai le réseau cyberGend de la gendarmerie nationale : nous comptons 4 500 enquêteurs cyber sur le territoire, avec l'objectif de parvenir à 6 500 d'ici à la fin du mandat du Président de la République.

Nous sommes particulièrement vigilants en ce qui concerne les attaques contre les entreprises. La Direction générale de la sécurité intérieure (DGSI) se tient à la disposition de toutes les entreprises qui pensent avoir été victimes d'une cyberattaque. Il est essentiel que la Direction générale de la sécurité extérieure (DGSE) centralise les principales attaques pour avoir connaissance des opérations d'ingérence étrangère.

Enfin, nous avons renforcé le dispositif de prévention, et ce dès le plus jeune âge. Pour ne prendre qu'un exemple, j'évoquerai le permis Internet grâce auquel 2 millions d'enfants ont été sensibilisés aux risques d'internet. Ce n'est pas anecdotique ; c'est souvent de cette manière que les bonnes pratiques dont je parle depuis le début de mon propos se développeront. Il faut qu'elles soient des automatismes.

En matière de cybercriminalité, je n'oublie pas que le numérique est un vecteur majeur de menaces terroristes. On voit bien comment les pires actes peuvent s'afficher librement sur les réseaux sociaux. En témoigne l'attentat de Christchurch : alors que la vidéo de treize minutes avait été retirée au bout de vingt-quatre minutes, si je me souviens bien, elle a été vue 1,5 million de fois en vingt-quatre heures - ceux qui la diffusaient s'étant adaptés pour contourner les mesures techniques mises en place par les plateformes.

Sur ce sujet, la France a pris ses responsabilités en créant la plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (Pharos), qui permet aux internautes de signaler les contenus terroristes ou haineux. Sur le plan européen, elle soutient l'adoption du règlement européen actuellement en cours de négociation afin de permettre le retrait d'un contenu terroriste en moins d'une heure après son signalement. Nous souhaitons que ce dossier puisse très vite revenir devant le nouveau Parlement européen.

Pour réussir en la matière, nous aurons besoin des géants du numérique, mais pas seulement. Lors du premier G7 des ministres de l'intérieur, j'ai invité les responsables des Gafam - Google, Apple, Facebook, Amazon et Microsoft - afin d'avancer sur ce sujet, qui a également été abordé par les chefs d'État et de gouvernement dans le cadre du G7. Ces grands opérateurs ont plutôt été réactifs et se montrent généralement très réceptifs à nos demandes, ce qui a conduit à un infléchissement de la position des États-Unis sur cette question. C'est ce que nous avions appelé « les engagements de Paris » après le G7 ministériel. Le Canada, qui n'était pas du tout offensif en la matière, nous a suivis dans la coopération. Mais nous nous heurtons à une difficulté : concilier la nécessité de lutter contre le terrorisme et la liberté de l'information qui doit circuler sur les réseaux - les Gafam et les entreprises y sont très attachés. Il nous faut donc continuer à faire pression sur ces entreprises.

Concernant la question des grandes plateformes que vous avez évoquée, Monsieur le Président, elles sont plutôt coopératives sur des sujets tels que celui de la lutte contre le terrorisme, contrairement à d'autres opérateurs moins importants mais qui permettent de diffuser des informations et font partie des angles morts, et sur lesquels je voudrais insister.

Les grands opérateurs ont, en effet, des représentants physiques en Europe : Laurent Solly, qui représente Facebook pour la France et l'Europe, est un ancien préfet et un interlocuteur que les administrations connaissent. Ainsi, en matière de lutte contre le terrorisme, Facebook peut se montrer proactif. En revanche - sans même parler du darknet - nous ne disposons pas toujours de correspondant pour d'autres plateformes de communication très utilisées, notamment par les jeunes - le site « jeuxvideo.com » par exemple, s'il ne fallait en citer qu'un exemple. On se focalise beaucoup sur les Gafam - et pour plusieurs raisons, y compris pour des raisons de citoyenneté fiscale, sur lesquelles il ne m'appartient pas de me prononcer - mais le risque se situe aussi au-delà de ces acteurs : les cybercriminels qui utilisent les réseaux savent très bien s'adapter au caractère coopératif ou non des intermédiaires techniques.

Aussi, au fil des années, la plateforme Pharos a enregistré une très forte baisse du nombre de sollicitations, et ce pour plusieurs raisons. Même si elle existe encore, la menace exogène est affaiblie. Daech, qui avait beaucoup utilisé les réseaux sociaux pour diffuser ses outils de haine, est affaiblie, et a aussi compris qu'il avait plus de libertés sur d'autres réseaux, comme le darknet, qui pose de véritables difficultés. Il nous faut donc mener le combat sur ces différents fronts. J'y insiste, se focaliser uniquement sur les Gafam reviendrait à passer à côté d'une partie de la menace.

Pour répondre ensuite à votre question concernant le risque de manipulation de l'information et la sincérité des scrutins, je veux rappeler qu'en France notre mode de scrutin nous protège : la proclamation des résultats ne se fait que sur le fondement des procès-verbaux papier, ce qui limite très sensiblement le risque d'attaque. Il existe certes d'autres types de fraudes, plus locales - je ne pense pas qu'elles soient nombreuses -, mais elles ne sont pas dirigées depuis l'étranger et ne relèvent pas de la question de la souveraineté numérique. Depuis 2007, 66 communes peuvent utiliser des machines à voter, ce qui représente 3 % du corps électoral, leur sécurité est très surveillée, et il n'est pas dans notre intention de revenir sur le moratoire qui avait été décidé sur cette question.

Par ailleurs, des manipulations de l'opinion peuvent être orchestrées par une nation étrangère *via* la propagation de fausses informations. Ce risque est réel, il touche tous les États occidentaux, cibles de systèmes organisés d'influences. Ainsi a-t-on vu comment 1 % des émetteurs, sur Twitter, pouvaient être à l'origine, sur tel ou tel sujet, de 50 % des tweets, ce qui ne saurait relever du hasard.

En la matière, le ministère de l'intérieur a adopté une posture de grande vigilance. De plus en plus d'outils pour vérifier la véracité d'une information sont à la disposition du public. Des bonnes pratiques existent contre la désinformation en ligne ; la Commission européenne les a recensées dans un guide avant les élections européennes. Le problème reste que chacun peut aujourd'hui se créer sa propre communauté ou banque de

données d'informations et s'y enfermer. Les médias traditionnels, y compris les chaînes d'information en continu, sont dépassés par ce phénomène.

J'en viens à énumérer un certain nombre de défis pour notre souveraineté numérique. Premier défi : celui de l'intelligence artificielle. En pleine expansion, elle suscite des débats, notamment sur son usage public, qui doit s'assortir de nécessaires contrôles. À l'heure où toutes les sociétés industrielles investissent massivement dans ce domaine, le ministère de l'intérieur ne saurait passer à côté et il s'est d'ailleurs doté d'un coordonnateur ministériel en matière d'intelligence artificielle.

Autre défi : celui de l'identité numérique, levier fort de garantie de notre souveraineté numérique. Sur ce sujet, nous ne sommes pas en avance, et des pays comme l'Estonie peuvent nous donner des leçons de modernité. Néanmoins, nous avançons : l'année dernière, un programme interministériel chargé de l'identité numérique et hébergé par le ministère de l'intérieur a été mis en place. Il conduit le chantier de la future carte d'identité numérique. Il nous faut garantir le meilleur niveau de sécurité possible.

Dernier défi majeur : celui de la sécurité de nos données. Le piratage de nos données sensibles peut représenter une faille de sécurité majeure pour notre pays et nous placer en situation dangereuse. Nous avons pris des mesures de protection maximales - ce qui ne signifie évidemment pas que le système soit infaillible : j'en appelle à la modestie. Nous assurons nous-mêmes la maîtrise de nos centres d'exploitation informatique, et nous sommes dotés d'un Cloud souverain, particulièrement protégé, pour héberger nos données sensibles. Nous venons de surcroît de créer une direction du numérique unique au sein du ministère - j'ai pris cette décision il y a quelques semaines, et la direction sera opérationnelle au 1er janvier prochain.

La souveraineté numérique est vraiment une question de premier plan. Peut-être ma culture, dans ce domaine, est-elle une culture de l'ancien monde. N'y voyez aucune provocation de la part d'un ministre ayant accompagné la création de La République En Marche : la plupart d'entre nous avons un rapport appris au numérique, et non un rapport d'évidence, comme l'est celui de certains des acteurs auxquels nous avons à faire face. Sur cette question sensible et très complexe, aucune affirmation ne saurait être réputée à l'épreuve du doute, l'imagination de nos ingénieurs et de certains de nos adversaires étant souvent sans limites pour exploiter toutes les failles. J'insisterai sur un mot : vigilance absolue. Et je l'assortirai d'un autre, qui qualifie le mieux l'action du ministère pour lutter contre ces risques : détermination absolue.

M. Gérard Longuet, rapporteur. - Je reprendrai d'ailleurs à mon compte la distinction que vous avez formulée pour conclure, qui me paraît importante pour les sociétés européennes : la différence entre l'appris et

l'évident, cette différence ne nous interdisant aucunement de mettre en garde les générations pour lesquelles le numérique est un univers évident, dont elles ne prennent peut-être pas toute la mesure.

Pourquoi les plateformes Percev@l - pour signaler une fraude à la carte bancaire à la police nationale ou à la gendarmerie et THESEE - pour porter plainte pour tout fait d'escroquerie en ligne -se sont-elles développées séparément ? Considère-t-on que la carte de crédit est d'usage universel quand les escroqueries sont par nature plus locales - elles peuvent passer par la carte de crédit, mais pas nécessairement ?

S'agissant de l'identification des personnes, l'identification officielle était historiquement un privilège de l'État ; ce privilège est aujourd'hui de plus en plus contesté par les géants du numérique, qui font valoir leur intérêt, en termes de fidélisation et de captation d'une clientèle, à organiser eux-mêmes l'identification. Quelle place l'État veut-il jouer en matière d'identification à l'intérieur de ce monde numérique - je ne parle pas du monde physique, celui des frontières matérielles ? Existe-t-il une convergence entre l'identification dans l'espace numérique et l'identification dans l'espace matériel ? En particulier, quelle peut être la place de la reconnaissance faciale ? Votre administration, qui a longtemps été la mienne en tant que membre du corps préfectoral, a lancé le projet Alicem - authentification en ligne certifiée sur mobile. Où en sommes-nous ? Comment réagissez-vous aux interrogations exprimées par le monde associatif ou la CNIL (Commission nationale de l'informatique et des libertés) sur le recours obligatoire à la reconnaissance faciale ?

Ma deuxième question a trait à l'intégrité des processus électoraux. En la matière, avez-vous des pistes concrètes ? Vous avez évoqué le vote électronique, qui reste aujourd'hui marginal en France. Dans certaines organisations administratives ou associatives ou à l'occasion d'un éventuel recours accru au référendum, on peut imaginer que le vote électronique pourrait se développer. Le ministère doit-il prendre, à cet égard, des initiatives ?

Troisième question - nous la poserons également à votre collègue Mme la Garde des sceaux : quid de l'utilisation des algorithmes dans vos champs de compétence ? Certains services, en particulier dans la gendarmerie, réfléchissent à développer des logiciels d'anticipation et d'analyse décisionnelle -pourquoi pas en matière de circulation automobile par exemple. Que pouvez-vous nous dire des projets en cours ?

Dernier sujet sur lequel je souhaite vous interroger : vous avez dit quelque chose de vrai, mais qui mérite, me semble-t-il, un approfondissement. Les Gafam, avez-vous dit, ont l'immense mérite d'avoir une taille critique leur permettant de mettre en place des structures et de travailler avec vous. Quel type de coopération pouvez-vous justement imaginer afin de promouvoir, de leur part, une attitude plus conforme à nos

intérêts nationaux ? Vous semblez penser que les Gafam sont plus enclins à adopter des comportements responsables que des acteurs dont l'objectif est simplement d'obtenir un profit immédiat sans endosser les responsabilités inhérentes à l'action d'une grande structure justifiant par-là d'adopter à l'égard de ces géants numériques une attitude ouverte...

M. Christophe Castaner, ministre. - Je commencerai par répondre à votre dernière question : nos interlocuteurs ne sauraient se résumer aux seuls Gafam - j'y ai insisté, car un réflexe courant, bien naturel, consiste à se focaliser sur ces derniers. Avec les Gafam, nous avons face à nous des gens dotés d'une incarnation physique, de moyens humains et algorithmiques, avec lesquels il est possible de discuter et de travailler. Lorsqu'une contrainte leur est imposée, ils ont la capacité technique d'y faire face - je ne leur prête cependant aucune propension à être naturellement bons, ni, d'ailleurs, naturellement mauvais.

J'ai en tête, *a contrario*, des exemples de réseaux sociaux où des menaces de mort sont diffusées contre un commissaire de police pendant les manifestations des « gilets jaunes » et où aucun interlocuteur ne nous répond lorsque nous cherchons à identifier les auteurs de ces menaces, l'anonymat étant une valeur absolue desdits réseaux, quand, au contraire, la sécurité exige de la transparence.

Il ne suffit pas, par ailleurs, de poser la question des acteurs : les nouveaux outils posent eux-mêmes un problème de perte de maîtrise - je pense par exemple à la localisation des données hébergées dans le cloud. Aux États-Unis, en vertu du *Cloud Act*, toute information relevant de la juridiction américaine doit être communiquée aux autorités américaines à la demande. Une législation similaire existe en Chine.

Certains outils, en outre, ont évolué : la 3G a été conçue sur un modèle européen ; tel n'est pas le cas de la 5G. Aujourd'hui, ce que nous savons faire sur la 3G - je parle d'actes autorisés par la loi, interventions techniques, écoutes téléphoniques, par exemple -, nous ne savons pas forcément le faire sur la 5G. Or les cybercriminels savent parfaitement exploiter ce genre de failles. Au-delà des entreprises, donc, de nouveaux supports et outils peuvent nous échapper, ce qui n'est pas sans poser problème du point de vue de la souveraineté nationale. La création de notre propre système de stockage des données me paraît un horizon nécessaire. Nous devons y travailler à l'échelle de l'Europe.

Sur Percev@l et THESEE, j'ai senti de la part de M. le rapporteur une petite pique contre le ministère de l'intérieur. Il peut arriver en effet que la police et la gendarmerie cheminent sans que leurs travaux ne se croisent... Une telle situation peut accoucher d'une saine émulation, mais la convergence est toujours préférable. J'ai donc décidé de fusionner les services de ces deux administrations en une seule direction du numérique. Certains avaient le sentiment de perdre ainsi un volet déterminant de leur

action - les discussions ont été parfois difficiles - mais cette fusion ne veut pas dire que la gendarmerie et la police ne pourront pas continuer d'expérimenter chacune de leur côté.

Percev@l est une plateforme de lutte contre les usages frauduleux de la carte bancaire ; THESEE relève d'une démarche analogue, dédiée à la lutte contre les escroqueries en ligne. Ces deux contentieux sont distincts et les projets ont fait l'objet, dès 2015, d'une coordination. L'existence de deux plateformes ne pose donc pas de problème.

S'agissant de l'identité numérique, nous savons tous que l'intelligence artificielle suscite une angoisse profonde, fondée ou non, qui conduit à freiner l'exploitation de certaines techniques. Nous avons tort ! Car elles accroissent l'efficacité de l'action publique pour protéger les Français ; il convient simplement d'entourer leur emploi de toutes les sécurités. Les caméras-piétons par exemple avaient initialement provoqué la polémique. Le ministre de l'époque s'est opposé à leur développement, elles étaient alors perçues comme une contrainte pour les forces de l'ordre. Puis elles sont apparues comme une protection... si bien qu'elles viennent d'être étendues aux sapeurs-pompiers. Naturellement, des contrôles de ce dispositif existent. L'interpellation est filmée : lorsque le policier ou le gendarme revient à son bureau, il n'a pas la possibilité de regarder les images ; celles-ci sont conservées, mais pour un temps déterminé. Leur accès est ainsi limité, afin de préserver les libertés fondamentales.

Il en va de même concernant l'usage de l'intelligence artificielle par les services. Considérez l'attentat qui s'est produit récemment à Lyon devant La Brioche dorée : il a eu lieu un vendredi à 16 h 30 ; 30 enquêteurs ont visionné les images enregistrées par l'ensemble du réseau des caméras de vidéoprotection, c'est ainsi que l'on a retrouvé et identifié l'auteur, le dimanche soir. Il a été interpellé le lendemain matin. Avec l'intelligence artificielle, on aurait su en quinze minutes où il était allé, grâce à la reconnaissance faciale. La technique peut bien entendu faire débat, si elle n'est pas entourée de toutes les protections qui s'imposent. C'est parce qu'il y a effectivement un risque de détournement, qu'il faut des garde-fous. Dans le dispositif d'authentification en ligne certifiée sur mobile (Alicem) que vous avez évoqué, et sur lequel nous travaillons, aucune donnée biométrique ne peut être partagée. La photo extraite de la puce reste stockée sur le téléphone portable de l'utilisateur. La vidéo de reconnaissance faciale créée au moment de l'identification est effacée après vérification. Les données ne font l'objet d'aucun traitement et ne sont bien sûr pas transmises à des tiers.

Grâce à de tels outils, l'État assurera mieux sa mission régalienne de certification des identités dans le monde digital, préfigurant un service numérique plus large. N'oublions pas une chose : ce que nous ne faisons pas, d'autres le feront. Voyez les monnaies parallèles ! Il est indispensable de proposer des systèmes d'identité sécurisés à tous les acteurs publics ou privés. L'enjeu est également de simplifier les démarches administratives.

L'échéance de 2022 approche ! La carte d'identité numérique estonienne comporte 15 à 20 services intégrés. Il faut aller le plus loin possible en ce sens, tout en préservant les libertés.

Enfin, ces outils servent à la lutte contre l'usurpation d'identité en ligne. Il importe donc de rassurer nos concitoyens. La Quadrature du net a formé un recours contre le décret en Conseil d'État autorisant cette application mobile : à nous de prouver que le dispositif est sécurisé.

Quant aux élections européennes, aucune attaque significative n'a été identifiée. La loi du 22 décembre 2018 relative à la lutte contre la manipulation de l'information a créé le référé civil pour faire cesser la diffusion de fausses informations ; un dispositif ministériel a également été mis en place. Mais il n'a pas été nécessaire de recourir à ces outils. L'Agence nationale de la sécurité des systèmes d'information (Anssi) a effectué à notre demande un audit, et nous avions un dispositif de supervision : aucun dysfonctionnement n'a été détecté. Cependant le « retex » (retour d'expérience) n'est pas achevé : si des anomalies étaient identifiées avant la conclusion de vos travaux, je vous en tiendrais informés.

Le développement du vote électronique n'est pas à notre programme : sujet trop sensible et outil pas forcément indispensable...

M. Gérard Longuet, rapporteur. - Il ne faut pas casser l'ambiance des soirées électorales !

M. Christophe Castaner, ministre. - C'est ce que j'allais dire. Comme élu rural des Alpes-de-Haute-Provence, j'y suis attaché ! La question de la dématérialisation de la propagande électorale reviendra en revanche à l'ordre du jour... N'oublions pas la rupture numérique, de plus en plus réduite, mais qui existe.

Un mot sur votre question sur l'utilisation des algorithmes. Une expérience a été menée par la gendarmerie au moyen d'un algorithme d'intelligence artificielle pour avancer dans la connaissance du phénomène délictuel. Depuis le XIX^{e} siècle, des travaux ont été menés en matière de criminologie prédictive - je songe à ceux des époux Glueck - qui visaient à définir une sorte de prédestination au comportement délictuel. Des études ont plus récemment montré que les heures propices aux actes criminels n'étaient pas les mêmes en Haute-Savoie, à Marseille ou à Paris. L'intelligence artificielle travaille à partir des infractions ciblées, sans utiliser les données personnelles, mais en traitant des informations de masse et en procédant à des recoupements territoriaux. Il ne s'agit pas de prédire l'avenir, mais ce type d'expérience préfigure ce que pourrait être la police ou la gendarmerie de demain, pour gagner en efficacité. Même chose pour la sécurité routière : en identifiant des paramètres tels que les aléas météorologiques ou les heures auxquels les actes délictueux sont plus fréquents, on pourrait ajuster la présence préventive des patrouilles sur le terrain.

Les risques de détournement des outils numériques existent. Il ne faut pas en avoir peur ni, à l'inverse, être trop candide : nos partenaires n'appliquent pas forcément les mêmes limites que nous, et nos adversaires, lorsqu'ils soutiennent la cybercriminalité, n'ont aucune limite... N'ayons pas de ces pudeurs de gazelle qui empêcheraient même d'aborder le sujet. Nous pouvons en parler ! La décision, elle, revient au Parlement. Mais il est clair que nous avons besoin de dispositifs de contrôle, d'arbitres et de juges extérieurs, afin de garantir le meilleur usage de ces outils.

M. Gérard Longuet, rapporteur. - Êtes-vous en relation avec les autres responsables européens pour définir des types de coopération possibles avec les Gafam ?

M. Christophe Castaner, ministre. - Bien sûr, et le récent sommet des ministres de l'intérieur à Helsinki a consacré sa première partie à ce sujet, afin de parvenir à une position commune pour négocier avec les Gafam et d'autres. La présidence finlandaise a aussi présenté une initiative sur l'intelligence artificielle afin que chaque État membre n'avance pas seul dans son coin. J'ajoute que le Parlement européen est très jaloux des libertés - un peu comme la commission des lois du Sénat !

M. Patrick Chaize. - Une question liminaire puisque nous abordons le vote électronique : pour les personnes handicapées, et notamment pour les non-voyants, ne pourrait-il tout de même pas être envisagé ?

Vous avez beaucoup parlé des comportements : il faut donc parler éducation et formation ! À cet égard, quelles actions sont menées conjointement avec les autres ministres ? Car le numérique est un sujet transversal. J'ai milité en ce sens ; nous avons créé un groupe d'études numériques qui regroupe l'ensemble de nos commissions. Hélas, le secrétariat d'État au numérique n'est plus sous la responsabilité transversale du Premier ministre et je ne perçois guère cette transversalité au Gouvernement. Comment le sujet est-il traité en son sein ?

J'aimerais avoir votre avis sur le texte « anti Huawei » - la proposition de loi sur la sécurité des réseaux mobiles - adopté il y a quelques semaines par le Parlement. C'est le ministre de l'économie qui participait à la discussion ; or il s'agit de sécurité intérieure !

Mme Viviane Artigalas. - Monsieur le ministre, vous avez dressé une véritable revue de la question, sans omettre les points de vigilance, et en montrant combien la souveraineté numérique est une mission régalienne essentielle de l'État. Celui-ci doit poser un cadre transversal : je souhaite que vous nous disiez plus précisément comment l'exécutif organise le travail collectif sur cette mission si importante, qui concerne tous les ministères.

Vous avez parlé de la prise de conscience, de la vigilance, de la prévention et de l'éducation : il y faut des moyens humains et financiers, un personnel très compétent, à l'affût de toutes les novations utilisées par nos

adversaires. Quels moyens, concrètement, sont mis en oeuvre ? Quels moyens seraient nécessaires ?

M. Stéphane Piednoir. - Les jeunes et les enfants devraient recevoir une formation qui leur donne de bons réflexes pour leur vie entière : vous avez parlé du permis Internet, un laissez-passer favorisant un bon usage d'internet... Mais la vigilance conduit parfois à la défiance, et certaines associations, voire certains élus, contestent des dispositifs simples, tels que les compteurs Linky. Sincérité et confiance sont essentielles en politique : comment convaincre que les dispositifs sont sûrs, qu'il ne sera pas fait un usage détourné d'une future identité numérique ?

M. André Gattolin. - Un éventuel blackout numérique nous exposerait à des risques immenses, notamment pour la santé publique. Dans ce domaine, envisage-t-on des solutions de secours, des situations offline, une forme de « plan Orsec » en cas de catastrophe numérique locale ou nationale ? Sans tomber dans la science-fiction, ces questions font-elles l'objet de réflexions ?

En matière internationale, on vante le multilatéralisme, mais on doit souvent se contenter d'accords bilatéraux, et les conventions fiscales historiques ont bien du mal à tenir compte de l'extraterritorialité des entreprises. Le numérique nous place également face à des difficultés pour lutter contre la criminalité. Disposons-nous aujourd'hui des instruments législatifs nécessaires ? Il y a quatre ans, la France a conclu un accord d'extradition avec un grand pays d'Orient : elle a réclamé plusieurs centaines d'extraditions au titre des fraudes bancaires, et l'État en question n'a jamais répondu à nos demandes, alors que, de notre côté, nous extradions vers lui des personnes accusées de crime. Comment adapter le cadre juridique au monde globalisé dans lequel nous vivons ?

M. Laurent Lafon. - En matière de cybercriminalité, on a le sentiment, peut-être à tort, d'être systématiquement sur la défensive. Se développe ainsi de manière insidieuse le sentiment d'impunité des cybercriminels, dont l'identification est très difficile, et qui sont rarement situés sur le territoire national.

Premièrement, cette impunité est-elle réelle ou bien vos services parviennent-ils à mener des enquêtes approfondies sur les personnes physiques coupables de ces actes ? Deuxièmement, quels sont, en la matière, les liens entre votre ministère et le ministère de la justice ? Bien sûr, je poserai également cette question à Madame la Garde des sceaux, que nous auditionnerons demain. Troisièmement, quel est l'état exact des coopérations internationales existantes, notamment avec les pays de l'Est de l'Europe ? Vous avez évoqué l'Union européenne et le G7 ; mais la plupart des cybercriminels semblent ailleurs, dans des pays où les libertés publiques et individuelles n'ont pas forcément la même force que chez nous. Peut-on

développer la collaboration internationale en la matière, comme on l'a fait pour lutter contre le terrorisme, à la suite des attentats ?

M. Rachel Mazuir. - Nous sommes effectivement engagés dans une démarche essentiellement défensive, qui vise en particulier les Gafam. En la matière, le Gouvernement appelle de ses voeux une souveraineté européenne : on ne peut qu'être d'accord avec lui sur ce point. Peut-on également envisager une souveraineté industrielle européenne, ou bien est-il trop tard ?

Quant aux géants chinois du numérique, les BATX - Baidu, Alibaba, Tencent, Xiaomi -, ils semblent pour l'heure rester l'arme au pied ; mais, ici où là, ils entrent tout de même dans le jeu. Quel est votre sentiment à leur égard ?

M. Franck Montaugé, président. - Pourriez-vous nous préciser votre réponse au sujet des manipulations électorales, non au moment du vote, mais en amont ? Nous pensons notamment à l'affaire Cambridge Analytica. Ces manipulations de grande envergure sont une véritable préoccupation.

M. Christophe Castaner, ministre. - Sur ce point, lors des dernières élections européennes, nous avons mis en place un dispositif interministériel à même de contrer la moindre attaque de *fake news* ; en l'occurrence, il n'y en a pas eu. J'ajoute que je n'ai pas de retour d'expérience quant aux élections précédentes...

M. Franck Montaugé, président. - ...Ma question va au-delà des *fake news* ; je pense à des manipulations de données, à l'insu des citoyens, destinées à influencer leur vote et déployées à une échelle industrielle.

M. Christophe Castaner, ministre. - Le dispositif interministériel dont il s'agit couvrait précisément l'ensemble des éléments susceptibles d'être exploités. Politiquement, la maîtrise d'informations relatives aux habitudes ou aux goûts de nos concitoyens permet aujourd'hui d'envoyer tel ou tel message avantageant un candidat face aux autres. C'est sur ce point qu'il faut agir, en veillant au respect du cadre législatif : les informations personnelles ne sont pas à libre disposition. Elles ne peuvent donc pas être utilisées dans le cadre d'une campagne, comme on a pu le voir dans tel ou tel pays étranger. À terme, il faudra que ce dispositif gouvernemental, qui, par définition, n'est pas à même d'inspirer la confiance de tous les partis, de tous les candidats, soit aussi dépolitisé que possible : ainsi, il deviendra un guichet auquel chaque candidat pourra recourir.

J'en viens aux actions de prévention, que le ministère de l'intérieur déploie à plusieurs niveaux. Au titre de la sensibilisation comme de l'enquête, 8 600 policiers et gendarmes sont actuellement spécialisés sur ces sujets. J'ai la volonté de renforcer ces effectifs de 800 personnes d'ici à la fin du quinquennat. Ces agents assument toutes les missions, y compris judiciaires, que l'on connaît dans la chaîne d'engagement de la police et de la gendarmerie ; mais s'y ajoutent des missions de prévention. Il s'agit à la fois

d'actions de haut niveau, qui peuvent être accompagnées par la DGSI - cette dernière est mobilisée pour les opérateurs d'importance vitale, et elle fait l'objet d'un plan de recrutement et de renforcement de 1 900 nouveaux effectifs, dont une partie sera consacrée à ces sujets.

De plus, conformément au plan d'action gouvernementale validé par le Président de la République, les préfets de région vont animer, sur l'ensemble de territoire, un travail de sensibilisation des acteurs, notamment des entreprises, et mettre à leur disposition les différentes ressources existantes.

À titre judiciaire, pour la phase d'instruction, un référent est aujourd'hui présent dans chaque zone pour sensibiliser les acteurs économiques. S'y ajoute un dispositif d'hypermobilisation dans la ruralité, avec la gendarmerie nationale : dans tel territoire, une entreprise de vingt salariés représente un enjeu majeur.

Enfin, la sensibilisation aux comportements est déployée en faveur de nos concitoyens, en lien avec l'éducation nationale. Il s'agit du « permis internet », qui a concerné 2 millions d'enfants et, plus largement, du travail d'éveil des consciences. L'éducation nationale est très mobilisée en la matière.

Monsieur Chaize, le secrétaire d'État au numérique est, certes, rattaché à Bercy ; mais ce nouveau positionnement n'a aucune conséquence sur le travail interministériel. L'animation horizontale se poursuit comme par le passé. De plus, la revue stratégique de cyberdéfense fournit un cadre de travail transversal. Elle est pilotée par le ministère des armées, qui agit de manière interministérielle. De son côté, l'Anssi a élaboré un guide d'hygiène informatique. Ce document est transversal et interministériel, à l'instar de la plateforme *cybermalveillance.gouv.fr*.

C'est à ces différents niveaux qu'il faut agir pour changer les comportements, dans le public comme dans le privé : menacer une grande banque française, c'est aussi porter atteinte à la souveraineté nationale, d'autant que les coûts en jeu sont très élevés. Il y a quelques années, le spectre des cyber-rançons était extrêmement large - on attaquait les particuliers en leur demandant 100 euros. Aujourd'hui, le spectre s'est fortement réduit - on attaque quelques grands groupes, mais on leur demande 150 millions d'euros.

Monsieur Gattolin, vous m'interrogez au sujet de la gestion de crise. Je ne peux pas vous en dire trop au sujet d'un éventuel blackout. Mais le ministère de l'intérieur dispose, comme les autres ministères, d'un plan de continuité d'activité. Outre les attaques, il faut se préparer au risque de panne du réseau numérique, notamment en région parisienne : nous avons demandé aux opérateurs de travailler sur ce point.

Je vous renvoie au travail que le Secrétariat général de la défense et de la sécurité nationale (Sgdsn) a consacré à ces gestions de crise. Il existe, en

outre, un plan interministériel. Des exercices réguliers sont menés pour faire face aux risques d'attaques et le ministère de l'intérieur dispose de son propre système de contrôle interne. Le but, c'est de disposer d'une architecture de sécurité, y compris électronique.

En cas d'attaque ou de panne, nous devons nous préparer à la possibilité de travailler en mode dégradé : nous avons pris cette précaution tout récemment encore, à l'occasion du G7, et nous disposons, en la matière, de ressources expertes en interne.

Monsieur Chaize, vous évoquez aussi la loi dite - à tort ! - « anti-Huawei ». À l'époque où j'étais vice-président de la région PACA - il n'y a pas si longtemps -, j'ai pu visiter le siège de cette entreprise, à Shenzhen. Huawei s'apprêtait alors à produire des téléphones portables, il a acquis sur ce marché une position dominante. Aujourd'hui, cet opérateur applique une loi chinoise donnant aux autorités du pays des pouvoirs exorbitants par rapport à notre propre droit national, que j'ai précédemment évoqués. Nous voulons tout simplement fixer des critères de sécurité pour autoriser le déploiement d'équipements indépendants et, ce faisant, garantir notre souveraineté. Bref, nous ne contestons pas la place de qui que ce soit parmi les opérateurs privés, mais nous ne voulons pas non plus faire preuve de naïveté.

En l'occurrence, nous sommes face à un changement de modèle : la 3G a été développée sur le modèle européen, mais ce n'est pas le cas de la 5G. Bruno Le Maire vous apportera certainement des réponses plus complètes en la matière. Mais, j'y insiste, il ne faut pas laisser ce champ entier déserter l'Europe. Nous avons évoqué la portée extraterritoriale du droit américain. La véritable solution, c'est notamment d'avoir une monnaie européenne suffisamment puissante pour que les entreprises européennes puissent travailler à travers le monde sans utiliser le dollar. Il faut raisonner de la même manière au sujet du cloud et, plus largement, pour l'ensemble de nos outils.

Pour les personnes handicapées, nous voulons garantir les plus grandes facilités de vote, avec un site internet d'accès aux professions de foi , avec la possibilité d'être accompagné dans l'isoloir - ce que le président du bureau de vote peut autoriser - et avec les procurations, ou encore avec le déplacement à domicile de l'officier de police judiciaire. Nous étudions également de nouvelles techniques. Cela étant, nous n'envisageons pas la dématérialisation totale du vote pour les seules personnes souffrant de handicap visuel. Non seulement nous n'aurions sans doute pas les moyens d'imposer un tel dispositif à tous les bureaux de vote de France - il risque d'être extrêmement coûteux -, mais il faut éviter toute rupture d'égalité.

Au sujet des coopérations internationales, le risque d'impunité fait nécessairement l'objet de discussions. Certains criminels savent pertinemment choisir le pays à partir duquel ils émettent, afin de ne pas être

inquiétés. J'ai pu m'en assurer une nouvelle fois en visitant la plateforme Pharos, pour ce qui concerne les contenus pédopornographiques.

Ces enjeux font l'objet d'échanges et de discussions, et nous allons avancer. Avec certains pays, nous pouvons travailler de manière satisfaisante, plusieurs exemples récents le prouvent. Je pense à l'atteinte frauduleuse qui a infecté 450 000 ordinateurs à travers le monde et au sujet de laquelle la gendarmerie nationale a publié une communication il y a quelques jours. Les investigations ont permis de localiser la source malveillante en Palestine et l'attaque a été neutralisée. En revanche, il ne me semble pas que l'individu en question ait été interpellé. On observe, à cet égard, la limite de notre système.

Avec certains pays, les coopérations sont parfaites ; avec d'autres, il est nettement plus compliqué d'agir. De surcroît, les opérations multiples peuvent impliquer trois, quatre, voire vingt-huit pays, à l'échelle de l'Union européenne. Face à une affaire massive d'escroquerie, nous avons abouti, en France, à 17 interpellations en flagrant délit, et à 95 interpellations partout dans le monde. Cela étant, de manière générale, les marges de progrès restent importantes.

Enfin, le ministère de l'intérieur travaille de manière tout à fait efficace avec le ministère de la justice. Depuis que je suis ministre de l'intérieur, je n'ai pour ainsi dire observé aucun dossier au titre duquel un obstacle a empêché notre bonne action mutuelle. Il peut y avoir des tensions, mais je considère cette fluidité à la fois comme une évidence et comme une exigence. Dans quelques jours, je présenterai ainsi un nouveau plan de lutte contre les stupéfiants. A ce titre, je défendrai le dispositif le plus interministériel possible, car il faut sortir de nos chapelles. Face à la cybercriminalité, nous avons, avec le ministère de la justice, une véritable proximité, que je qualifierai même de culturelle.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible en ligne sur le site du Sénat.

Audition de M. Bruno Sportisse, Président-Directeur Général de l'INRIA, le 2 septembre 2019

M. Franck Montaugé, président. - Nous recevons M. Bruno Sportisse, président-directeur général de l'Institut national de recherche en informatique et en automatique (Inria).

Cette audition sera diffusée en direct sur le site internet du Sénat. Elle fera également l'objet d'un compte rendu publié. Un faux témoignage devant notre commission d'enquête serait passible des peines prévues aux articles 434-13, 434-14 et 434-15 du code pénal.

Conformément à la procédure applicable aux commissions d'enquête, M. Bruno Sportisse prête serment.

M. Franck Montaugé, président. - L'Inria est l'un des principaux centres de recherche français dédiés aux sciences du numérique, de l'informatique et aux mathématiques, souvent à l'interface d'autres disciplines. Il compte environ 200 équipes de recherche, en général communes avec des partenaires académiques, qui impliquent plus de 3 000 scientifiques. En outre, il travaille avec de nombreuses entreprises et il a accompagné la création de plus de 160 start-up.

Par la position qu'il occupe, l'Inria est un acteur essentiel de la recherche dans le domaine des technologies de souveraineté nationale. Il participe notamment à la mission interministérielle relative à la blockchain, ou technologie de registres distribués, avec l'institut Mines-Télécom et le Commissariat à l'énergie atomique (CEA). Cette mission rendra ses conclusions en novembre prochain. Elle a pour but de permettre à la France de jouer un rôle d'influence à l'échelle internationale dans ce domaine.

En outre, en matière de cybersécurité, l'Inria a développé avec l'Agence nationale de la sécurité des systèmes d'information (Anssi) un étroit partenariat dont vous nous expliquerez l'ambition.

Pour l'ensemble de ces raisons, il nous a paru intéressant d'entendre votre conception de la souveraineté numérique et votre appréciation des politiques publiques menées en la matière.

M. Bruno Sportisse, président-directeur général de l'Inria. - La souveraineté numérique est un sujet clef pour l'autonomie stratégique de la France. Il y a quelques années, un investisseur connu de la Silicon Valley, Marc Andreessen, annonçait que le logiciel allait « dévorer le monde ». Aujourd'hui, nous y sommes : le logiciel dévore le monde, méthodiquement, dans tous les domaines de l'économie et de la société. Les algorithmes et les logiciels jouent un rôle critique dans l'accélération numérique. À cet égard, je formulerai trois remarques.

Premièrement, il faut analyser la situation nouvelle dans laquelle nous place l'intelligence artificielle. Cette dernière représente la forme aboutie de la déferlante numérique, très loin des représentations fantasmées. Elle repose sur la conjonction de masses de données, souvent privées, issues de plusieurs sources avec des puissances de calcul disponibles et des algorithmes plus ou moins éprouvés, déployés *via* des logiciels, permettant de les faire parler et, à des fins de prédiction, de les rendre intelligentes.

Or, dans tous les champs de la société et de l'économie, des acteurs savent que cette puissance prédictive peut, sous certaines conditions, améliorer significativement leur activité. Cette maturité est également un changement capital, et elle survient dans un contexte de démocratisation du numérique. Désormais, toutes les composantes de notre société, privées ou publiques, sont concernées.

La souveraineté numérique met donc en jeu notre souveraineté tout court. Elle n'est plus réductible à une affaire de spécialistes, à une question de « tuyaux » relevant de l'informatique de gestion, comme on pouvait encore le dire il y a cinq ans : ce temps est révolu. C'est à la fois une source de risques - des pans entiers de notre souveraineté peuvent être perdus - et une occasion à saisir pour redéfinir radicalement un grand nombre de sujets, qu'il s'agisse des verticaux économiques, de la santé, de l'agriculture, de la mobilité, de la gestion de nos villes et de l'action publique en général. Tous les acteurs existants sont susceptibles de s'approprier le numérique. Encore doivent-ils assimiler l'exigence stratégique, en reconnaissant que le numérique est, non à côté, mais au coeur de leur activité, et suivre les bonnes modalités opérationnelles, qui reposent sur l'accès aux talents, sur des investissements massifs en faveur de la prise de risques et sur une régulation fixant un cadre à la confiance et à l'innovation numérique sous contrôle.

Deuxièmement, plusieurs points clefs doivent être garantis pour renforcer la souveraineté numérique. Les trente dernières années l'ont montré : le numérique se développe d'abord dans des écosystèmes d'acteurs propices à l'apparition de champions. Imaginez que l'une des grandes plateformes numériques dominant le monde ait une base française : notre société s'approprierait le sujet de la souveraineté numérique d'une manière radicalement différente.

Ces écosystèmes sont fondés à la fois sur des talents entrepreneuriaux ayant accès à des investissements massifs, publics et privés, prêts à assumer le risque, sur des conditions de jeu fixées par l'État, favorisant la croissance des entreprises, et sur une capacité d'accès à des talents scientifiques, technologiques et entrepreneuriaux au sein de grands campus universitaires de rang mondial.

Dans ce cadre, l'État doit soutenir des infrastructures critiques et il faut probablement redéfinir la notion d'infrastructure. La puissance de calcul disponible, nécessaire pour ne pas dépendre des outils proposés par les

grandes plateformes numériques, est une infrastructure ; les logiciels libres en sont une autre, et ils permettent des dynamiques d'ouverture du champ de l'innovation. Le développement d'internet a reposé sur des standards ouverts et l'Inria a joué un rôle clef à ce titre en défendant, à l'échelle européenne, le consortium mondial pour le web, ou W3C.

De vraies infrastructures se déploient autour du logiciel libre. L'Inria développe plusieurs projets à empreinte mondiale, comme la bibliothèque *scikit-learn* - bibliothèque d'apprentissage statistique en langage informatique Python -, boîte à outil technologique pour tous les ingénieurs, tous les acteurs qui veulent faire de l'intelligence artificielle, logiciel libre qui compte 500 000 à 1 million d'utilisateurs dans le monde. Citons encore le projet *software heritage*, projet de bibliothèque mondiale du logiciel, garantissant une traçabilité et participant, de ce fait, de la souveraineté numérique.

La commande publique innovante a toute son importance dans le développement des acteurs, témoin ce que fait l'agence Darpa aux États-Unis. Il faut également prendre en compte les conditions de régulation, pour ce qui concerne la confiance numérique, notamment pour la maîtrise des algorithmes. C'est tout l'enjeu actuel de l'intelligence artificielle. À ce titre, l'Inria mène le projet TransAlgo, relatif à la transparence des algorithmes. S'y ajoutent des programmes *ad hoc*, nationaux ou européens, pour diverses innovations. D'ici à quelques années, l'arrivée d'ordinateurs quantiques pourrait changer radicalement la donne, notamment en termes de sécurité numérique. Or, au-delà des volets matériels de ces technologies, les volets « logiciels » et « algorithmes » ont un rôle clef. Il faut dès à présent créer un écosystème autour du quantique.

Voilà pourquoi il faut revoir la notion d'infrastructure. Toute politique en faveur du numérique est d'ailleurs étroitement liée aux politiques en faveur de l'innovation et du financement de cette dernière.

De surcroît, la guerre du numérique est une guerre des talents, et les États doivent être en mesure de soutenir le développement de ces derniers en accompagnant leur prise de risque. Cet effort passe avant les grands plans, si séduisants et rassurants soient-ils. Si nous ne formons pas des talents de haut niveau dans le numérique, si nous ne leur offrons pas les perspectives nécessaires pour s'épanouir en France et y créer de la valeur, nous ne pourrons pas mener les prochaines batailles de la souveraineté numérique.

Dans ce contexte, le soutien à la recherche, à la formation et aux dynamiques d'innovations réelles propres au numérique me semble stratégique. La souveraineté numérique, c'est d'abord la capacité d'avoir des talents numériques à même de développer leur ambition en France.

Troisièmement et enfin, j'insisterai sur le rôle de l'Inria dans ce contexte. Cet institut a été créé il y a un peu plus de cinquante ans, dans le

cadre du plan Calcul, afin de garantir une souveraineté numérique nationale. Il s'agit d'un établissement public à caractère scientifique et technologique, placé sous la double tutelle des ministères chargés de l'industrie et de la recherche et doté d'un budget annuel de l'ordre de 240 millions d'euros, dont 170 millions d'euros de subventions pour charges de service public.

L'originalité de l'Inria, c'est son modèle organisationnel. Il dénombre 200 petites unités mobiles, les équipes projet, réparties sur le territoire et relevant de huit centres de recherche en partenariat avec les universités et avec d'autres établissements, comme le CNRS (Centre national de la recherche scientifique). Ces équipes sont créées pour quatre ans, sur la base de feuilles de route de recherche et d'innovation, d'où leur grande agilité. Dans ce cadre s'épanouit une recherche de rang mondial : c'est ce que vient de relever le Haut Conseil de l'évaluation de la recherche et de l'enseignement supérieur (Hceres). S'épanouissent également des partenariats industriels avec des leaders mondiaux, avec des leaders français, cependant que de petits projets innovants voient le jour sur l'initiative de start-up technologiques. Au total, en un peu plus de vingt ans, plus de 170 start-up ont été issues des travaux de l'Inria.

En résumé, l'Inria est l'institut du logiciel et des algorithmes, à la croisée des mathématiques et de l'informatique, et son action est de plus en plus interdisciplinaire. Un quart de nos équipes sont ainsi dédiées à l'application du numérique dans le domaine de la santé.

L'Inria est engagé dans la conclusion d'un nouveau contrat d'objectifs et de performance (COP) avec l'État pour 2019-2023. Le maître-mot de ce COP, qui devrait être finalisé en octobre prochain, c'est l'impact. En ce sens, l'Inria assume pleinement son statut d'outil public pour construire une souveraineté numérique au service de la transformation de notre société et de notre économie.

Pour ce qui concerne notre positionnement scientifique, notre priorité pour les années qui viennent, c'est la sécurité numérique, l'intelligence artificielle responsable et maîtrisée, le calcul haute performance et sa rencontre avec l'intelligence artificielle, la révolution quantique, et, de surcroît, le suivi de grands secteurs applicatifs comme la médecine personnalisée, laquelle est étroitement liée au développement du numérique, ou encore la maîtrise de l'énergie dans toutes ses composantes.

Pour ce qui concerne notre ambition d'impact économique, nous entendons renforcer nos liens avec le tissu industriel français, notamment numérique, avec Atos, Thales ou encore Dassault Systèmes, mais aussi avec le tissu des entreprises de taille intermédiaire (ETI). En parallèle, nous entendons accroître significativement le flux de projets innovants conçus par des start-up technologiques issues de nos équipes de recherche. C'est tout le sens de l'accord que nous venons de signer avec Bpifrance. Ainsi, nous

prévoyons d'atteindre, dans cinq ans, un flux annuel d'une centaine de projets pour irriguer notre tissu industriel.

Pour l'appui aux politiques publiques, nous nous adaptons aux évolutions de l'enseignement supérieur, de la recherche et de l'innovation, fondées sur la création de campus universitaires de rang mondial. Par ailleurs, l'Inria s'est vu confier un rôle clef dans le plan Intelligence artificielle annoncé par le Président de la République en mars 2018, à la suite du rapport Villani. Non seulement notre institut joue son rôle d'opérateur de recherche, mais il est également coordonnateur de ce plan. Enfin, nos partenariats en matière de sécurité et de défense, avec des acteurs comme l'Anssi ou l'Agence de l'innovation de défense, sont absolument stratégiques.

Ainsi décliné, notre positionnement stratégique se fonde sur une conviction : l'Inria est un outil public pour participer à la construction et au renforcement, par la recherche et par l'innovation, de notre souveraineté numérique.

M. Gérard Longuet, rapporteur. - Selon vous, « le logiciel est une infrastructure ». Cette formule apporte une véritable valeur ajoutée à notre raisonnement. Mais, à ce sujet, jugez-vous irréversible l'appropriation d'internet par un petit nombre de grands opérateurs au comportement monopolistique, notamment dans le domaine des systèmes d'exploitation ? Dans quelles conditions les logiciels libres peuvent-ils reconquérir une part de marché significative ? D'ailleurs, seront-ils destinés à tous ou bien seront-ils réservés à la valeur ajoutée de ceux qui créent de l'activité et qui innovent ?

Votre expérience de la recherche et de l'industrie vous donne-t-elle le sentiment qu'il existe, à cet égard, des obstacles typiquement français ? Vous évoquez la question des talents : à ce titre, on pense aux problèmes de financement et aux effets de taille. Comment rivaliser avec les acteurs américains, qui sont de taille mondiale, qui disposent de financements en conséquence et qui peuvent s'offrir les talents dont ils ont besoin ? Au fond, dans ce monde ouvert, marqué par une certaine unité culturelle, où le *brain drain* doit marcher à fond, la lutte n'est-elle pas profondément déséquilibrée ? L'Europe en général et la France en particulier ne sont-elles pas structurellement mal outillées pour cette chasse aux talents ?

L'Inria considère-t-il que la France est suffisamment présente dans les instances de gouvernance et de normalisation des systèmes numériques mondiaux ? Nous avons été étonnés de voir certains organismes se retirer de cette gouvernance au motif qu'en définitive il ne s'y passait rien d'important. À ce sujet, quel est votre sentiment et quelle devrait être selon vous la politique de la France ? Dans le même esprit, comment soutenir les logiciels libres ? La commande publique, pour l'équipement des administrations, peut-elle être un levier d'action ? À l'inverse, ne risque-t-on pas de nourrir l'illusion d'un cloud national souverain ? Bref, quel doit être le jeu d'une

grande puissance qui n'est pas, hélas ! la première en la matière - à savoir la nôtre ?

Enfin, en tant que représentants des territoires, nous sénateurs regardons avec une certaine inquiétude la métropolisation à l'oeuvre. L'Île-de-France n'a rien perdu de sa superbe, bien au contraire. Heureusement, quelques métropoles émergent en dehors d'elle, parce que l'industrie les a choisies comme points d'appui : ainsi de Toulouse ou de Bordeaux pour l'aéronautique. Mais, au-delà, nous avons le sentiment que les universités de province s'essoufflent un peu et sont désormais sur la défensive. Le ressentez-vous également ?

M. Bruno Sportisse. - J'ai simplement mentionné la dynamique singulière des logiciels libres : mon discours n'était en aucun cas exclusif. Chaque année, une centaine de nouveaux logiciels sont reconnus par les équipes de l'Inria. Certains sont libres, d'autre non, car la création de valeur ne le permet pas. Sur ce sujet, il ne faut pas avoir de dogme dans un sens comme dans l'autre.

Cela étant, le monde du logiciel libre permet souvent aux acteurs économiques de recruter les talents dont ils ont besoin en puisant dans les communautés de développeurs. Il est important que les acteurs européens, notamment français, y prennent leur part.

Au sujet d'internet, la dynamique des standards ouverts peut être un levier d'action pour la France et pour l'Europe. Le web s'est précisément constitué sur la base de quelques standards ouverts, partagés par une communauté construite il y a plus de vingt ans, à savoir le W3C. Ce dernier repose sur quatre piliers, dont l'un est à Sophia Antipolis, où l'Inria a d'ailleurs l'un de ses centres régionaux. Je suis moi-même président de ce noeud européen du web. Cette dynamique de standards ouverts s'inscrit dans un cadre multilatéral et, si elle est renforcée, elle est de nature à ne pas tomber dans les biais que vous avez évoqués. En d'autres termes, les instances multilatérales existent déjà : il faut être capable de les faire vivre dans la durée en se gardant de toute naïveté.

Pour ce qui concerne l'articulation entre la recherche et l'industrie, la clef est la mobilité entre le monde académique et le monde de l'entreprise. Le secteur numérique s'y prête bien, et la loi Pacte est de nature à renforcer cette articulation dans la durée. À ce titre, pour ce qui concerne le numérique, je suis plutôt optimiste : il existe de nombreux exemples de mobilité réussie dans la durée, notamment en Amérique. De son côté, la France a des marges de progression.

En revanche, le *brain drain* est un grave sujet de préoccupation, qui impose de se pencher sur l'environnement de recherche offert à nos talents. C'est tout l'enjeu du projet de loi de programmation pluriannuelle de la recherche annoncé par le Premier ministre. Nos talents doivent rester durablement dans nos laboratoires pour créer de la valeur en France.

Pourquoi, à trente-cinq ans, un chercheur de niveau mondial resterait-il en France, dans le secteur public, avec des conditions salariales significativement dégradées ? Les grands du numérique disposent de laboratoires de recherche menant des travaux tout aussi fondamentaux que nos laboratoires publics. En revanche, ainsi privatisée, l'action d'un chercheur ne sera peut-être plus à même de créer des emplois. Il est donc essentiel de garder ces chercheurs dans le secteur public, en lien avec l'industrie, car il faut sans cesse former de nouveaux jeunes. C'est l'enjeu du plan Intelligence artificielle et de la constitution d'instituts interdisciplinaires d'intelligence artificielle, les 3IA ; c'est l'enjeu de la programmation pluriannuelle ; et ce combat doit être mené dans la durée. Si le *brain drain* devient massif, s'il n'y a plus de talents, il n'y aura plus de souveraineté.

Vous évoquez les instances de gouvernance mondiale et la question de la standardisation. C'est un sujet clef, qui suppose une bonne coordination entre la recherche et l'industrie. Un nombre significatif de nos chercheurs est engagé dans des actions de standardisation, et l'un des volets du plan Intelligence artificielle y est consacré. Il s'agit à la fois d'un enjeu éthique et d'une question industrielle.

M. Gérard Longuet, rapporteur. - Selon vous, est-il possible de construire, dans cette démarche de gouvernance, une solidarité européenne durable ?

M. Bruno Sportisse. - Il faut tenir compte de la diversité des acteurs et des situations. Chaque État s'emploie à tenir ses propres lignes industrielles. Avant tout, la France doit assurer une bonne coordination de l'ensemble de ses acteurs. Ces derniers sont tous de bonne volonté, mais il faut faire vivre la position française. Ensuite, en procédant par cercles concentriques, les positions européennes sont à construire selon les domaines. Pour l'intelligence artificielle, les efforts de coordination nationaux et européens sont engagés. En tant que Français et Européens, nous devons impérativement agir en ce sens.

Enfin, l'action de l'Inria est très largement décentralisée : six de nos huit centres de recherche sont situés en dehors de l'Île-de-France - Grenoble, Nancy, Lille, Bordeaux, Rennes et Nice -, et leur dynamique s'inscrit pleinement dans celle des grands campus universitaires où ils sont présents. Mais je ne peux parler que des centres de recherche où opère l'Inria.

M. Stéphane Piednoir. - La question des talents est essentielle, car la recherche en dépend ; et, en évoquant le plan Calcul, on mesure le chemin parcouru. Les questions d'ordre financier mises à part, éprouvez-vous, au sein des universités, des difficultés à former le vivier de chercheurs ? La suppression du sacro-saint bac S est-elle de nature à inspirer des inquiétudes quant à la qualité de nos étudiants en mathématique et en informatique ?

M. Bruno Sportisse. - Votre question renvoie à un sujet plus large : l'attractivité des sciences et des technologies, qu'il faut développer assez tôt

dans les parcours scolaires. L'Inria se préoccupe effectivement d'attirer de jeunes diplômés de l'enseignement supérieur. Il regroupe non seulement des chercheurs, mais aussi des développeurs de logiciels. Mais, avant tout, il faut donner aux jeunes l'envie de se tourner vers les sciences et les technologies, qu'il s'agisse du numérique ou d'autres domaines. Voilà pourquoi, dans la durée, nous menons des actions volontaristes en milieu scolaire de concert avec le ministère de l'éducation nationale.

M. Laurent Lafon. - Pour obtenir des financements en faveur de la recherche de la part du secteur privé, l'Inria élabore-t-il des partenariats avec telle ou telle entreprise, française ou étrangère, travaillant notamment dans le domaine de l'intelligence artificielle ? Dans l'affirmative, quels garde-fous placez-vous ou pourriez-vous concevoir pour éviter les « fuites » au profit d'entreprises pour qui la souveraineté numérique n'est pas nécessairement la priorité ?

M. Bruno Sportisse. - Votre question est particulièrement pertinente au regard de notre action dans la durée. Il y a une quinzaine d'années, l'Inria a conclu un partenariat stratégique avec un grand acteur technologique extra-européen ; et, à l'époque, plusieurs de ses partenaires ont exprimé la crainte qu'une telle initiative ne porte atteinte à notre souveraineté numérique.

Bien au contraire, nous suivons en la matière une position constante : de telles actions sont le moyen de faire avancer notre pays, car il faut être au contact des meilleurs pour prendre part aux évolutions à l'oeuvre et attirer nous-mêmes des talents. La ligne de crête est étroite, mais c'est le seul chemin permettant d'avancer.

Cela étant dit, nous devons également être capables de travailler avec d'autres partenaires, notamment pour irriguer le tissu français des grandes entreprises et des ETI, afin de renforcer nos interactions avec l'industrie. Les « garde-fous », pour reprendre vos termes, relèvent de la gouvernance des partenariats. C'est à nous de définir quels sujets peuvent ou non faire l'objet de coopérations de cette nature.

Cette mécanique de partenariats maîtrisés avec le monde industriel doit relever d'une véritable stratégie. Elle ne doit pas obéir, avant tout, à une recherche de financements, ce qui est souvent un petit travers français. Pour sa part, l'Inria a toujours suivi une stratégie de l'impact. Ainsi, il serait essentiel de nouer des partenariats avec quelques acteurs économiques français permettant de diriger vers eux un flux massif de jeunes formés, sans pour autant développer un modèle économique - nous n'allons pas nous transformer en agence d'intérim. Cette initiative aurait sans doute un impact beaucoup plus fort pour le tissu économique français que la construction de partenariats fondés sur des enjeux de financements. Mais un tel effort exige d'affirmer que l'Inria est avant tout un outil au service de la souveraineté numérique.

M. Franck Montaugé, président. - Comment l'Inria appréhende-t-il l'impact des technologies dites de « blockchain » ?

M. Bruno Sportisse. - Ce sujet suscite une grande attention, car il regroupe un très grand nombre de thématiques : sécurité numérique, cryptographie, systèmes distribués, articulation entre technologies numériques et monde du droit, etc.

À mon sens, un véritable écosystème français doit se constituer autour de la blockchain. La Caisse des dépôts et consignations a d'ores et déjà pris un certain nombre d'initiatives à propos des transactions. À présent, il faut consolider et regrouper les nombreux apports souhaitables en la matière et même travailler à l'échelle européenne.

M. Franck Montaugé, président. - La blockchain est souvent présentée comme une technique infalsifiable : peut-elle, ou non, être cassée ?

M. Bruno Sportisse. - Malgré les promesses, certains exemples internationaux ont déjà prouvé que la blockchain pouvait être mise en échec ; aussi, l'enjeu relève au premier chef de la sécurité numérique. Il s'agit d'un véritable sujet de maîtrise technologique et il faut, à cette fin, mobiliser les acteurs.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible en ligne sur le site du Sénat.

Audition de Mme Nicole Belloubet, ministre de la justice,
le 3 septembre 2019

M. Franck Montaugé, président. - Notre commission d'enquête poursuit ses travaux avec l'audition de Mme Nicole Belloubet, garde des sceaux, ministre de la justice. Cette audition sera diffusée en direct sur le site Internet du Sénat et fera l'objet d'un compte rendu publié. Je rappelle qu'un faux témoignage devant notre commission d'enquête serait passible des peines prévues aux articles 434-13, 434-14 et 434-15 du code pénal.

Conformément à la procédure applicable aux commissions d'enquête, Mme Nicole Belloubet prête serment.

M. Franck Montaugé, président. - Le développement du numérique voit s'affronter des États et des espaces continentaux sur le terrain de l'économie mais aussi du droit, utilisé comme un moyen de conquête et de protection. La confrontation des cultures et des systèmes juridiques dans le champ du numérique ainsi que le rapport de force qui en résulte affectent la souveraineté de notre État.

Notre droit national et continental place la loi au centre ; le droit anglo-saxon de *common law* procède d'une autre logique, sans cesse plus forte, jusqu'à donner l'impression que notre loi, sur notre propre sol, s'efface de fait.

Dans ce contexte, madame la Garde des sceaux, votre ministère doit répondre aux défis que représente la révolution numérique pour notre souveraineté, pour l'intégrité de notre ordre juridique et l'autorité de nos magistrats et de nos lois.

Les modèles économiques des grands acteurs du numérique - gratuité d'accès, collecte massive, utilisation et valorisation des données personnelles, vente de publicités ciblées - passent par des stratégies d'évitement permettant d'échapper aux contraintes de notre ordre juridique. Obtenir la coopération de grandes plateformes situées à l'étranger n'est pas toujours aisé. Quelles difficultés nos magistrats et vos services rencontrent-ils, et quelles solutions nous sont offertes ?

Pire, certains de ces acteurs sont susceptibles d'être en France les vecteurs, consentants ou non, d'ordres juridiques étrangers : les géants américains sont soumis à des régimes de sanctions extraterritoriales ou à des règles d'accès aux preuves électroniques, comme le *Cloud Act*. Comment s'explique ce contournement des traités d'assistance judiciaire mutuelle et comment l'éviter ? Faut-il renforcer la loi de blocage pour interdire, par exemple, la transmission d'informations stratégiques hors de ce cadre protecteur ?

Mme Nicole Belloubet, garde des sceaux. - Nous avons déjà abordé le sujet lors de l'examen, en 2017 et 2018, du projet de loi relatif à la

protection des données personnelles qui a permis de tirer les conséquences du règlement européen de protection des données (RGPD) et de la directive qui l'accompagnait. Mais la question de la souveraineté numérique telle que vous l'abordez est beaucoup plus vaste et embrasse des champs de réflexion et d'action qui dépassent la seule protection des données personnelles ainsi que le périmètre de compétence de mon ministère.

On compare parfois l'espace numérique à celui des océans. C'est en effet un espace de liberté, avec des îlots de souveraineté qui tentent de s'affirmer juridiquement. Comme jadis, on voit apparaître de grandes compagnies commerciales qui tirent des richesses considérables de cet espace à conquérir - d'autant qu'elles le créent elles-mêmes - et des corsaires ou pirates qui profitent de cette liberté et des faiblesses du droit. Le droit de la mer a été une lente construction au cours des siècles, au prix de conflits, de rivalités, mais aussi d'une coopération réelle entre les États. Il faut que notre droit de l'espace numérique se mette en place plus vite, car les enjeux sont considérables et nous n'avons pas le temps d'attendre.

L'expression de notre souveraineté dans cet espace de liberté est difficile. Les acteurs non étatiques sont puissants et protégés par les États où ils se sont développés, États-Unis ou Chine. Les intérêts privés et nationaux s'entremêlent. L'Europe doit composer avec ses propres difficultés à agir face à des acteurs qui peuvent faire preuve de cynisme tout en comprenant que l'Europe est un marché considérable à ménager. Les révolutions technologiques se succèdent, de plus, à un rythme si soutenu que le droit a du mal à s'adapter.

Défendre, voire reconquérir notre souveraineté numérique est un objectif que nous partageons. La notion de souveraineté recoupe d'ailleurs des notions diverses. Elle renvoie à notre capacité à défendre notre territoire et notre population, à préserver et développer nos intérêts. Elle suppose aussi que nous sachions faire respecter nos valeurs, c'est-à-dire la démocratie politique et l'État de droit, face aux risques liés au déploiement du numérique.

Pour reconquérir une souveraineté numérique, les États doivent d'abord répondre à des défis technologiques, ce qui suppose de développer une forte capacité d'innovation. Sans innovation technologique, nous serons déclassés, réduits à l'impuissance. L'exercice de la justice doit aussi s'appuyer sur ces innovations technologiques.

Mais nous devons aussi disposer des instruments juridiques qui nous permettent de protéger, d'agir et de sanctionner.

L'autre condition réside dans notre capacité à articuler souveraineté nationale et coopération internationale. Dans ce cadre, nous n'avons d'autre horizon qu'européen.

L'adoption du RGPD et sa mise en oeuvre par la loi du 20 juin 2018 relative à la protection des données personnelles illustrent la manière dont

nous pouvons agir pour préserver notre souveraineté numérique. Cela passe par une volonté résolue des États, une intégration européenne intense et une prise de conscience des acteurs eux-mêmes sur l'importance de protéger leurs données. II nous appartient de leur donner les outils pour exercer leurs droits de manière efficace contre les grands acteurs du numérique. En la matière, l'union fait la force.

Cette volonté de responsabiliser les acteurs s'est traduite par la nomination d'un délégué à la protection des données dans 53 000 organismes - soit 19 000 délégués au total, car la mutualisation est possible. Un tiers de ces organismes sont publics. Les collectivités territoriales se sont mobilisées : 11 800 communes, 82 départements, 12 régions ont nommé un délégué. Ce résultat est satisfaisant, car il s'agit d'une évolution lourde pour les acteurs. Ils jouent le jeu en dépit des craintes initiales ; la multiplication des délégués est le gage d'une diffusion massive de la culture de « protection des données ».

Les nouveaux outils offerts par la loi sont également utilisés par les citoyens. La loi du 20 juin 2018 a étendu l'obligation de notifier les violations de données à tous les acteurs qui recueillent des données personnelles, sous peine de sanctions très fortes - l'amende administrative pouvant être prononcée a été considérablement renforcée, j'y reviendrai. Au 27 juin 2019, 2 257 violations ont été notifiées en France. Ces violations auraient concerné plus de 95 millions de personnes - y compris bien sûr à l'étranger.

Le niveau de cybersécurité en France reste toutefois trop faible par rapport à l'Allemagne, au Royaume-Uni ou aux Pays-Bas. De nombreux organismes n'identifient pas les atteintes portées à la sécurité des données qu'ils traitent. Il faut donc continuer, avec la Commission nationale de l'informatique et des libertés (CNIL), ce travail d'information et de responsabilisation des acteurs.

La loi du 20 juin 2018 facilite aussi les plaintes auprès de la CNIL pour non-respect des dispositions relatives à la protection des données personnelles. Le nombre de plaintes a bondi en 2018, et on constate une hausse de 23 % au premier semestre 2019 par rapport à la même période en 2018, avant l'entrée en vigueur de la loi. Preuve que les particuliers hésitent de moins en moins à saisir la CNIL, et que la campagne de communication autour de la loi a été efficace. Au-delà des plaintes individuelles, la CNIL a également reçu cinq plaintes collectives, portées par l'association La Quadrature du Net, à l'encontre de Google, Apple, Facebook, Amazon et LinkedIn, réunissant près de 46 000 personnes.

Enfin, la loi du 20 juin 2018 a introduit une nouvelle sanction, avec une amende administrative pouvant désormais atteindre 20 millions d'euros ou 4% du chiffre d'affaires mondial, contre 3 millions d'euros auparavant, afin de peser sur les grands acteurs mondiaux. À ce jour, quatre sanctions ont été prononcées dont une, spectaculaire, de 50 millions d'euros contre

Google, le 21 janvier 2019, pour l'absence d'informations sur la finalité et la conservation des données des utilisateurs, l'exploitation massive et intrusive de celles-ci, ainsi que l'absence de consentement pour la personnalisation de la publicité. Il s'agit d'un montant record, auparavant, pour mémoire, une amende de 400 000 euros avait été infligée à la société Über fin 2018 sur la base de l'ancienne législation. Cette réforme marque bien un tournant dans notre rapport au numérique tout en créant un écosystème juridique global qui permettra à l'Europe de peser sur la scène internationale.

Face à ces enjeux, le ministère de la justice a dû s'organiser pour mieux maîtriser ses outils numériques, contrôler ses données et préserver la capacité du juge à rester maître de ses choix, de ses décisions, voire de ses valeurs dans une société numérisée. L'évolution vers plus de numérique est une nécessité pour le ministère de la justice d'autant plus qu'il a connu, en la matière, un retard regrettable.

Le plan de transformation numérique du ministère est à ce titre essentiel à l'action de la justice : il s'agit de la rendre plus lisible, plus accessible et plus démocratique, en l'ancrant toujours davantage dans le service du citoyen. Ce plan nous oblige à adapter notre socle technique, à développer des applications métiers pour les professionnels et les justiciables, et à construire des capacités d'accompagnement des utilisateurs. Ces sujets touchent au coeur de l'action des magistrats et jouent sur les perceptions de la justice, de son fonctionnement et de son efficacité, voire de sa légitimité.

Cette évolution majeure pose des questions de contrôle et de souveraineté. Les problématiques numériques modifient l'approche classique de traitement de l'information : elles intègrent des tiers externes d'importance grandissante dans le déploiement des infrastructures et des données. L'ère numérique globalise et crée de nouvelles dépendances. Il reste nécessaire de préserver les conditions d'exercice des libertés et les principes garantissant l'autonomie et l'indépendance des acteurs du droit et de la justice.

Ainsi, la justice doit veiller à la protection de son indépendance et des droits du justiciable en garantissant l'intégrité de ses données et la protection du secret. Dans ce cadre, il faut assurer l'intégrité et la traçabilité des informations, et préserver les traitements issus de ses systèmes d'information.

Par ailleurs, les moyens nécessaires à l'exploitation des plateformes numériques induisent une logique commerciale pour les développeurs, et des stratégies d'influence de toutes sortes qui peuvent être peu compatibles avec les logiques régaliennes et de souveraineté. Ces dispositions créent des opportunités permettant d'instrumentaliser des infrastructures ou de s'approprier des données éminemment souveraines. Il s'agit d'être vigilant sur les risques de glissement liés à ce changement d'environnement.

Je prendrai pour exemple la lutte contre la criminalité. La révolution numérique modifie profondément notre manière de mener cette action. Elle offre de nouveaux moyens de commission des infractions, favorisant même la création d'une criminalité spécifique, la cybercriminalité, qui n'existait pas auparavant. Elle entraîne, par ailleurs, une modification de notre rapport à l'application de la loi dans l'espace. Les lieux de commission de l'infraction ne peuvent plus être appréhendés de la même façon. L'accès aux preuves, lorsqu'elles sont numériques, nous invite également à modifier nos pratiques dans la mesure où elles ne peuvent pas être localisées et appréhendées comme le sont des objets matériels. Cette révolution favorise sans conteste une plus grande transnationalité des procédures. Notre ordre juridique interne est donc plus fréquemment confronté à ceux de nos voisins européens, ou au-delà, notamment quand il s'agit de collecter des preuves numériques.

C'est précisément afin de surmonter ces obstacles et de renforcer la coopération que l'Union s'est engagée dans d'importants travaux législatifs.

Tout d'abord, la Commission européenne a proposé deux textes, afin de faciliter l'accès aux preuves numériques entre États membres au sein de l'Union. Sont en cours de négociation une proposition de directive établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale et une proposition de règlement relative à l'accès aux preuves numériques en matière pénale, déterminant les conditions et modalités d'accès par les autorités judiciaires à la preuve numérique détenue par un opérateur fournissant des services sur le territoire de l'UE.

Le Conseil de l'Union européenne a arrêté sa position le 7 décembre 2018 sur la proposition de règlement, et le 7 mars 2019 sur la proposition de directive. Les discussions avec le Parlement ne pourront toutefois intervenir que dans le cadre de la nouvelle législature issue des élections de mai dernier, c'est-à-dire à compter de cet automne.

La France est très investie dans la négociation de ces deux textes et milite pour que ces derniers proposent des mécanismes simples pour les praticiens et efficaces pour les enquêtes judiciaires. Nous devons donc nous organiser pour mieux coopérer entre nous et faire en sorte que nos justices respectives demeurent efficaces face à une criminalité qui ne connaît plus les frontières. Mais nous devons aussi répondre aux défis que nous lancent les grandes puissances du numérique. Je pense en particulier aux États-Unis et au *Cloud Act*.

Le *Cloud Act* adopté en 2018 permet aux services d'enquête américains d'obtenir des données électroniques, y compris de contenu, quelle que soit leur localisation, auprès des opérateurs établis sur leur territoire. Il prévoit par ailleurs la conclusion d'accords bilatéraux permettant à des autorités étrangères de faire de même, excepté lorsque les données requises

appartiennent à des citoyens américains ou résidents permanents aux États-Unis, avec clause de réciprocité.

A priori, cela peut paraître être une avancée en matière d'enquête, mais le *Cloud Act* présente à mon sens plus d'inconvénients que d'avantages, notamment en multipliant les hypothèses de conflits de normes - particulièrement en matière de protection des données à caractère personnel - et en réduisant de fait les capacités d'enquête des autorités étrangères par un régime strictement encadré.

Le *Cloud Act* prévoit donc que la coopération n'est désormais possible qu'à condition qu'un accord ait été conclu avec les États-Unis. Or la clause de réciprocité qui devrait être contenue dans ces accords exécutifs pourrait être difficile à articuler avec le RGPD. En effet, les autorités pénales américaines pourraient requérir, auprès des opérateurs établis dans les États de l'Union, parties à ce type d'accord, la communication de données relatives à des citoyens ou résidents permanents d'autres États de l'Union que celui dans lequel l'opérateur est établi. À titre d'exemple, si la France concluait un tel accord exécutif avec les États-Unis, un hébergeur situé en Allemagne devrait, sur réquisitions des autorités américaines, fournir les données, y compris de contenu, relatives à des utilisateurs français. La conformité d'un tel accord à l'article 48 du RGPD n'est pas acquise.

En outre, on peut sérieusement être préoccupé par le fait que le *Cloud Act* permettrait à terme aux autorités judiciaires américaines d'accéder à des données, y compris de contenu, de personnes françaises, et donc, potentiellement d'entreprises françaises. Comment éviter cela ? Manifestement la réponse est européenne et l'Union s'est engagée dans la construction de cette réponse, qui n'est pas simple, car de nombreuses incertitudes ou incompréhensions demeurent.

Deux enjeux se font jour : préserver la capacité de nos magistrats à faire leur travail et protéger nos concitoyens contre l'accès illégitime à leurs données personnelles.

L'Union a décidé de s'engager dans la négociation d'un accord bilatéral sur le recueil de preuve numérique avec les États-Unis, car le *Cloud Act* peut mettre en échec les demandes des magistrats européens lorsqu'ils souhaitent obtenir des preuves numériques auprès des principaux fournisseurs mondiaux de communications électroniques. Cette négociation sera menée par la Commission au nom des Etats-membres. Ceux-ci sont néanmoins étroitement associés et la France a tout particulièrement veillé à ce que le mandat de négociation confié à la Commission le 6 juin dernier soit le plus exigeant possible.

Cette négociation prendra sans doute plusieurs années en raison d'une incompréhension avec les Américains : le *Cloud Act* prévoit la conclusion d'accords bilatéraux entre États ce qui est impossible légalement

côté européen puisqu'aux termes de la jurisprudence de la CJUE l'Union dispose d'une compétence externe exclusive en la matière.

Parmi les points importants de cette négociation, l'un des maîtres mots pour nous le terme « réciprocité ». Par ailleurs, nous avons insisté pour que les personnes morales soient expressément exclues de l'accord futur, afin d'éviter les risques d'intrusion ou de vampirisation des données stratégiques de nos entreprises sous un habillage judiciaire. Enfin, nous avons également pesé pour que soient écartées les données « dont la divulgation serait contraire aux intérêts essentiels d'un État membre ».

D'autres réflexions sont par ailleurs en cours pour peser face à certaines menées américaines. Je pense au renforcement de la protection de nos entreprises à travers la loi de blocage de 1968.

L'adoption récente du *Cloud Act* permet désormais aux autorités américaines, dans le cadre d'enquêtes pénales, de saisir de manière très simple et directe des données numériques pourtant hébergées à l'étranger, via les fournisseurs de services de communications électroniques américains ou situés aux États-Unis. *A contrario*, lorsque les autorités judiciaires françaises souhaitent saisir des données numériques hébergées aux États-Unis, elles doivent se plier au mécanisme beaucoup plus lourd et aléatoire de l'entraide judiciaire qui impose d'adresser une demande préalable aux autorités judiciaires américaines, lesquelles sont alors libres d'y donner suite ou non. Il y a donc là une situation d'asymétrie préjudiciable à notre souveraineté judicaire et numérique, plus particulièrement pour la confidentialité des informations stratégiques sensibles de nos entreprises lorsqu'elles sont stockées au format numérique.

Pour y faire face, le Gouvernement a amorcé une réflexion sur la base du rapport récemment remis par le député Raphaël Gauvain, afin d'actualiser la loi de 1968 dite de « blocage ». Pour mémoire, cette loi impose aux autorités administratives et judiciaires étrangères souhaitant se faire remettre des informations stratégiques détenues par des entreprises situées en France de passer par le canal de la coopération, c'est-à-dire de solliciter la communication de ces informations auprès des autorités nationales et non directement auprès des opérateurs économiques français visés. Le non-respect de la loi de blocage est sanctionné pénalement.

Certes, on pourrait considérer que la loi de 1968 s'applique d'ores et déjà à la transmission de données stratégiques numériques, relatives à des opérateurs économiques français, à des autorités ou entités étrangères. Mais le texte n'est pas explicite, ce qui pourrait faire peser un risque sur la légalité de la sanction pénale prévue, qui elle-même peut sembler insuffisante pour être considérée comme crédible et donc dissuasive pour les entités potentiellement concernées, les grands hébergeurs de données numériques, les Gafam notamment.

Cela dit, le Gouvernement envisage de consacrer un rôle spécifique dans l'avenir au service de l'information stratégique et de la sécurité économiques (Sisse) pour lui conférer un rôle d'accompagnement et de conseil des entreprises qui seraient concernées par des demandes étrangères directes visant à procéder à une saisie numérique. Le rôle du Sisse à cet égard pourrait notamment être d'évaluer la portée des informations confidentielles susceptibles d'être demandées par l'autorité étrangère, de rappeler à l'entreprise les dispositions de la loi de 1968 et d'engager un dialogue avec elle sur la conduite à tenir. Les réflexions sur ces différents aspects sont en cours d'étude et certaines d'entre elles pourraient faire l'objet de dispositions législatives.

Mesdames, messieurs les sénateurs, au travers ces premiers éléments, vous aurez compris que le Gouvernement et la Chancellerie accordent à la question qui vous occupe une très grande attention. Il faut en la matière avoir une pensée offensive et savoir promouvoir notre vision de la souveraineté numérique au sein de l'Union européenne. Nous nous y employons, mais vos travaux, j'en suis certaine, nous permettront de mieux faire valoir nos intérêts et contribueront à nous stimuler dans cette action essentielle.

M. Gérard Longuet, rapporteur. - Votre présentation reprend les lignes de force sur la souveraineté numérique que nous évoquons depuis le début de nos travaux, et rappelle votre implication dans l'adoption de la loi relative à la protection des données personnelles que vous aviez présentée au Sénat en 2018. Pour votre ministère, la souveraineté numérique appliquée à la coopération judiciaire est d'actualité et dépend non seulement de considérations économiques et technologiques, mais aussi juridiques.

Pour ce qui concerne la mise en place du RGPD, vous nous avez donné des éléments et cité des chiffres, mais je m'interroge sur la coexistence de sanctions administratives sur le fondement du RGPD et de poursuites pénales : quelle sera la politique du parquet pour sanctionner les manquements au RGPD ? Selon vous, quelle politique pénale devrait être adoptée par le Gouvernement ? Considérez-vous que la sanction administrative suffise ? Les amendes sont parfois élevées. Exonèrent-elles de la procédure pénale ? Il est facile de saisir les grands opérateurs qui défient les États ; il est possible de discuter avec des interlocuteurs qui ont des intérêts. Mais des opérateurs plus modestes peuvent échapper à ce type de régulation par la sanction administrative ; ils devraient être confrontés au risque de la sanction pénale si l'on veut qu'existe une dissuasion.

Pour ce qui concerne la CNIL, compte tenu de l'importance de l'enjeu, ses effectifs sont bien inférieurs à ceux des régulateurs des autres États membres de l'Union et elle paraît bien modeste. Il ne résulte pas de nos travaux qu'il faudrait fusionner les régulateurs, leurs compétences diverses - dès lors qu'il y a mutualisation et coordination - paraissant pertinentes. Pour autant, la question de l'insuffisance des moyens de la CNIL est préoccupante.

Le numérique a pour caractéristique d'être éternel, alors que les décisions de justice ont vocation à ne pas l'être. La prescription est un facteur de paix civique mais *l'open data* ne peut-il pas parfois servir à la contourner ?

Grâce à l'extension de l'intelligence artificielle, l'investissement dans des technologies algorithmiques pourrait aboutir à des méthodes d'aide à la décision, voire de prévisions qui feraient planer le spectre d'une justice prédictive à l'égard de petits délits dont le traitement pourrait être industrialisé. Cette crainte est-elle justifiée ?

Enfin, quel partenariat le ministère de la justice pourrait-il engager ou a-t-il engagé avec les Gafam ? Faut-il une attitude patriotique vis-à-vis des grands acteurs du numérique ou vaut-il mieux associer les grands acteurs à des coopérations ponctuelles ?

Mme Nicole Belloubet, garde des sceaux. - Pour ce qui concerne la coexistence de sanctions administratives et pénales, nous devons faire preuve d'exemplarité - c'est l'objet de la sanction pénale - et nous devons respecter des règles juridiques, notamment le principe *non bis in idem*. Le Conseil constitutionnel a rendu des décisions importantes - je pense notamment à sa jurisprudence lors de l'affaire Cahuzac - et admis sous certaines conditions deux types de sanctions pour des faits identiques qui relevaient de deux ordres juridiques différents. Dans le sujet qui nous occupe, tel est le cas et la double sanction pourrait donc jouer.

Quant à la CNIL, j'ai conscience de la modestie de ses effectifs, mais aussi de ses efforts considérables de réorganisation et d'adaptation. Des postes supplémentaires lui ont été octroyés pour faire face à ses nouvelles missions : entre 2010 et 2019, ses membres sont passés de 140 à 208. Son budget est passé de 14 à 18 millions d'euros. Le nombre des agents des structures comparables aux Pays-Bas et en Allemagne est similaire, tandis qu'au Royaume-Uni il atteint presque 700.

Sur la crainte d'une justice prédictive, il faut s'arc-bouter sur l'office même du juge et sur la question de l'individualisation des décisions qui garantit l'indépendance de la justice. Pour autant, il ne faut pas se priver d'éléments d'aide à la décision, tels les barèmes relatifs aux pensions alimentaires, notamment.

Par ailleurs, depuis la loi de 2016 pour une République numérique confortée par la loi de réforme de la justice de mars dernier, nous devons mettre à disposition en *open data* l'ensemble des décisions de justice, ce qui pourrait conduire des opérateurs privés à construire des banques de données ou des logiciels permettant de déterminer les chambres octroyant les meilleures indemnités. Lors de l'élaboration de cet *open data*, nous serons très vigilants sur ce point.

Enfin, aucun « partenariat » en tant que tel n'a été établi avec les Gafam, mais nous avons, bien sûr, un patrimoine applicatif qui s'est constitué au fur et à mesure - Microsoft, pour les postes de travail -, avec le

souci de la double source et des solutions alternatives libres. Pour des raisons de sécurité, nous hébergeons chez nous nos données, et avec le concours et la vigilance de l'Anssi.

Mme Catherine Morin-Desailly. - Lors de la dernière loi de finances, nous avons été surpris par la baisse des crédits. Or je veux insister sur la nécessité d'affecter des moyens adaptés aux autorités indépendantes, alors que la souveraineté est une question brûlante d'actualité. La présidente de la CNIL nous a fait part de ses besoins pour conduire sa mission difficile, de plus en plus pointue, avec l'entrée en vigueur du RGPD.

Cela dit, notre écosystème numérique s'est construit autour d'un système d'exploitation de nos données qui transitent par les plateformes devenues des « facilités essentielles » : nous dépendons d'elles. Eu égard à la manipulation d'informations au cours des derniers mois, quid d'une prise de décision quant à la réouverture de la directive e-commerce pour permettre de réfléchir à un statut des plateformes qui ne sont aujourd'hui redevables de rien ? Quid aussi des propositions de résolution européenne que nous adoptons et qui pourraient être des outils pour le Gouvernement... s'il s'en saisissait ?

Enfin, dans l'éducation nationale, des contractualisations sont intervenues avec Microsoft et Google. Quel est votre rôle, madame la Garde des sceaux, pour qu'à l'échelon interministériel s'opère une prise de conscience des risques de ces partenariats ? Je m'inquiète du mécénat et de l'aide au financement de la chaire d'enseignement de l'intelligence artificielle à Polytechnique. Ce sont des questions éminemment stratégiques.

Enfin qu'en est-il des contrats passés avec des entreprises telles que Cisco qui forment nos ingénieurs réseau dans l'ensemble des ministères où sont manipulées des données stratégiques ?

M. Franck Montaugé, président. - Vous avez parlé du rôle que vous entendez faire jouer au Sisse pour répondre au *Cloud act*. Allez-vous vous saisir aussi de la question de la protection des avis juridiques destinés à nos entreprises dont les autorités américaines peuvent parfois demander communication ? Envisagez-vous une évolution du statut des juristes d'entreprise ?

Mme Nicole Belloubet, garde des sceaux. - Madame Morin-Desailly, je soutiens les demandes de crédits de la présidente de la CNIL, qui sait aussi la nécessité de réorganiser cette instance en raison de l'évolution de ses missions.

Sur les risques pour la démocratie de la manipulation de l'information, la loi dite *fake new* permet d'apporter un certain nombre de réponses, ce qui montre une volonté d'agir. J'ai évoqué récemment ce sujet au Conseil de l'Europe et un certain nombre d'États sont intéressés par ce type de législation.

La directive e-commerce a été adoptée à une époque où les acteurs privés comme les Gafam n'existaient pas. Il est donc important de réfléchir à un nouvel encadrement, car les Gafam fournissent plus que de l'hébergement passif. La réouverture de ce dossier serait intéressante - je le dis, bien sûr, sans préempter le cadre de la nécessaire concertation interministérielle.

Quant aux propositions de résolution européenne adoptées par le Parlement, ces textes sont un point d'appui très utile dans nos négociations. Ils renforcent la position du gouvernement français.

Aucune contractualisation entre le ministère de la justice et les Gafam n'a été formalisée ; des partenariats ont été conclus notamment avec Microsoft. Je sais que mes collègues des autres ministères, tout comme moi, sont très mobilisés sur les risques qui pourraient découler d'une telle contractualisation.

Monsieur le président, le rapport Gauvain insiste sur la protection des avis juridiques possédés par certaines entreprises et souhaite que soit mis en place un certain nombre de dispositions. Les intérêts peuvent être antagonistes. Cette protection est favorable aux entreprises quand des autorités étrangères veulent accéder à des données constituant les gènes mêmes de ces entreprises. Mais des impératifs de valeur constitutionnelle existent. Ainsi en matière de détection de la fraude fiscale ou de lutte contre la délinquance financière, si ces données sont trop protégées, les juges français risquent d'être mis en difficulté. Nous devons donc trouver un système équilibré.

Une des réponses aux pouvoirs des autorités américaines serait, selon le rapport Gauvain, que nous nous dotions d'avocats en entreprise, en dégageant un statut particulier. Mais je note que la question fait débat et que les avocats français ne sont pas tous favorables à cette notion, estimant qu'une partie du marché pourrait leur échapper - c'est un fait, il y a des différences d'approche entre le barreau de Paris et les autres. Une des solutions à l'étude serait plutôt de permettre d'instaurer un *legal privilege* dont les titulaires pourraient être reconnus par les autorités judiciaires américaines, sans octroyer le titre d'avocat. Ils seraient inscrits au tableau B de l'ordre des avocats.

M. Laurent Lafon. - Nous avons compris la stratégie suivie en matière de coopération internationale. Je veux évoquer les pays hors Union européenne et États-Unis. Les cybercriminels ont perçu les faiblesses du système et vont se localiser dans des pays où les règles juridiques sont moins exigeantes. Le sentiment d'impuissance à leur égard est-il réel ? Quel est l'état des coopérations que vous pouvez mettre en oeuvre avec certains pays à l'Est de l'Europe, en Afrique ou au Moyen-Orient ?

Mme Nicole Belloubet, garde des sceaux. - La cybercriminalité nous a déjà obligés à évoluer. Ainsi, grâce à l'adoption de la dernière loi relative à

la justice, nos enquêteurs ont la possibilité d'infiltrer les réseaux. Nous avons également mis en place des parquets spécifiques gérant des dossiers spécifiques, comme celui de Pontoise qui gérera une base numérique particulière concernant les fraudes à la carte bleue, laquelle permettra une réelle efficacité. Des procédures d'enquête et des procédures judiciaires nouvelles sont donc mises en place. Dans le cadre de la proposition de loi de Mme la députée Avia relative à la cyberhaine, nous entendons mettre en oeuvre un parquet fléché sur ces questions.

Pour ma part, je ne parlerai pas d'impuissance, mais de rapidité d'adaptation. Au sein de l'Union européenne, la réactivité est réelle en raison des mécanismes de coopération extrêmement simples. Les textes relatifs à l'accès aux preuves numériques nous faciliteront la tâche.

M. Jérôme Bascher. - Aujourd'hui, la sanction correspond à une amende ou une peine de prison, alors qu'il faudrait peut-être en trouver d'autres comme - pourquoi pas ? - pirater l'identité numérique de hackers. Le ministère de la justice se met-il en capacité d'inventer de nouvelles réponses pénales ?

Mme Nicole Belloubet, garde des sceaux. - Je n'ai pas la réponse précise à votre question, monsieur le sénateur. Mais le ministère ne reste pas figé sur les sanctions classiques. Ainsi, l'Agence de gestion et de recouvrement des avoirs saisis et confisqués (Agrasc) est une autre réponse, infiniment plus efficace que la peine de prison ou d'amende. C'est un succès. L'effacement des contenus est une réponse, mais elle n'est pas toujours la plus optimale.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible en ligne sur le site du Sénat.

Audition de Mme Florence Parly, ministre des armées,
le 3 septembre 2019

M. Franck Montaugé, président. - Nous poursuivons nos travaux avec l'audition de Mme Florence Parly, ministre des armées. Cette audition sera diffusée en direct sur le site Internet du Sénat. Elle fera également l'objet d'un compte rendu publié. Je rappelle qu'un faux témoignage devant notre commission d'enquête serait passible des peines prévues aux articles 434-13, 434-14 et 434-15 du code pénal.

Conformément à la procédure applicable aux commissions d'enquête, Mme Florence Parly prête serment.

M. Franck Montaugé, président. - Vous avez la responsabilité d'un ministère régalien essentiel pour la souveraineté numérique. La revue stratégique de défense et de sécurité nationale de 2017 fait de notre souveraineté numérique un enjeu prioritaire et la revue stratégique de cyberdéfense de février 2018 définit la souveraineté numérique comme « la capacité de la France, d'une part, d'agir de manière souveraine dans l'espace numérique, en y conservant une capacité autonome d'appréciation, de décision et d'action, et, d'autre part, de préserver les composantes les plus traditionnelles de sa souveraineté vis-à-vis de menaces nouvelles tirant partie de la numérisation croissante de la société ».

Un pays ne peut être souverain s'il ne parvient pas à contrôler les activités numériques qui affectent son territoire et s'il ne dispose pas des technologies clés et des infrastructures critiques. Un pays ne peut pas non plus être souverain sans les armes lui permettant de garantir son autonomie et la maîtrise des théâtres opérationnels affectés par de nouvelles menaces numériques. Avons-nous aujourd'hui tous les moyens de nos ambitions dans tous ces domaines ?

Le 18 janvier 2019, notre pays s'est doté d'une doctrine militaire de lutte informatique offensive (LIO). La capacité à se protéger contre les attaques informatiques, à les détecter, à en identifier les auteurs est l'un des éléments clefs de notre souveraineté, mais elle ne pouvait se suffire à elle-même. N'avons-nous pas tardé à nous doter d'une capacité de riposter ? Nous sommes-nous donné la possibilité d'être suffisamment offensifs pour être dissuasifs ?

Mme Florence Parly, ministre des armées. - Vous avez déjà reçu de nombreux et éminents représentants du ministère des armées pour évoquer la souveraineté des outils numériques, les attaques cyber et les moyens humains et financiers qui y sont consacrés. Je compléterai leur éclairage, tracerai quelques perspectives et essaierai de cerner les enjeux à venir.

Je rappellerai certains constats : notre supériorité opérationnelle passe par la puissance numérique. Notre outil de défense repose en grande

partie sur l'exploitation de ce potentiel. L'information a toujours précédé l'action. Le numérique accélère et multiplie l'information. Plus aucune opération ne se fait sans recours au numérique. Pour repérer l'ennemi ou le terrain, agir avec précision ou optimiser les moyens, il faut des réseaux de capteurs et des capacités de modélisation numérique.

Le numérique, ce sont aussi des opportunités, pas encore toutes exploitées, mais immenses, comme l'intelligence artificielle et la capacité à traiter massivement des données. L'exercice de la souveraineté passe par l'aptitude à saisir ces opportunités.

Le numérique est partout dans notre quotidien. Le ministère des armées n'y échappe pas, que ce soit dans ses frégates, ses avions, ses blindés de plus en plus truffés de microprocesseurs, de puces ou de logiciels. Nos communications s'appuient sur des réseaux numérisés, transitant parfois par des opérateurs privés, que ce soit par des câbles ou des flux satellitaires... Cette exposition au numérique peut être pour le meilleur - puissance et opportunités opérationnelles - ou porteuse de risques - vulnérabilité et dépendance... En effet, le numérique, c'est aussi de la conflictualité : les attaques cyber ne sont pas l'apanage du secteur civil. Nos systèmes militaires sont épiés, visés, voire attaqués.

J'ai engagé une démarche de transformation numérique du ministère des armées avec ce souci constant de notre souveraineté. Pour orchestrer cela, j'ai créé la Direction générale du numérique, opérationnelle depuis juin 2018, connue et reconnue comme un acteur majeur aux niveaux ministériel et interministériel. Les enjeux de souveraineté sont au cœur de son action. Nous avons lancé la rénovation du socle numérique du ministère des armées pour tirer toutes les potentialités de la transformation numérique tout en renforçant la sécurité et la résilience. Pour cela, une nouvelle unité de management a été créée au sein de la Direction générale de l'armement (DGA) chargée de la conduite d'opérations d'armements, dont certains incluant les systèmes d'informations. Elle travaille étroitement avec la Direction interarmées des réseaux d'infrastructure et des systèmes d'informations de la défense (Dirisi), responsable des réseaux et de l'hébergement des données et des systèmes d'information du ministère des armées. Cette unité devra répondre aux enjeux de souveraineté, au même titre que les unités de management chargées des avions de combat ou des sous-marins. Systèmes d'information et numérique sont pris en compte en tant que tels.

Les données sont un sujet à part entière. Nous devons les acquérir, les stocker et les traiter en toute indépendance. Nous avons élaboré une stratégie cloud pour assurer la sécurité et la souveraineté de l'usage de nos données, sans nous priver des services de plus en plus vastes des opérateurs. Nous devrons faire émerger des opérateurs de confiance répondant aux besoins des administrations, des entreprises françaises et du ministère.

L'intelligence artificielle est un sujet majeur de préoccupation. Nous investissons massivement, 100 millions d'euros par an, sur ce défi technologique. Nous recruterons 200 experts - un véritable défi pour nos ressources humaines.

Le ministère des armées a largement contribué, par ses commandes et son soutien à la recherche, à l'excellence de la filière française sur les moyens de calcul de très haute performance. Vous avez auditionné les responsables des grandes entreprises qui y contribuent.

Concernant la sécurité d'approvisionnement des composants, nous travaillons avec le ministère de l'économie et des finances sur le plan Nano 2022, afin de créer une filière industrielle de confiance pour la conception et la réalisation des composants électroniques. La dépendance ne peut pas être un problème traité isolément par la défense, mais doit intégrer tous les acteurs industriels, et être envisagée à l'échelle européenne.

La souveraineté numérique doit garantir à la France sa capacité à agir de façon souveraine dans l'espace numérique, en conservant son autonomie d'appréciation, de décision et d'action. La revue stratégique de défense de 2017 rappelait que le cyberespace entraîne de nouvelles vulnérabilités, faisant de notre souveraineté numérique un enjeu prioritaire.

Nous avons constaté, fin 2017, des connexions anormales sur le serveur de messagerie internet du ministère des armées. Un attaquant cherchait à accéder directement au contenu des boîtes mails de 19 cadres du ministère, dont celles de personnalités extrêmement sensibles. Sans notre vigilance, toute la chaîne de l'alimentation en carburant de la marine nationale aurait été exposée. Cette tentative d'attaque a duré jusqu'en avril 2018. Nous avons pu remonter la chaîne des serveurs jusqu'aux adresses IP. Ce mode d'attaque est bien connu de nos services, et certains l'attribuent à Turla.

Tous les incidents, nombreux, ne sont pas forcément des attaques. Nous constatons en moyenne deux incidents par jour sur les réseaux du ministère des armées, mais le chef d'état-major des armées a constaté une forte croissance de ces incidents, d'environ 20 %, entre 2017 et 2018.

Le cyber est une arme d'espionnage, mais certains États l'utilisent pour déstabiliser, manipuler, entraver ou saboter. C'est vrai en temps de paix, mais surtout en temps de crise - comme actuellement dans le Golfe - ou de guerre. De plus en plus de nations intègrent la dimension cyber dans leurs stratégies ou leurs modes d'action, cumulant capacités conventionnelles et cyber. Ne soyons pas naïfs ! Ces constats fondent l'action de notre ministère, à pied d'oeuvre pour saisir les opportunités, prévenir les risques et réduire les fragilités.

Concernant les opportunités, le cyber est au coeur de la loi de programmation militaire (LPM). Les investissements humains et financiers permettent d'imposer la France comme un acteur incontournable :

1,6 milliard d'euros seront consacrés au cyber entre 2019 et 2025. Nous devons renforcer nos capacités de prévention, de détection et d'attribution des cyberattaques. D'ici à 2025, nous aurons 4 000 cybercombattants et cybercombattantes, soit 1 000 de plus qu'actuellement. Ces recrutements, très importants, concernent le développement des capacités cyber du ministère, et nous renforçons l'expertise en cyberdéfense de la DGA. Nous prenons en compte, aussi transversalement que possible, la sécurité à l'intérieur des programmes d'armement pour préserver la souveraineté numérique des armées.

Aux moyens de la LPM s'ajoute la consolidation de la stratégie de cyberdéfense, qui garantit la résilience numérique et l'aptitude au combat. En début d'année, nous avons énoncé une doctrine cyber avec une stratégie à la fois défensive et offensive. Défensivement, nous voulons mieux anticiper les menaces par le renseignement, détecter, réparer leurs effets, les caractériser, remonter jusqu'à leur source, et protéger les réseaux. Il faut repenser la résilience numérique en intégrant tous les enjeux du numérique. En 2017, nous avons créé le Comcyber, commandement de la cyberdéfense, dirigé alors par le général Olivier Bonnet de Paillerets. Ce commandement, qui a montré son utilité, est intégré dans la chaîne de commandement, et ses moyens seront renforcés par la future LPM.

En matière de cybersécurité, le ministère des armées prend ses responsabilités en lien très étroit avec l'Agence nationale de la sécurité des systèmes d'information (Anssi). Cela étant, ma conviction est que notre effort doit aller bien au-delà. Il doit être collectif pour être efficace. La cyberdéfense n'est pas qu'une affaire de spécialistes : elle relève de la responsabilité de tous et doit constituer une priorité pour tous nos agents. C'est l'esprit et l'objet de l'instruction que le ministère a diffusée en décembre dernier. C'est ce que nous appelons la « cyber-hygiène ».

C'est également l'esprit de la décision que j'ai prise en janvier de cette année d'organiser une chaîne cyberdéfensive de bout en bout, de Balard jusqu'à nos partenaires industriels et leurs sous-traitants. Cette démarche est bien avancée et se concrétisera prochainement par la signature d'une convention entre le ministère des armées et huit grands industriels de défense. Cette convention établira des objectifs partagés pour les premières actions concrètes engagées dans le domaine de la cybersécurité. Il est indispensable de renforcer les liens entre l'État et ses principaux maîtres d'oeuvre, de faciliter la concertation autour de l'évolution des moyens, et de préserver notre base industrielle et technologique de défense. Notre stratégie contribuera très directement à la préservation de notre souveraineté.

En 2019, l'actualité nous a rappelé que les groupes industriels peuvent eux aussi être l'objet de cyberattaques, ciblant non seulement les données personnelles de leurs employés, mais aussi la documentation technique des équipements que ceux-ci conçoivent. Je pense en particulier à l'attaque qui a visé l'un des sous-traitants d'un grand groupe, phénomène

qui montre l'importance d'un système assurant la sécurité de chaque chaînon de notre défense nationale. Il convient d'avoir une acception très large de cette chaîne : chaque entreprise, chaque partenaire du monde de la défense a ainsi un rôle à jouer en matière de souveraineté numérique.

Aujourd'hui, nos adversaires cherchent à exploiter toutes les failles qui se présentent pour nous atteindre, qu'elles se situent chez les industriels, leurs sous-traitants et fournisseurs, ou parmi leurs employés. Chaque système d'arme, chaque ordinateur ou smartphone, chaque objet connecté, peut être demain, à l'insu même de son propriétaire, non seulement une cible, mais également le vecteur de transmission d'une cyberattaque. C'est pourquoi nous prenons cette problématique extrêmement au sérieux.

Nous sommes également prêts à employer l'arme cyber en opération à des fins offensives, que ce soit de façon isolée ou en appui de nos moyens conventionnels, afin d'en démultiplier les effets. Une stratégie offensive est indispensable, car il faut préparer nos armées à cette nouvelle guerre, en nous assurant qu'elles disposent d'une doctrine et de capacités offensives dans le domaine informatique. C'est aussi cela la souveraineté à l'heure du numérique.

Ainsi, en cas d'attaque contre nos forces, nous nous réservons le droit de riposter, et ce dans le respect du droit, par les moyens et au moment que nous jugerons opportuns. Nous nous réservons aussi le droit de neutraliser les effets et les moyens numériques employés. Nous considérons l'arme cyber comme une arme opérationnelle à part entière. C'est un choix que nous faisons en responsabilité. Il faudra naturellement en faire un usage proportionné, mais nous n'aurons pas peur de l'utiliser.

J'aurai très prochainement l'occasion de présenter à nos partenaires notre vision du droit international appliqué aux cyberopérations. Le domaine juridique et normatif est en effet un aspect essentiel de l'exercice de notre souveraineté.

Je souhaite également aborder la question des coopérations. Leur champ ne se limite pas aux seules industries numériques et de défense. L'exercice de notre souveraineté dans le domaine numérique ne se conçoit qu'à travers le développement de coopérations internationales, tout particulièrement à l'échelon européen. Certains pourraient considérer qu'il existe une contradiction entre la notion de souveraineté numérique et celle de coopération. Il n'en est rien : c'est à travers des coopérations fortes que nous pourrons préserver notre souveraineté numérique. Celles-ci conditionnent en effet la préservation de nos expertises qui ne sauraient se maintenir si elles sont trop isolées et fragmentées. Elles conditionnent également la résilience de nos systèmes qui doivent disposer d'une certaine profondeur pour anticiper et réagir aux attaques.

Nous travaillons avec nos partenaires à la fois dans le domaine industriel pour garantir notre aptitude à développer les systèmes dont nos

armées ont besoin et auront besoin dans le futur, et dans le domaine militaire pour mutualiser nos compétences et nos expertises. Le Comcyber a été créé pour assurer la cohérence du modèle de cyberdéfense du ministère dans les domaines des ressources humaines, de la politique internationale ou pour des besoins techniques spécifiques. Cela étant, il développe lui-même des partenariats stratégiques que nos services de renseignements utilisent. Il s'agit là d'un défi majeur.

J'en terminerai par les quatre défis que mon ministère doit relever.

Le premier est celui de l'expertise. C'est à la Direction générale de l'armement de placer le numérique et la cybersécurité au coeur du processus d'acquisition, de développement et de qualification de nos systèmes d'armement. Il s'agit de prendre en compte cette nouvelle doctrine offensive le plus en amont possible pour concevoir et développer les armements de demain. Cet objectif ne peut être atteint sans la mise en place d'une véritable politique d'innovation numérique. L'Agence de l'innovation de défense travaille en lien très étroit avec la Direction générale du numérique pour développer des outils - en particulier dans le domaine de l'intelligence artificielle - et des méthodes managériales dédiés à l'innovation numérique. Il reviendra donc à la Direction générale du numérique de les diffuser, d'en contrôler la mise en oeuvre et de les adapter.

Le deuxième défi est celui de l'acculturation de nos militaires et de nos personnels civils à cette nouvelle arme spécifique. Je ne développerai pas ce point, car je sais que le chef d'état-major des armées l'a déjà fait devant vous. J'insisterai simplement sur l'initiative des combattantes du numérique, les Combattantes@Numérique, démarche très intéressante, qui a été lancée en septembre 2018 et que je suis de près. Ce réseau vise à encourager les femmes à s'approprier les compétences du numérique et à les attirer dans les industries du numérique. Le ministère prend une part très importante dans ce projet. Près de 70 femmes issues des filières du numérique travaillent à faire changer les représentations.

Le troisième défi a trait à la coopération avec nos partenaires internationaux. Nous devons continuer à nous tourner vers nos alliés. Comme dans le désert, les océans, l'air et l'espace, nous ne pouvons laisser aux agresseurs le monopole de l'avantage d'évoluer dans un espace sans frontières : il n'y a pas de cyberdéfense sans alliance, et il n'y a pas d'alliance sans partenaires de confiance. Aujourd'hui, toutes les attaques ont une ampleur internationale. L'OTAN, par exemple, met en oeuvre des coopérations et des exercices en matière de cybersécurité. Nous avons ainsi gagné un défi lancé par cette organisation en avril dernier.

Les cybermenaces pèsent sur tous les pays du continent européen. Nous avons donc intérêt à unir nos efforts plutôt qu'à combattre en ordre dispersé. L'union fait la force : je n'imagine pas l'Europe de la défense sans un volet « cyberdéfense ». De ce point de vue, la création du fonds européen

de défense, dont nous attendons beaucoup, devrait représenter un premier pas. Nous serons pleinement engagés dans la promotion d'initiatives en matière de cyberdéfense à l'échelon européen, notamment au travers de la création de clusters permettant d'associer dans un même pôle des chercheurs, des industriels et des entrepreneurs.

Enfin, il revient au ministère de fiabiliser nos filières d'approvisionnement dans le domaine des composants, et de le faire en lien avec les acteurs civils, là encore au niveau européen. Nous avons identifié des partenaires comme l'Estonie, l'Espagne ou le Danemark avec lesquels il est indispensable de développer notre connaissance de la menace et de nous entraîner. L'exemple de l'Estonie est intéressant : ce pays, comme vous le savez, a fait l'objet d'attaques importantes il y a quelques années et a alors su réagir avec fermeté.

Le quatrième défi, probablement le plus difficile à relever, est celui des ressources humaines. Dans ce domaine, notre politique se veut ambitieuse et attractive. Certaines personnes auditionnées ont évoqué la rigidité des procédures de recrutement et le problème du niveau des rémunérations. Je souhaite au contraire insister sur les facilités nouvelles qu'un certain nombre d'outils nous offrent : je pense en particulier à la loi de transformation de la fonction publique.

Par ailleurs, la question des rémunérations est moins problématique que l'on pourrait le croire lorsqu'il est question de recruter des jeunes en début de carrière. Nous sommes en réalité parfaitement capables d'attirer de jeunes talents. Au fond, le vrai défi qui se présente à nous est celui de les fidéliser. D'ailleurs, l'enjeu est certainement davantage de déterminer la durée de l'engagement que nous leur proposons que de parvenir à les recruter. Il faut à la fois être capable d'attirer sans cesse de nouveaux talents et d'assurer un turnover permanent.

Nous sommes conscients que la cyberdéfense nécessite des compétences de haut niveau, et que celles-ci sont très rares et très disputées. Le métier de combattant du numérique est très récent : il nous revient donc de développer cette filière. Malgré un univers extrêmement compétitif, nous sommes satisfaits de constater que les jeunes montrent une réelle envie de nous rejoindre. L'attractivité du drapeau n'est pas forcément un vain mot.

Aujourd'hui, il ne faut fermer aucune porte et il faut envisager des filières de formation, d'entraînement et de recrutement nouvelles. Dans cette bataille pour l'innovation et la sécurité numérique, chacun doit être mobilisé, depuis nos combattants numériques, qui sont de plus en plus nombreux, jusqu'aux étudiants, depuis les PME jusqu'aux soldats de notre réserve cyber qui, loin d'être occasionnelle, est utilisée quotidiennement.

M. Gérard Longuet, rapporteur. - Le sujet est absolument passionnant, madame la ministre. Nous savons combien votre ministère s'implique pour préserver la souveraineté numérique de notre pays. Lors de

précédentes auditions, nous avons pu nous familiariser avec la politique que vous défendez, en particulier l'affirmation d'une stratégie offensive en matière de cybersécurité. Face aux défis à relever, j'ai deux préoccupations.

La première concerne la dimension économique du monde numérique. La France, que nous le voulions ou non, est un acteur important, mais minoritaire dans ce secteur. En effet, la majeure partie des investissements est aujourd'hui contrôlée par des acteurs extérieurs.

Je prendrai l'exemple du plan Nano 2022. Il s'agit d'un rendez-vous extraordinairement important. Seulement, les entreprises les plus importantes ne sont pas françaises et les débouchés de l'industrie commandent souvent, hélas, la réussite de ceux qui, en amont, conçoivent et imaginent les systèmes. Selon vous, peut-on maintenir un haut niveau de qualifications technologiques et scientifiques en France, alors que les acteurs nationaux n'auraient pas atteint une taille suffisante ? La question se pose aussi en matière de ressources humaines.

Nous avons réussi à maintenir une autonomie assez forte de nos industries de défense dans la plupart des domaines stratégiques, notamment grâce à la politique de dissuasion. Toutefois, le secteur du numérique étant profondément dual, le chiffre d'affaires des grands acteurs ne risque-t-il pas de marginaliser nos industriels au regard de leur place sur le marché ?

En matière de ressources humaines, a-t-on tenté de freiner le *brain drain*, notamment en s'intéressant aux expériences de pays plus petits qui ont mieux réussi que nous à mobiliser leurs effectifs ? Je suis étonné par exemple des résultats industriels d'Israël en matière de défense, malgré sa population réduite.

Mon second sujet concerne spécifiquement les conflits, tensions ou offensives cyber. Notre lutte informatique est bonne, mais le problème de l'identification de la menace se pose. En matière de défense, à la différence du domaine judiciaire, on ne peut pas se baser sur une forte présomption ; il faut travailler sur des faits établis. Cette difficulté d'identification tend à protéger nos adversaires et, en la matière, nous ne pouvons pas vraiment compter sur nos amis, en dépit des accords de coopération. Nos voisins n'hésiteront en effet jamais à nous « faire les poches »...

Votre bataille pour faire évoluer le droit international me semble donc indispensable, madame la ministre. Vous avez cité trois pays européens sérieux avec lesquels on peut travailler. Vous avez en revanche écarté trois grands pays, l'Italie, le Royaume-Uni et l'Allemagne, qui disposent pourtant d'une industrie de la défense et jouent un rôle significatif. Si nous n'arrivons pas à nous accorder avec eux et à jouer le jeu de la transparence, il sera difficile d'agir au plan international. En effet, une guerre contre un adversaire que l'on ne parvient pas à identifier ou que l'on identifie sans pouvoir le responsabiliser pour son acte est difficile à conduire.

Ces questions ne sont sans doute pas très concrètes, mais elles sont au coeur de ce problème majeur qu'est la souveraineté numérique. Il est assez facile de défendre un territoire délimité par des frontières, beaucoup moins de défendre un espace numérique traversé en permanence de part en part.

À quel moment la fréquentation non souhaitée de cet espace justifie-t-elle une réaction excédant le simple cadre numérique pour devenir politique ou militaire ? La question reste ouverte.

Mme Florence Parly, ministre. - Le défi numérique est mondial, c'est une évidence, et nous ne pouvons pas éluder la réalité des rapports de force entre grands groupes industriels.

Nous ne sommes toutefois pas complètement démunis. Y compris dans ses périodes budgétaires les plus sombres, la France a toujours préservé sa capacité d'investissement, ce dont nous devons nous réjouir. On peut certes regretter l'abandon ou le ralentissement de certains projets, mais nous sommes l'un des seuls pays européens à avoir soutenu notre effort de défense.

Par ailleurs, comme vous l'avez mentionné, monsieur le rapporteur, la préservation de la dissuasion nucléaire sert d'aiguillon puissant pour maintenir et faire progresser certaines de nos capacités. En renonçant aux essais nucléaires et en développant un programme de simulation, nous avons ainsi pu préserver nos capacités de recherche et de développement dans le domaine des supercalculateurs. Nous ne couvrons sans doute pas tous les domaines, mais notre pays a consenti un effort considérable pour préserver son effort d'investissement contre vents et marées. Nous disposons aujourd'hui de groupes industriels de défense de taille significative.

Il en va différemment dans le domaine du numérique *stricto sensu*. Toutefois, les entreprises de ce secteur répondent avant tout à des besoins et des usages civils, les utilisations potentiellement militaires des capacités numériques qu'elles développent étant essentiellement indirectes.

M. Gérard Longuet, rapporteur. - Les données de masse concernant les individus, en particulier leur géolocalisation, sont-elles utilisées à des fins militaires, en particulier pour identifier des mouvements de population ?

Mme Florence Parly, ministre. - On ne peut pas garantir que certains pays n'utilisent pas à des fins militaires des données individuelles. Je ne citerai aucun nom dans le cadre de cette audition publique, mais vous aurez sans doute deviné... Le risque existe, incontestablement.

Je relèverai aussi le rôle très important joué par le groupe Thales pour notre souveraineté numérique, l'acquisition stratégique majeure qu'il a récemment réalisée le confirmant. Les investissements réalisés par le groupe Orange y contribuent également.

Le combat militaire de demain sera de plus en plus connecté. D'ores et déjà, nos équipements militaires sont constitués de nombreux capteurs et logiciels, mais cette réalité sera multipliée par un facteur 50 ou 100 à l'avenir. Ainsi, les caractéristiques principales du programme d'équipements terrestres de nouvelle génération Scorpion ne résident pas tant dans le blindage et la maniabilité physique des véhicules que dans leur capacité à transmettre des flux de données en temps réel aux équipements avec lesquels ils interagiront. Nous pouvons mentionner également le système de combat aérien du futur, qui fait actuellement l'objet d'études.

Intégrer dans les équipements cette capacité d'échange de données avec des partenaires externes, c'est vraiment le défi technologique de demain pour nos armées. Il nous faudra non seulement concevoir des matériels furtifs et rapides qui volent, naviguent et roulent, mais aussi être capables d'aménager cette connectivité en toute sécurité, c'est-à-dire en la protégeant des interactions extérieures.

Je ne réponds pas directement à votre question sur le dimensionnement de nos capacités industrielles, monsieur le rapporteur, mais je peux en revanche vous dire que nous mobilisons tous les moyens dont nous disposons, dans mon ministère ou en dehors - Bruno Le Maire vous parlera plus doctement que moi du plan Nano.

S'agissant des moyens propres au ministère des armées, la loi de programmation militaire a fait du renseignement et du cyber ses deux axes prioritaires. On peut naturellement discuter de l'ampleur de l'effort consenti et de sa pertinence, mais il n'y a aucune naïveté de notre part, nous sommes parfaitement conscients de l'importance de l'enjeu.

Quant au défi des ressources humaines, nous sommes conscients qu'après avoir été attirés vers la finance, nos meilleurs cerveaux sont fortement attirés par toutes ces entreprises qui, pour beaucoup d'entre elles, se situent à l'ouest du continent américain.

Pour réagir, ne sous-estimons pas les potentialités de la loi de transformation de la fonction publique, qui assouplit considérablement les possibilités de recrutement de contractuels et leur offre une nouvelle grille de rémunération, plus en phase avec le marché de l'emploi. Le ciblage féminin n'est pas non plus un gadget, car, dans ce domaine-là également, nous ne pouvons pas nous priver de la moitié du vivier de talents.

Enfin, la réserve cyber comprend presque une centaine d'hyper-spécialistes et d'experts de leur domaine. Il s'agit de salariés d'entreprises du secteur privé qui mettent quotidiennement leurs compétences au service de nos armées.

Nous devons développer l'ensemble de ces politiques. La prise de conscience est réelle. Il nous reste maintenant à faire le meilleur usage possible des nouveaux outils à notre disposition. Avant de dire que nous ne

faisons pas assez, nous devons d'abord apporter la démonstration que nous avons poussé jusqu'au bout l'utilisation des outils existants.

Israël constitue en effet un exemple d'un petit pays extrêmement actif et performant ; l'Estonie également a développé des filières de formation très performantes et produit un grand nombre d'ingénieurs cyber en proportion de l'importance de sa population.

M. Gérard Longuet, rapporteur. - Il faut dire que ce petit pays a des voisins assez encombrants et inquiétants !

Mme Florence Parly, ministre. - L'identification de la menace est un sujet très sensible. Dans ce domaine, nous souhaitons exercer pleinement notre souveraineté. Nous ne souhaitons pas que les attaques soient dénoncées par tel ou tel pays ou organisation, car cela doit rester une décision souveraine de l'État.

M. Gérard Longuet, rapporteur. - Ce que vous dites est extrêmement important !

Mme Florence Parly, ministre. - Le Président de la République y est très attaché. Il y va de notre diplomatie : nous pouvons avoir intérêt à dire ou ne pas dire, et c'est à nous de décider de la nécessité de communiquer nos informations.

Dans la mesure où nos partenariats sont de confiance, ils sont forcément sélectifs. La liste que j'ai présentée n'est pas exclusive, et nous avons de nombreux partenariats avec l'Allemagne, le Royaume-Uni, mais aussi les États-Unis.

Le sujet est encore en devenir. Nous avons pris la mesure des défis et nous n'entretenons aucune naïveté. Voilà pourquoi nous avons souhaité clairement énoncer que le cyber pouvait être une arme à part entière. Pour autant, tout ne doit pas être public.

M. Pierre Ouzoulias. - Le général Lecointre, chef d'état-major des armées, et le général Bonnet de Paillerets nous ont dit que la maîtrise des codes sources était essentielle en matière de souveraineté. Votre ministère est lié à Microsoft par un partenariat de longue date. Des militaires qui ne sont pas sous votre tutelle, comme les gendarmes, ont réussi à se passer des Gafam pour mettre en place des logiciels libres. Le partenariat avec Microsoft s'achève en 2021. Intégrerez-vous le critère de la maîtrise des codes sources dans le futur appel d'offres ?

M. Rachel Mazuir. - J'ai été ravi de constater l'importance que vous accordez au personnel. Selon Guillaume Poupard, seulement 60 % des places de nos écoles de formation sont remplies. C'est un problème majeur. Quant à fidéliser les étudiants que l'armée intègre, cela prend du temps. Or souvent l'armée est un passage intéressant, mais où l'on ne s'éternise pas.

La 5G complique la situation en ce qui concerne les acteurs de confiance. Quand on est en Opex, comment cela se passe-t-il ? A-t-on développé des méthodes pour sécuriser les opérations ?

M. Jérôme Bascher. - Vous avez mentionné la nécessité d'une acculturation. Dans cette perspective, tous les agents de votre ministère doivent être bien conscients qu'ils sont tracés. Je vois que vos collaborateurs se déplacent avec leurs deux téléphones, l'un personnel, l'autre crypté...

Un certain nombre d'armes connectées peuvent faire feu automatiquement, ce qui pose un problème de droit, car il est nécessaire de pouvoir identifier d'où viennent la prise de décision et l'ordre de tir.

Autre question : qu'est-ce qu'une cyberguerre ? Vous avez annoncé que vous feriez des propositions sur ce sujet : quelles sont vos premières pistes ?

Enfin, version dégradée de cette dernière question : la cyberattaque offensive s'exercera-t-elle sous le radar du droit, à l'image de ce que font nos forces spéciales, ou bien fera-t-elle partie d'une échelle de graduation de la guerre, entre le conventionnel et la dissuasion nucléaire, par exemple ?

M. Laurent Lafon. - Je vous transmets une question de notre collègue Catherine Morin-Desailly qui n'a pu être présente à cette réunion. La société Palantir a été financée par des fonds d'investissement liés à la CIA. Elle bénéficie d'une avance technologique en matière de traitement des données. Elle mène une politique volontaire d'entrisme, qu'il s'agisse de la commande publique ou du recrutement. Les liens qu'elle a noués avec X-Forum portent leurs fruits puisque de jeunes polytechniciens viennent d'être recrutés.

Mme Florence Parly, ministre. - Ce n'est pas devant le rapporteur de cette commission d'enquête que je rappellerai l'origine du partenariat avec Microsoft. Le ministère des armées disposait de très nombreuses licences éparses avec Microsoft. Nous avons souhaité rationaliser cette situation qui nous exposait à moult difficultés. La démarche a été raisonnée : mon ministère a souhaité inscrire des règles de fonctionnement sur la bonne utilisation de ces licences. Tel a été l'objet du contrat que nous avons passé avec Microsoft.

Quant à savoir si cette situation a vocation à perdurer, c'est une question légitime. Depuis la signature du contrat, des logiciels libres se sont développés. Cependant, nous devons sans cesse ménager l'interopérabilité de nos forces. Nos alliés fonctionnent à partir de codes sources qui proviennent de la même entreprise, ce qui constitue une difficulté et ralentit le développement du recours aux logiciels libres.

Quant à la fidélisation des étudiants, nous cherchons à nous assurer pendant 5 ans la collaboration de ces jeunes gens. Imposer une durée plus longue serait contreproductif. À l'échelle des évolutions technologiques très

rapides, 5 ans plus tard, les étudiants qui sortent des cursus de formation ont acquis des qualifications et expertises nouvelles. Nous rémunérons donc des étudiants et leur garantissons une embauche contre cet engagement à servir et nous envisageons de faire de même vis-à-vis des personnels civils.

En opération extérieure, nous devons maintenir un flux de communications et pour ce faire disposons de systèmes de communication propres. Dans le cadre de la loi de programmation militaire, nous avons prévu le renouvellement de l'ensemble de nos capacités satellitaires. Le programme Syracuse 4 doit nous permettre de disposer des capacités d'échanges et de flux de données encore plus importantes qu'actuellement. Nous devons lancer deux satellites en 2020 et 2021 et notre système devrait être entièrement renouvelé. Nous ne sommes donc pas tributaires des opérateurs de télécommunications.

Pour ce qui concerne le droit, la question est vaste et va au-delà du cyber. Sont posées les questions des robots, de la place de l'homme dans leur intervention et face au développement de l'intelligence artificielle qui équipera un certain nombre de nos armes. Nous avons décidé de créer un comité ministériel d'éthique, car nous devons avoir une doctrine claire sur des sujets complexes.

Lors de mon annonce de l'utilisation prochaine de drones armés, j'ai rappelé le socle de notre doctrine : à aucun moment le recours à une arme ne doit être automatique ; un humain doit toujours être dans la boucle. Dans ce cas de figure, celui qui appuiera sur le bouton sera sur le théâtre d'opérations et sera intégré aux équipages qui recourent à d'autres moyens aéronautiques. C'est fondamental dans la manière de concevoir l'utilisation de ces armes.

Il en va de même pour les robots : celui qui actionnera l'arme ne sera pas le robot. En matière d'intelligence artificielle, nous devrons veiller à ce que les algorithmes ne puissent pas prendre le pas sur l'humain. Mieux vaut soulever ces défis majeurs dès le départ pour se donner une chance d'y répondre de façon satisfaisante. Nous voulons avoir la main sur ces choix fondamentaux.

M. Rachel Mazuir. **-** Merci, madame la ministre, d'avoir répondu à la question de savoir comment les robots terrestres vont interagir : ils ne tireront pas depuis Balard.

Mme Florence Parly, ministre des armées. - Et d'autant moins que ceux que nous expérimentons ne sont pas armés.

M. Rachel Mazuir. **-** Mais ils peuvent l'être !

Mme Florence Parly, ministre des armées. - Le robot peut être très utile dans de nombreux cas sans être armé. Nous avons présenté un robot mule pour aider au transport de charges, à l'évacuation de blessés. Mais la question se posera et il vaut mieux y avoir réfléchi. Le comité ministériel d'éthique devra nous y aider.

Sur l'évolution du droit international, nous partagerons avec vous nos travaux conduits avec différents groupes de travail de l'ONU. Nous avons travaillé sur les thèmes suivants : le droit de répondre à toute cyberopération constitutive d'une violation du droit international ; une cyberopération peut constituer une agression armée justifiant l'usage de la légitime défense ; l'attribution d'une cyberopération d'origine étatique relève d'une décision de politique nationale.

L'entreprise Palantir fournit des services utilisés par certains ministères ou services de l'État faute d'alternative souveraine. Notre défi est de développer des solutions de confiance. Le programme Artemis (Architecture de traitement et d'exploitation massive de l'information multi-source) lancé par la DGA sera doté de 60 millions d'euros. Il a pour objectif de trouver une solution souveraine de traitement massif de données pour le ministère des armées à travers un partenariat innovant, avec Thales, Sopra-Steria, Atos et Capgemini, qui a démarré en 2017. L'industrialisation devrait commencer en 2022. Mais ce n'est pas le ministère des armées seul qui pourra assurer le financement de solutions dont notre pays, comme d'autres membres de l'Union européenne, a besoin. Nous ne pouvons pas être dépendants d'un unique fournisseur de services.

Enfin, le partenariat développé par l'école Polytechnique n'est pas sous notre radar.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible en ligne sur le site du Sénat.

Audition de MM. Julien Groues, directeur général et stéphan Hadinger, directeur technique pour Amazon Web services, le 3 septembre 2019

M. Franck Montaugé, président. - Mes chers collègues, notre commission d'enquête poursuit ses travaux avec l'audition des représentants de l'entreprise *Amazon Web Services France*, M. Julien Groues, directeur général, et Stéphan Hadinger, directeur technique.

Cette audition est diffusée en direct sur le site Internet du Sénat. Elle fera également l'objet d'un compte rendu publié.

Je rappelle, pour la forme, qu'un faux témoignage devant notre commission d'enquête serait passible des peines de prison prévues aux articles 434-13, 434-14 et 434-15 du code pénal.

Conformément à la procédure applicable aux commissions d'enquête, MM. Julien Groues et Stéphan Hadinger prêtent serment.

M. Franck Montaugé, président. - Nous connaissons tous les activités d'Amazon, du site de vente en ligne à la place de marché et la logistique en passant par le Cloud, la distribution physique, les assistants vocaux, la maison connectée, la musique, le cinéma, le textile, la reconnaissance faciale, le micro-travail avec *Amazon Mechanical Turk* ... et même le développement de lanceurs spatiaux, même si cette activité est portée par une entreprise bien distincte d'Amazon. C'est pourquoi je vous invite avant tout à répondre aux questions que nous avons à vous poser ! Je commencerai par deux questions relatives aux données.

Le Cloud Act permet aux autorités américaines de disposer des données que vous stockez, quel que soit le lieu de stockage. Cela inquiète légitimement les pouvoirs publics français, car sont concernées tant les données personnelles que les données stratégiques des entreprises, qui peuvent ainsi être pillées. Or de nombreuses entreprises françaises vous confient leurs données en utilisant vos solutions de cloud.

Pouvez-vous nous assurer qu'Amazon, ou ses filiales, ne permet pas et ne permettra pas aux autorités américaines de prendre connaissance des données de nos concitoyens et de nos entreprises ? Comment comptez-vous concilier ces obligations avec les règles européennes protégeant les données personnelles, le RGPD ?

Par ailleurs, en avril dernier, la presse a rendu public le fait qu'Amazon collecte, à travers l'assistant Alexa, les conversations de ses utilisateurs à leur insu. Surtout, les données enregistrées sont transmises à des centres d'écoute où des humains les analysent, afin d'améliorer les performances de reconnaissance vocale. Certains employés de ces centres auraient confié avoir été témoins de moments intimes, criminels, voire des deux. Or cette information n'a jamais été clairement communiquée aux

consommateurs et on peut légitimement penser que nombre de ceux-ci n'auraient pas acheté votre enceinte connectée s'ils avaient su qu'ils pouvaient être écoutés par des humains.

Cet été, une autorité allemande de protection des données a ordonné à Google de mettre un terme à cette pratique. Dans la foulée, Apple a annoncé une suspension temporaire de cette pratique, le temps de permettre à ses clients de choisir d'y participer ou non. Quid d'Amazon ? Pourquoi ne pas avoir été plus clair avec les utilisateurs ? Plus généralement, quelle est votre politique de protection des données à caractère personnel ?

M. Julien Groues, directeur général d'*Amazon Web Services France*. - Je vous remercie de votre invitation. Ces deux questions d'introduction vont me permettre d'apporter un certain nombre d'éclaircissements. Il s'agit de sujets extrêmement importants et complexes, qui méritent le temps de la réflexion et de l'échange.

Avant d'y répondre et d'aborder le sujet de la souveraineté numérique, qui nous amène ici, je voudrais revenir sur les activités d'*Amazon Web Services* que nous représentons aujourd'hui - j'utiliserai l'acronyme AWS pour plus de simplicité -, et sur notre approche de la sécurité et la confidentialité.

AWS, au sein du groupe Amazon, est une entité séparée du reste des activités de distribution et de détaillant d'Amazon.com et d'Amazon.fr. Le groupe Amazon.com a ouvert ses portes virtuelles en 1995 et, comme toute entreprise, a eu des besoins grandissants en matière d'informatique, d'infrastructures pour gérer une base de clientèle de plus en plus large, avec des besoins de création d'applications et de mise à disposition de ces applications à un nombre croissant de clients à travers le monde.

Après une décennie où ont été créées ces infrastructures informatiques, nous nous sommes rendu compte que nous avions de réelles compétences dans la création d'applications modernes, sécurisées et rapides, d'une part, et en matière d'opération de centres de données de taille importante, d'autre part.

Depuis environ 13 ans aujourd'hui, c'est-à-dire depuis 2006, où nous avons lancé les premiers services d'AWS, nous proposons des solutions cloud à nos clients. Nous avons désormais une nouvelle mission, qui est d'accompagner les développeurs et les entreprises dans leur utilisation de plateformes webs afin de leur permettre de créer leurs propres applications sécurisées et performantes. Concrètement, nous proposons aujourd'hui 165 services à la demande, que les entreprises et les développeurs peuvent utiliser. Il s'agit principalement de puissance de calcul de stockage, d'intelligence artificielle, avec la reconnaissance faciale, la sécurité, l'Internet des objets, etc.

Nous avons des centres de données dans 22 régions dans le monde, notamment en Europe, aux États-Unis, au Brésil, au Japon et en Afrique du

Sud, de sorte que nous pouvons servir nos clients à peu près partout sur la planète. Depuis 2017, nous avons ouvert une « région » en France. Constitue une région, pour AWS, trois zones de disponibilité, chacune disposant au moins d'un centre de données, ce qui nous permet d'offrir des services dans la région de Paris à nos clients, mais aussi à nos clients étrangers qui souhaitent héberger leurs données sur le territoire français.

Il s'agit d'investissements importants, comme vous pouvez l'imaginer, mais qui permettent à nos clients d'avoir des applications extrêmement rapides en France, et aussi, pour ceux qui le souhaitent, de pouvoir héberger leurs données sur le territoire français.

AWS a des millions de clients dans plus de 190 pays aujourd'hui. Cela va des multinationales aux petites entreprises, des universités aux hôpitaux, des agences d'État aux sociétés pharmaceutiques, mais il y a aussi Amazon.com, le détaillant.

On peut dire que nos clients utilisent les services d'AWS pour réinventer l'expérience de leurs propres clients. Cela se voit aujourd'hui dans le divertissement, dans l'hôtellerie, dans le luxe, dans les jeux vidéo. Des organismes privés et publics utilisent les services d'AWS pour améliorer la vie de nos concitoyens. Ainsi, le centre de recherche contre le cancer de Londres utilise la puissance du cloud AWS pour calculer en quelques minutes les dosages des traitements, ce qui améliore la vie des patients. De même, l'organisation Thorn, aux États-Unis, utilise la reconnaissance faciale sur les images d'Internet pour identifier les victimes du trafic d'êtres humains.

En France, nous avons des dizaines de milliers de clients, qui vont des start-up aux multinationales et aux grandes entreprises du CAC 40. Des organisations à but non lucratif bénéficient elles aussi des services du cloud AWS pour innover et améliorer l'expérience de nos concitoyens. Ces entreprises et organismes s'appuient sur un large réseau de partenaires en France, avec notamment Atos, Capgemini ou Accenture.

Aujourd'hui, lorsque nous interrogeons nos clients, ils nous disent faire confiance à AWS pour cinq raisons : l'agilité, la réduction des coûts informatiques, l'élasticité, la capacité à innover et la capacité de se déployer mondialement.

J'en viens à la sécurité, qui faisait l'objet de votre question. Effectivement, c'est une question prioritaire pour nos clients comme pour nous. Je vous rassure, chez AWS, c'est même la première des priorités. D'ailleurs, notre directeur technique nous le rappelle souvent : sans sécurité, nous perdrions bien évidemment la confiance de nos clients.

Il y a, parmi nos clients, des prestataires de services financiers ou de soins, des organisations opérant sur des marchés régulés, qui attachent une importance toute particulière à cette question de la sécurité des données. En général, ils se tournent vers nous pour quatre raisons.

La première, c'est la protection des données. Les infrastructures physiques d'AWS permettent des dispositifs de protection efficace pour assurer la confidentialité des clients. Toutes les données sont stockées dans des centres de données hautement sécurisés.

La deuxième, c'est le respect des exigences en matière de conformité. Nous gérons des dizaines de programmes de conformité dans nos infrastructures, dont nous faisons bénéficier tous nos clients. Nous sommes d'ailleurs contrôlés très fréquemment par des auditeurs tiers.

La troisième raison, c'est la mise à l'échelle rapide. Aujourd'hui, que vous soyez un développeur ou une grande entreprise, vous bénéficiez des mêmes niveaux de sécurité dans le cloud, quelle que soit la taille de votre entreprise.

Enfin, la dernière, c'est de pouvoir réaliser des économies considérables. La sécurité nécessite des investissements extrêmement importants pour les entreprises. En utilisant le cloud AWS, vous bénéficiez des investissements que nous avons réalisés. Nos équipes parlent énormément de sécurité avec nos clients, avec les développeurs, avec les start-up, et les accompagnent pour partager les bonnes pratiques, notamment l'utilisation du chiffrement.

J'en viens au sujet de la souveraineté numérique, qui nous réunit aujourd'hui. C'est un sujet qui est complexe, et vous êtes bien placés pour le savoir après avoir auditionné de nombreuses entreprises, experts et représentants du Gouvernement.

À mon sens, s'agissant de l'utilisation de la technologie cloud, la question de la souveraineté peut se réduire à celle de la sécurité de données qui sont confiés aux fournisseurs tels qu'AWS. Pour répondre à cet enjeu, il faut, selon nous, assurer la combinaison de quatre facteurs. Tout d'abord, il faut que nos clients gardent la propriété et le contrôle de leurs données. Dans les contrats d'*Amazon Web Services*, ce point est extrêmement clair : nos clients gardent le contrôle de leurs données. Qui y a accès ? À quelles données ? Ce contrôle, c'est nos clients qui le décident. Par ailleurs, même si ces données nous sont confiées pour des traitements, nos clients en gardent la propriété.

Ensuite, nos clients choisissent la localisation de leur stockage, quel que soit leur pays d'origine. En outre, ils ont la garantie de la réversibilité. Ils peuvent changer de fournisseur ou rapatrier leurs données dans leurs propres centres d'hébergement. C'est un point extrêmement important de cette souveraineté. Enfin, l'utilisation de notre technologie permet aux entreprises de libérer de la main-d'oeuvre et des marges de manoeuvre financières qu'elles peuvent concentrer sur l'innovation et la création de nouveaux services.

Pour conclure, et avant de laisser Stéphan Hadinger vous répondre sur la question plus précise du *Cloud Act*, je tiens à dire que nous offrons de

véritables opportunités à nos entreprises pour innover au profit des citoyens. L'avenir des entreprises, c'est de savoir exploiter leurs données pour créer de la valeur. De plus en plus de start-up françaises doivent émerger et se déployer mondialement. C'est pour cela que nous soutenons de nombreux programmes d'éducation avec les universités pour former les personnes qui le souhaitent aux nouvelles technologies. Nous allons former environ 3 000 personnes cette année. Nous fournissons enfin un accompagnement technique aux start-up afin qu'elles puissent se concentrer sur la création de leur modèle d'affaires. C'est un enjeu extrêmement important pour la souveraineté d'un pays que de savoir maîtriser cet environnement.

M. Stéphan Hadinger, directeur technique d'*Amazon Web Services France*. - Le *Cloud Act* est effectivement une question essentielle qui a suscité de nombreuses interrogations, en particulier depuis son entrée en vigueur début 2018. Nous avons assisté à beaucoup de controverses, notamment sur l'idée que le *Cloud Act* permettait au gouvernement américain d'avoir un accès libre et sans entrave aux données des clients de fournisseurs de cloud, ce qui est faux. Il a également été avancé que l'on ne pouvait plus avoir confiance dans les fournisseurs de cloud américains, ce qui est également faux. Par ailleurs, il faut savoir qu'il ne s'applique pas qu'aux fournisseurs de cloud.

Je vous propose donc d'aborder quelques-uns des plus grands mythes, qui sont autant d'idées fausses, autour du *Cloud Act*. Tout d'abord, d'après l'analyse de nos juristes, le *Cloud Act* ne fournit pas aux autorités judiciaires américaines un accès direct et illimité aux données stockées. C'est un mécanisme qui permet aux autorités de saisir un tribunal pour demander l'accès à des données dans le cadre d'affaires criminelles et pénales graves, comme des cas de terrorisme, des cas de pédophilie ou d'infractions liées à la drogue. Les autorités doivent respecter des normes juridiques rigoureuses pour obtenir un mandat délivré par un tribunal américain. Notamment, un juge indépendant doit conclure que les preuves recherchées sont clairement spécifiées et que les motifs qui sont présentés par les autorités sont raisonnables et directement liés à un crime. Enfin, la demande doit être claire, précise et proportionnée. Notons que ces normes sont parmi les plus strictes au monde.

Ensuite, le *Cloud Act* ne modifie pas la manière dont AWS protège les données de ses clients. Nous sommes toujours extrêmement précautionneux et rigoureux quant à la protection des données. En effet, le *Cloud Act* reconnaît spécifiquement le droit pour les fournisseurs de cloud de contester toute demande d'accès. Concrètement, chaque fois que nous recevons une demande, quel qu'en soit, d'ailleurs, le pays d'origine, nous avons une équipe dédiée de juristes qui analyse la demande et qui vérifie que l'émetteur de la demande est bien habilité. Nous informons également nos clients afin qu'ils puissent se défendre contre cette demande. Généralement, l'analyse conclut soit à une contestation de la demande, si elle

n'est pas conforme aux normes, ou si nous la jugeons contraire à des lois internationales ou à des intérêts de pays étrangers, soit à une réponse partielle ou complète. Dans ce dernier cas, la décision remonte directement au plus haut niveau de l'entreprise, et, pour nos équipes techniques, ce sujet est traité comme un incident de sécurité.

Les deux points que je viens de présenter englobent la partie juridique de la protection des données, mais il y aussi des mécanismes techniques. Nous invitons très fortement nos clients à chiffrer leurs données, en particulier leurs données sensibles, dans le cloud. Pour cela, nous leur fournissons des services, mais ils sont libres d'utiliser toute technologie qu'ils souhaitent. Notons également que le *Cloud Act* n'oblige pas les fournisseurs de cloud à déchiffrer les données. Or, comme vous le savez, une donnée chiffrée sans la clé correspondante est complètement inutilisable.

Enfin, il faut savoir que le *Cloud Act* ne s'applique pas qu'aux fournisseurs de cloud. Ce terme est un acronyme qui signifie *clarifying lawful overseas use of data*, que je traduirai par « clarifier l'utilisation licite de données à l'étranger ». Malheureusement, l'utilisation de cet acronyme a laissé penser que le *Cloud Act* ne s'appliquait qu'au cloud, ce qui est une idée fausse. En réalité, il s'applique de manière beaucoup plus large, notamment aux services de télécommunication, et concerne donc les opérateurs de téléphonie mobile ou fixe, aux plateformes de médias sociaux, aux plateformes de messagerie, et bien sûr, aux plateformes de cloud.

Notons également qu'en vertu d'un droit international bien établi et complètement indépendant du *Cloud Act*, une entreprise est soumise à la juridiction des États-Unis si elle est américaine, bien sûr, mais également si elle entretient des contacts minimaux avec les États-Unis. En conséquence, une société non américaine sera aussi soumise au *Cloud Act* si elle a, par exemple, une succursale, un bureau, une filiale ou des employés sur le territoire américain. Le ministère de la justice a récemment fait remarquer que le fait d'avoir un site web qui vend à des clients américains, sans même avoir une présence sur le territoire américain, était probablement suffisant pour relever de la juridiction des États-Unis. M. Richard Downing, du département de la justice, a conclu qu'aujourd'hui la plupart des grands fournisseurs de cloud américains ou non américains étaient soumis à la juridiction des États-Unis.

En conclusion, comme vous le constatez, nous prenons le *Cloud Act* très au sérieux. Nous n'en faisons pas la promotion ; néanmoins, nous appliquons la loi, et nous devons à nos clients des explications et de la transparence. Toutefois, nous constatons qu'il provoque beaucoup de confusion. C'est pourquoi il me semble nécessaire de mener rapidement des négociations entre la France et les États-Unis, ou entre l'Europe et les États-Unis, afin d'établir un cadre juridique clair. C'est d'ailleurs ce qu'a déclaré M. Bruno Le Maire le 2 juillet dernier à Bruxelles.

M. Gérard Longuet, rapporteur. - Vous êtes au fond prestataire des concurrents de votre maison-mère ...

M Julien Groues. - Nous opérons dans de nombreux secteurs, et effectivement, parmi nos millions de clients, certains ont des services ou des offres qui peuvent être concurrents de ceux du groupe Amazon.

M. Gérard Longuet, rapporteur. - Est-ce qu'AWS pourrait exister indépendamment d'Amazon ?

M Julien Groues. - Aujourd'hui, ce sont deux entreprises distinctes, toutes les deux avec un PDG à sa tête. Amazon.com est client d'AWS.

M. Gérard Longuet, rapporteur. - Et AWS a-t-il l'exclusivité des prestations informatiques pour le compte d'Amazon.com ?

M Julien Groues. - Je n'ai pas la réponse. Une majorité de ces prestations, je pense.

M. Gérard Longuet, rapporteur. - Je n'ai pas de question à proprement parler, puisque nous n'avons pas assez de recul par rapport au *Cloud Act*. Certains de nos interlocuteurs nous ont déjà présenté cet argument qui consiste à dire qu'il ne s'agit pas d'un pouvoir absolu de l'administration américaine, laquelle doit passer par un juge indépendant, ce qui n'est pas tout à fait la même chose, surtout quand on connaît les magistrats américains. Quelle est la procédure d'appel si un magistrat refuse l'accès aux données au Trésor américain ?

M. Stéphan Hadinger. - Comme vous avez pu le constater, je ne suis pas juriste...

M. Gérard Longuet, rapporteur. - Vous maîtrisez pourtant parfaitement votre sujet !

M. Stéphan Hadinger. - Je ne pourrai cependant pas entrer dans les détails. Je le répète, la sécurité est vraiment la priorité pour nos clients, et nous leur offrons une protection tant juridique que technique.

M. Gérard Longuet, rapporteur. - J'ai du mal à concevoir que vous puissiez transmettre avec un grand sourire à un procureur américain ayant obtenu satisfaction auprès d'un juge indépendant des données chiffrées, donc parfaitement incompréhensibles...

M. Stéphan Hadinger. - Nous mettons à disposition de nos clients des solutions de chiffrement intégrées. C'est un progrès pour nombre de nos clients qui devaient suivre un cheminement lent et coûteux quand ils souhaitaient procéder au chiffrement dans leurs propres infrastructures. Avec notre cloud, en quelques clics, vous pouvez assurer la totalité du chiffrement sur la totalité de vos infrastructures. Après, il reste la question des clés de chiffrement. Nous proposons des solutions intégrées où les clés sont gérées dans des boîtiers - des HSM (*Hardware Security Module),* des modules de sécurité matérielle -, qui sont construits pour que les clés ne

puissent jamais en sortir. Cela reste une option, et nos clients peuvent choisir de surchiffrer leurs données les plus sensibles avec des solutions de partenaires tels que Thalès.

M. Gérard Longuet, rapporteur. - Quelle sera l'attitude de l'hébergeur vis-à-vis d'un procureur américain ayant obtenu la communication partielle de données chiffrées et se retrouvant comme une poule avec un couteau ? Il faut bien expliquer à la poule comment fonctionne le couteau...

M. Stéphan Hadinger. - Ces mécanismes de boîtiers de sécurité que nous utilisons, et que certains de nos partenaires commercialisent, sont conçus techniquement pour que seul le client ait accès aux clés pour déclencher un déchiffrement.

M. Gérard Longuet, rapporteur. - Vous renvoyez donc le procureur vers le client.

M. Jérôme Bignon. - Vous ne pouvez donner que ce que vous avez.

M. Jérôme Bascher. - Monsieur le directeur, avez-vous un lien autre qu'actionnarial avec votre société-mère ? Autrement dit, est-ce que les données dont vous disposez peuvent être réclamées par votre société-mère ?

Par ailleurs, vous nous avez un peu rassurés sur le *Cloud Act*, mais qu'est-ce qui empêche de faire un second *Cloud Act* qui irait un cran plus loin et qui vous obligerait plus qu'avant par rapport aux autorités américaines ? On peut penser à l'affaire du pétrole iranien.

M Julien Groues. - Sur les liens entre Amazon.com et AWS, je le répète, il s'agit de deux entités séparées du groupe Amazon. Au sein d'AWS, nous gérons le groupe Amazon comme tous les autres clients, avec une séparation des données, des environnements et de nos procédures.

M. Jérôme Bascher. - Ce n'est pas tout à fait ma question. Sans violer le secret des affaires, pouvez-vous nous dire si vous avez un lien contractuel avec Amazon.com qui vous obligerait à faire remonter vers cette entité des données sur vos autres clients ?

M Julien Groues. - Je n'ai jamais connu ce cas de figure. Je me renseignerai et reviendrai vers vous pour vous donner la réponse.

M. Franck Montaugé, président. - Existe-t-il des solutions fiables et accessibles financièrement aux particuliers pour le chiffrement des données personnelles ? Je pense par exemple aux données captées par Amazon.com.

M. Stéphan Hadinger. - Je vais revenir sur le modèle de sécurité, ce que l'on appelle le modèle de responsabilité partagée d'AWS. Nous faisons en sorte que les données appartiennent à tout moment exclusivement à nos clients, qui ont tous les contrôles sur les modalités d'accès à ces données et qui peuvent mettre en place des mécanismes de chiffrement s'ils le souhaitent. Cela signifie aussi qu'eux seuls connaissent la nature de ces

données. Nos services opérant de manière automatique, nous n'avons aucune connaissance, dans la majorité des cas, du type de données pour lesquelles nos clients utilisent le cloud AWS. Le seul cas où nous en avons connaissance, c'est quand nous travaillons avec eux sur des références publiques. J'y insiste, grâce à la plateforme, nous n'avons pas connaissance du type de données que mettent de nos clients. Partant de là, nous appliquons des normes de sécurité internationales, comme l'ISO 27001, le PCI DSS (*Payment Card Industry Data Security Standard*), norme de sécurité protégeant les informations confidentielles, qui est lié à la sécurisation des numéros de carte bancaire, et ce de manière uniforme sur l'ensemble des données de nos millions de clients. Si vous utilisez AWS pour mettre des données personnelles, la plateforme est sécurisée comme s'il s'agissait de données bancaires ou de données de santé, car nous appliquons toujours ce même modèle.

La réponse est donc oui : vous pouvez utiliser le cloud AWS pour vos données personnelles et vous pouvez les chiffrer. Nous proposons un service simple, qui s'active en un seul clic, et dont le coût est nul ou quasi nul selon les cas.

M. Franck Montaugé, président. - Ce n'est pas tout à fait ma question. Si j'utilise Amazon « commerce » pour une recherche, cela crée un flux de données, de connexions. Est-ce que ces données de navigation, de circulation peuvent rester personnelles et non utilisables par un tiers, fût-il Amazon ?

M. Stéphan Hadinger. - Vous l'avez compris Amazon.com et Amazon.fr sont des clients d'AWS, et opèrent leurs propres applications ...

M. Franck Montaugé, président. - Donc vous ne pouvez pas me répondre...

M. Stéphan Hadinger. - Effectivement, je ne connais pas en détail les mécanismes qu'utilisent Amazon.fr et Amazon.com.

M. Gérard Longuet, **rapporteur**. - Lorsque l'on cherche quelque chose chez Amazon, la Pierre philosophale, par exemple, on accumule toute une série de de recherches et toutes ces démarches sont chez Amazon.com, qui, peut-être, va demander à AWS de les stocker s'il considère que cela vaut le coup de les garder. AWS n'est pas saisi par le client final. C'est Amazon qui apporte des données à héberger.

M. Franck Montaugé, **président**. - Lesquelles données sont réutilisées, mais cela ne me pose pas de problème. Je souhaitais juste des précisions sur l'enjeu fondamental que vous avez pointé, à savoir le chiffrement des données. Pour conclure, j'aurai deux questions à vous poser. Comment prenez-vous en compte d'éventuelles contradictions entre le *Cloud Act* et le RGPD ? Avez-vous des statistiques concernant les demandes d'accès formulées par les États-Unis ?

M. Julien Groues. - Effectivement, entre le RGPD et le *Cloud Act*, d'après nos juristes, il peut y avoir un confit. Cela nous donne des éléments supplémentaires pour contester les demandes américaines. Le *Cloud Act* prévoit d'ailleurs ce cas de conflit avec les droits des pays dans lesquels sont stockées les données.

M. Stéphan Hadinger. - Sur ces questions de sécurité, nous publions des rapports de transparence. Dans les douze derniers mois, nous avons reçu 25 demandes émanant des autorités judiciaires américaines. La majorité de ces demandes concernait des clients américains sur le territoire américain. La majorité de ces demandes a été contestée. Aucune de ces demandes ne concernait une société cotée, une organisation publique ou un client français.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible en ligne sur le site du Sénat.

Audition de MM. Michel Coulomb, responsable des ventes, région sud incl. France, Daniel Matray, responsable App Store Europe, et Erik Neuenschwander, responsable vie privée des utilisateurs, d'Apple, le 3 septembre 2019

M. Franck Montaugé, président. - Nous entendons à présent des représentants de l'entreprise Apple : MM. Michel Coulomb, responsable des ventes pour l'Europe du Sud, Daniel Matray, responsable *App Store* pour l'Europe, et Erik Neuenschwander, responsable Vie privée des utilisateurs.

Je rappelle, pour la forme, qu'un faux témoignage devant notre commission d'enquête serait passible des peines prévues aux articles 434-13, 434-14 et 434-15 du code pénal.

Conformément à la procédure applicable aux commissions d'enquête, MM. Michel Coulomb, Daniel Matray et Erik Neuenschwander prêtent serment.

M. Franck Montaugé, président. - Nous connaissons tous les activités d'Apple, du concepteur de terminaux - ordinateurs, téléphones intelligents, tablettes - au navigateur web en passant par le système d'exploitation, le magasin d'applications, les assistants vocaux ou encore les objets connectés.

Je commencerai par deux questions relatives aux données.

Le *Cloud Act* permet aux autorités américaines de disposer des données stockées, et ce quel que soit le lieu de stockage. Cela inquiète légitimement les pouvoirs publics français car les données personnelles aussi bien que les données stratégiques des entreprises peuvent ainsi être pillées. Or de nombreux utilisateurs confient leurs données à *iCloud*, dans le cadre duquel votre firme a au demeurant recours à des sous-traitants comme Google ou Amazon. Pouvez-vous nous assurer qu'Apple ne permet pas et ne permettra pas aux autorités américaines de prendre connaissance des données de nos concitoyens et de nos entreprises ? Comment comptez-vous concilier ces obligations avec les règles européennes protégeant les données personnelles (RGPD) ?

Par ailleurs, la presse a rendu public le fait que les assistants vocaux d'Amazon, de Google, de Microsoft et d'Apple enregistraient les conversations de ses utilisateurs à leur insu. Les données enregistrées sont transmises à des centres d'écoute où des humains les analysent, afin d'améliorer les performances des systèmes de reconnaissance vocale. Certains employés de ces centres auraient confié avoir été témoins de moments intimes, criminels, voire des deux. Cette information n'a jamais été clairement communiquée aux consommateurs et on peut légitimement penser que nombre d'entre eux n'auraient pas acheté votre enceinte connectée s'ils avaient su qu'ils pouvaient être écoutés par des humains.

Cet été, une autorité allemande de protection des données a ordonné à Google de remédier à cette situation. Dans la foulée, Apple a annoncé une suspension temporaire de cette pratique, le temps de laisser à ses clients la possibilité d'accepter ou de refuser d'y participer. Pourquoi ne pas avoir été plus clair avec vos utilisateurs ?

Enfin, Apple communique beaucoup sur sa volonté de se différencier des autres Gafam, professionnels de la collecte de données personnelles. Quelles mesures avez-vous mises en place pour respecter la vie privée des utilisateurs ?

M. Michel Coulomb, **responsable des ventes d'Apple pour l'Europe du Sud.** - Le respect de la vie privée est au coeur de nos activités, de la conception et du développement de nos produits et services, depuis 44 ans qu'Apple existe et 38 ans que l'entreprise est implantée en France. Nous respectons toutes les lois européennes en la matière : les données de nos utilisateurs européens sont régies par le RGPD, et nous faisons du respect de ce règlement une priorité absolue.

M. Erik Neuenschwander, responsable Vie privée des utilisateurs d'Apple. - Nous avons une équipe basée à Cork, en Irlande, dirigée par un officier de protection des données, qui travaille avec les autorités au niveau mondial, afin d'examiner la légitimité des requêtes de ces dernières et d'y répondre. Le RGPD est appliqué à ces requêtes, quel que soit l'endroit où les données sont stockées. Quant aux sous-traitants, ils conservent les données que nous leur confions sous une forme encryptée, sans avoir accès à la clé de décryptage qui est stockée dans les centres de données d'Apple.

Avant même le lancement de l'assistance vocale Siri, nous avons conduit une évaluation sur ses conséquences en matière de vie privée, et appliqué à cet outil le *privacy by design* (le respect de la vie privée dès la conception), comme à tous nos produits et services. Son principe le plus important est la « minimisation » des données, qui consiste à laisser autant que possible ces données sur l'appareil lui-même et à en « minimiser » la collecte. Nous limitons également l'utilisation des données récoltées au service lui-même. Ainsi les données remontées par Siri ne sont utilisées que pour servir à l'amélioration du programme, avec un identifiant anonymisé généré de manière aléatoire par l'appareil lui-même. Ainsi, les données sont associées à l'appareil, mais pas à l'utilisateur lui-même.

Autres principes importants du *privacy by design*, la transparence et le consentement. L'utilisation de Siri sur un appareil est au libre choix de son propriétaire : un écran lui propose de donner ou non son consentement, en lui fournissant des informations sur la conception de Siri et en précisant que l'utilisation des données est exclusivement prévue pour améliorer le programme dans une procédure de contrôle qualité appelée *grading*.

Malgré cela, le public a estimé qu'Apple ne respectait pas ses standards élevés en matière de vie privée. Nous avons donc, de manière

proactive, suspendu le *grading* tout en menant une évaluation en interne afin de garantir que l'ensemble de nos procédures respectent ces standards. Le *grading* ne sera rétabli qu'après des changements en ce sens. Ainsi, nous ne stockerons plus les données audio des utilisateurs par défaut ; à la place, ceux-ci devront donner leur consentement pour qu'elles soient stockées et utilisées pour améliorer Siri.

M. Gérard Longuet, rapporteur. - Comment stockez-vous et traitez-vous les empreintes digitales que vous recueilliez via *TouchID* et les photographies qui vous sont envoyées par *FaceID* ? Ces données restent-elles sur l'appareil ou sont-elles stockées sur l'*iCloud* ?

M. Michel Coulomb. - Les informations recueillies via *FaceID* et *TouchID* sont uniquement stockées sur l'appareil et ni Apple, ni une tierce partie ne peuvent y accéder. Pour les photographies, plusieurs méthodes de stockage sont possibles. Beaucoup de consommateurs préfèrent les stocker sur le cloud afin de les partager. Elles y sont alors stockées sous forme encryptée, et Apple n'y a pas accès.

M. Gérard Longuet, rapporteur. - Que ferez-vous des données recueillies par la nouvelle fonctionnalité de signature de documents ?

M. Michel Coulomb. - Nous avons en effet annoncé au moins de juin cette nouvelle fonctionnalité, *Sign In with Apple*, qui sera intégrée à la prochaine mise à jour d'iOS et des autres logiciels au mois d'octobre.

M. Erik Neuenschwander. - *Sign in with Apple* donne aux utilisateurs la possibilité de s'identifier sans avoir à créer de nouveaux mots de passe - ce qui multiplie les risques d'oubli et expose au *phishing*, une pratique consistant à subtiliser les mots de passe des utilisateurs pour prendre le contrôle de leur compte.

De plus, nous proposons une authentification à deux facteurs (*two-factor authentication*) pour améliorer la sécurité des comptes Apple : un code sera envoyé sur le téléphone de l'utilisateur, en plus du code d'accès. La grande majorité de nos comptes ont désormais cette fonctionnalité.

Mais la troisième fonctionnalité est la plus importante, car elle assure que les données collectées ne sont pas utilisées à d'autres fins. D'abord, Apple ne construit pas de profil utilisateur sur la base d'une connexion via l'identification Apple à une application de sport ou de restauration par exemple. Ensuite, Apple donnera la possibilité à l'utilisateur de fournir à chacune des entreprises avec lesquelles il est en relation une adresse électronique *ad hoc* pour le contacter. Ainsi, il sera plus difficile pour ces entreprises de réunir et combiner les données qu'elles auront reçues.

C'est pourquoi nous estimons que *Sign in with Apple* améliorera la sécurité et la confidentialité des données des utilisateurs.

M. Gérard Longuet, rapporteur. - Apple fait l'objet d'un récent recours collectif déposé par des développeurs, qui contestent notamment la

commission de 30 % prélevée par l'entreprise contre l'accès à son magasin d'applications. Ce chiffre est-il immuable ou négociable ?

M. Michel Coulomb. - Nous avons développé un système d'exploitation pour chacun de nos produits. En revanche, nous développons peu de logiciels nous-mêmes et nous préférons travailler avec des développeurs extérieurs afin d'enrichir le panel à disposition des utilisateurs. 20 millions de développeurs travaillent avec nous dans le monde, dont plusieurs centaines de milliers en France. Nous avons créé une véritable économie à partir de rien, puisque l'*App Store* n'existait pas il y a onze ans. En une décennie, nous avons versé 1,3 milliard d'euros aux développeurs français au titre des ventes réalisées sur *l'App Store* en France et partout dans le monde. Nous sommes présents dans 155 pays : autant de marchés accessibles immédiatement aux développeurs qui lancent une application sur notre plateforme.

M. Daniel Matray, responsable App Store Europe. - Nos deux millions d'*apps* sont disponibles dans 155 pays et 81 langues. L'*App Store* a révolutionné la distribution de logiciels, qui voici onze ans s'effectuait encore par voie physique.

Notre premier objectif est que les consommateurs puissent trouver sur l'*App Store* les meilleures applications adaptées à leurs besoins. Le deuxième pilier, c'est que les développeurs d'applications aient un canal de distribution dans les 155 pays où nous sommes présents pour toucher le plus grand nombre possible de clients. Ces 20 millions de développeurs se trouvent aussi bien dans un garage en Californie que dans une grande entreprise à Paris ou une PME dans la Marne. Nous les rencontrons régulièrement, pour leur expliquer les outils et les procédures. Il y a beaucoup de *success stories* liées à *l'App Store* en France.

Le développeur peut choisir de rendre son logiciel payant, mais il existe d'autres options comme la publicité ou la vente de produits physiques. Pour les applications gratuites, Apple ne perçoit pas de commission. En revanche, nous prélevons une commission de 30 % pour la vente des applications payantes, qui utilisent nos moyens de paiement. Ayant moi-même été développeur, je rappelle néanmoins qu'à l'époque de la distribution physique de logiciels, la commission était comprise entre 60 et 70 %. Le développeur d'aujourd'hui peut créer une application à domicile, avec toute la technologie mise à disposition par Apple, qui la distribue ensuite. Plus besoin, pour le développeur, de trouver un distributeur local pour chaque marché.

La commission est de 30 % pour les achats uniques. Pour les abonnements, elle est de 30 % la première année et de 15 % les suivantes, ce qui est extrêmement avantageux et ce qui fait de ce service un succès.

M. Gérard Longuet, rapporteur. - Qu'en est-il de votre pénétration du secteur bancaire, avec le lancement d'*ApplePay* et bientôt de l'*Apple Card* ?

Qu'en est-il également de vos intentions dans le domaine des véhicules autonomes ?

M. Michel Coulomb. - Nous cherchons à développer des services visant à simplifier la vie de nos utilisateurs. Lancé en France il y a trois ans, *ApplePay* s'inscrit dans cette logique en proposant sous forme dématérialisée les cartes de crédit de nos 34 banques partenaires. En d'autres termes, c'est une carte de crédit virtuelle. Apple n'est pas un établissement financier, mais se présente comme un relais technologique pour faciliter l'utilisation des cartes de crédit.

L'*Apple Card* a été lancée au mois de juillet aux États-Unis, en partenariat avec Goldman Sachs.

Quant aux véhicules autonomes, Apple n'a pas annoncé de nouveaux produits pour l'automobile. Nous proposons seulement le logiciel *CarPlay*, disponible sur presque tous les modèles automobiles, qui fait apparaître les fonctionnalités de l'iPhone sur l'écran de la voiture.

M. Gérard Longuet, rapporteur. - Apple a récemment racheté la start-up Drive.ai, qui travaille sur les véhicules autonomes...

M. Michel Coulomb. - Les rachats de start-ups ne font pas l'objet d'annonces, c'est pourquoi je ne puis vous en dire davantage sur ce point, mais j'essaierai de vous apporter des précisions.

M. Jérôme Bascher. - Le fait qu'une partie des données soit exploitée par Apple, et l'autre non rend les choses illisibles et incompréhensibles. Une solution du type « tout ou rien » ne serait-elle pas préférable ?

Comment expliquez-vous qu'Apple n'ait pas percé dans le monde administratif français, laissant d'autres technologies s'imposer ?

M. Michel Coulomb. - Nous avons un succès considérable auprès des consommateurs français et des professionnels : depuis nos débuts, nous sommes présents sur le marché de l'éducation, et dans le monde de l'entreprise et du secteur public. Cependant, nous sommes un fournisseur parmi d'autres, dans un secteur très compétitif, avec un nombre d'options très important pour les utilisateurs et avec des concurrents venant du monde entier.

M. Daniel Matray. - Toutes les administrations sont présentes sur nos plateformes : la majorité des entreprises publiques ont une application dans l'Apple Store ou sont disponibles sur nos différentes plateformes. Nous sommes très ouverts aux administrations, comme aux entreprises privées, et nous travaillons avec elles pour développer des applications à l'intention de leurs administrés et de leurs clients.

La sécurité est très importante : pour développer une application et accéder à notre plateforme, il faut respecter des règles très précises. Les

consommateurs doivent être protégés et connaître la provenance de leurs applications.

M. Erik Neuenschwander. - La compréhension et la confiance de l'utilisateur constituent une part importante du respect de la vie privée. Nous essayons de diminuer les sources de confusion. Nous y contribuons notamment en développant une technologie embarquée dans l'appareil pour améliorer l'expérience utilisateur sans qu'Apple ait à traiter les données. Ainsi, la reconnaissance faciale est entièrement traitée par l'appareil de l'utilisateur, grâce aux photographies qu'il a fournies, sans remontée jusqu'à Apple. C'est l'ambition que nous nous sommes fixée : améliorer l'expérience utilisateur sous le contrôle direct de ce dernier.

Lorsqu'il est nécessaire de faire remonter des données, nous avons développé les alertes au moment approprié (*just in time alerts or just in time consents,* l'alerte au bon moment ou le consentement au bon moment) pour avertir le consommateur des avantages d'une utilisation donnée et de l'usage qui sera fait des données transmises. Ce n'est pas parfait, mais nous nous engageons à améliorer nos processus et à réduire les erreurs dans ce domaine.

M. Pierre Ouzoulias. - J'utilise probablement des ordinateurs Mac depuis 38 ans... J'ai commencé avec un Mac 512, à une époque où le logiciel devait être chargé dans l'ordinateur via une disquette. Mais pendant ces 38 ans, Apple a aussi formaté mon esprit, au point que je n'arrive pas à changer de système d'exploitation ! Votre modèle économique est d'autant plus réussi que vous ne vendez plus de logiciels : une grande partie de votre notoriété repose sur votre capacité à formater la manière dont nous utilisons vos produits. N'y voyez aucun reproche, mais plutôt une servitude volontaire ! Apple a néanmoins une certaine réticence à accepter l'interopérabilité et à nous permettre de recréer le même univers numérique avec d'autres matériels. N'y a-t-il pas une contradiction entre ce modèle économique et l'interopérabilité, qui est l'une des conditions de la souveraineté numérique ?

M. Michel Coulomb. -En matière de technologie, 38 ans, c'est une très longue période. Nous avons su conserver la confiance de nos clients en innovant et en créant constamment de nouveaux produits et services sans dévier de nos fondamentaux : excellence des produits, respect de l'environnement et de la vie privée, recherche d'une technologie au croisement avec les sciences humaines. Apple est spécial parce que nous avons toujours développé, de façon synchrone, des produits matériels et des logiciels.

M. Erik Neuenschwander. - Nous avons fait en sorte que les données des utilisateurs puissent être transférées librement d'un service à l'autre grâce à un portail que nous avons mis à leur disposition, et à partir duquel ils peuvent obtenir des copies de leurs données. C'est l'une des

exigences fondamentales du RGPD. Nous sommes heureux de le faire et confiants dans le fait que nos clients resteront convaincus de l'intérêt de nos services.

M. Daniel Matray. - La très grande majorité de nos services, comme *iTunes* ou *Apple Music*, sont disponibles sur d'autres plateformes, que ce soit Windows, Android ou Google. Nous sommes un environnement ouvert. Les applications de *l'App Store* peuvent être transférées sur des périphériques et d'autres accessoires. Cette liberté, tout en garantissant une sécurité optimale, est dans l'intérêt du consommateur.

M. Patrick Chaize. - Que se passe-t-il si, en vertu du *Cloud Act*, un juge américain persiste à donner aux autorités des États-Unis un accès à des données personnelles protégées par le RGPD ? Quel volume de demandes a été adressé à Apple par un juge, et combien d'entre elles ont été acceptées ?

M. Erik Neuenschwander. - Les demandes de ce type sont adressées au bureau de la protection des données d'Apple, qui applique le RGPD.

Les statistiques sur le nombre de demandes et les réponses qui y ont été apportées, pays par pays, sont disponibles sur notre site, sur une page dédiée : www.apple.com/legal/transparency/.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible en ligne sur le site du Sénat.

Audition de M. Bruno Le Maire, ministre de l'économie et des finances,
le 10 septembre 2019

M. Franck Montaugé, président. - Monsieur le ministre, notre commission d'enquête termine ses travaux avec votre audition, qui fait l'objet d'une captation vidéo disponible en ligne sur le site Internet du Sénat ; un compte rendu sera également publié.

Une commission d'enquête fait l'objet d'un encadrement juridique strict. Je vous informe qu'un faux témoignage devant notre commission serait passible des peines prévues aux articles 434-13 à 434-15 du code pénal.

Conformément à la procédure applicable aux commissions d'enquête, M. Bruno Le Maire prête serment.

M. Franck Montaugé, président. - La France importe des biens et services numériques et les données de ses citoyens sont utilisées en masse à l'étranger : cette situation n'est pas à l'avantage de l'État. Quelle est la stratégie du Gouvernement ? Quels sont ses objectifs en matière d'économie numérique et de conquête de ces nouveaux marchés ? Vous avez régulièrement évoqué le sujet de la souveraineté technologique en des termes très offensifs. Très récemment, vous vous êtes prononcé pour une cryptomonnaie publique. La France a adopté une taxation sur les services numériques, façon pour elle d'imposer sa souveraineté fiscale aux acteurs du numérique. Comment le Gouvernement entend-il conduire sa stratégie pour que cette position ne se traduise pas par un recul face aux réactions des États-Unis ou d'Amazon qui a récemment annoncé qu'il répercuterait la taxe sur les entreprises utilisant sa plateforme ? Vous avez aussi pris des positions fortes sur le sujet du cloud, de l'informatique en nuage, avec la mise en place d'un cloud de confiance parfois désigné comme cloud souverain. Où en est ce sujet ? Parallèlement, afin de contrer les effets du *Cloud Act*, vous avez annoncé une réforme de la loi de blocage. Quel est votre calendrier et quelles sont les perspectives de la négociation entre l'Union européenne et les États-Unis sur ce sujet ?

M. Bruno Le Maire, ministre. - La question de la souveraineté numérique me tient particulièrement à cœur : notre souveraineté nationale, comme la souveraineté européenne, dépend en effet de notre capacité à bâtir technologiquement, financièrement et industriellement notre souveraineté digitale. Depuis une quinzaine d'années, nous avons à l'évidence pris du retard à cause de notre incapacité à faire émerger des géants du numérique français ou européens comparables aux géants américains ou chinois et à financer les technologies de rupture indispensables, notamment dans le domaine de l'intelligence artificielle. Or ces ruptures technologiques non seulement construiront ou non notre souveraineté politique, mais elles feront au XXIe siècle des vainqueurs et des vaincus, comme l'avait fait au XIXe siècle la révolution industrielle. Ceux qui maîtriseront les technologies de rupture

seront les vainqueurs et leurs clients seront les vaincus. Il est donc indispensable de maîtriser, dans les années qui viennent, un certain nombre de ces technologies de rupture : je pense en particulier à l'intelligence artificielle, à la nano-électronique et au calculateur quantique. On peut toujours parler de souveraineté politique matin, midi et soir en sautant sur son fauteuil comme un cabri, mais, sans maîtrise de ces ruptures technologiques, il n'y a plus de souveraineté politique. Quand vos voitures sont guidées par des logiciels étrangers ou que vos communications sont transmises par des fibres étrangères, vous n'avez plus de souveraineté politique. Voilà à quel niveau je veux placer les enjeux liés à la révolution digitale.

Cela implique que nous répondions à toutes les questions issues de cette révolution technologique. Quelle fiscalité construire pour financer ces ruptures technologiques ? Comment protéger nos données personnelles et nos données publiques ? Comment concilier ces ruptures technologiques avec la maîtrise de nos destins individuels et le respect de la vie privée, qui font partie de notre modèle de société européen, très différent de celui qui se bâtit aux États-Unis ou en Chine ? Les deux sujets politiques que votre commission d'enquête, que je trouve particulièrement bienvenue, doit traiter me semblent en effet être ceux-ci : la souveraineté politique et le mode de société dans lequel nous voulons vivre au XXIe siècle.

Comment pouvons-nous faire de la France le pays de l'innovation de rupture en Europe et combler le retard que nous avons pris depuis plusieurs années ? C'est très simple : il faut de l'argent ! Le financement est la clé absolue.

S'il n'y a pas de champion digital en Europe, c'est d'abord parce qu'il n'y a pas les financements nécessaires, ce qui permet ainsi à tous les géants du numérique, notamment américains, de racheter nos technologies et nos start-up. Nous sommes bons pour créer des start-up, nous sommes bons sur la recherche, notamment fondamentale, ou sur l'innovation, mais comme nous n'avons pas les moyens de les faire grandir, nous faisons le profit et la chance de pays étrangers. Je me demande même si l'argent public est bien employé quand il sert au financement de start-up qui sont ensuite rachetées par les Américains... Il est donc indispensable que nous ayons des financements qui se chiffrent en centaines de millions d'euros pour les projets les plus importants. On dénombre 36 « licornes » chinoises, c'est-à-dire des entreprises avec un chiffre d'affaires supérieur à 1 milliard de dollars, contre 93 aux États-Unis, 6 seulement en France et une poignée en Europe.

Depuis mai 2017, nous avons pris des décisions, dont certaines ont été critiquées, mais que je revendique parce que je les crois indispensables au financement de cette innovation. D'abord, un allégement massif de la fiscalité sur le capital, sur lequel un comité d'évaluation placé auprès de France Stratégie rendra ses premières conclusions au cours de l'automne.

Ensuite, la sanctuarisation du crédit d'impôt recherche ; je sais qu'il est critiqué, car il représente aujourd'hui plus de 6 milliards d'euros de dépense publique, mais - je le redirai à l'occasion de la présentation du projet de loi de finances pour 2020 d'ici quelques jours -, s'il faut tenir compte des remarques de la Cour des comptes sur les dépenses de fonctionnement, qui doivent être moins lourdes pour le contribuable, il ne faut pas modifier les paramètres fondamentaux, notamment sur le régime de groupe. Ce serait une erreur stratégique, car nos entreprises ont besoin de stabilité pour investir. Si nous voulons garder des centres de recherche en France et continuer à être dynamique en matière de financement de l'innovation, il faut une fiscalité stable, notamment sur le crédit d'impôt recherche. Enfin, je revendique la cession d'actifs publics, même si cette question fait couler beaucoup d'encre. Certains veulent que l'État gère les jeux de hasard ; je considère que ce n'est pas son rôle. Nous engageons donc la privatisation de la Française des jeux d'ici à la fin de l'année 2019 si les conditions de marché le permettent, en apportant toutes les protections nécessaires qui n'existent d'ailleurs pas aujourd'hui face à l'addiction au jeu. Car c'est bien tout le paradoxe, l'État a la maîtrise de la Française des jeux, mais il ne remplit pas son rôle en matière de protection contre l'addiction au jeu.

Je préfère donc renforcer le rôle de l'État en créant une autorité administrative indépendante, dont le premier objectif sera de lutter contre l'addiction au jeu, tout en laissant des opérateurs privés s'occuper des jeux de hasard, de tirage et de grattage, qui ne relèvent pas de la responsabilité de l'État.

Il en est de même pour Aéroports de Paris : nous allons renforcer les protections, notamment sur les tarifs aéroportuaires et les contrôles aux frontières, mais ce n'est pas le rôle de l'État de gérer des activités commerciales d'un aéroport - boutiques, hôtels ou parkings. L'argent de l'État sera mieux employé en investissant dans ce fonds pour une innovation de rupture, doté de 10 milliards d'euros, qui a deux avantages. Le premier, c'est qu'il dégagera des financements stables sur une longue durée pour financer des innovations de rupture inaccessibles aux opérateurs privés faute de rentabilité - 250 millions d'euros de revenus par an, représentant 2,5 milliards sur dix ans, garantis, car non soumis aux procédures budgétaires. Deuxième avantage, il préfigure le fonds pour l'innovation de rupture européen que nous appelons de nos voeux avec le Président de la République, et qui nous permettrait de disposer du même instrument que la *Defense Advanced Research Projects Agency* (Darpa) américaine, qui garantit des financements de longue durée à hauteur de plusieurs centaines de millions d'euros pour des innovations de rupture très coûteuses et non rentables au départ.

Cette politique commence à donner des résultats : le marché du capital-risque français est en pleine croissance, puisque les levées de fonds sont passées de 1 milliard d'euros en 2014 à 3,6 milliards en 2018 et devraient

atteindre 5 milliards en 2019. Nous sommes devenus la première destination pour les investissements industriels et les investissements en recherche et développement, avec 144 projets en 2018, soit plus que l'Allemagne et le Royaume-Uni réunis. Enfin, la France est le premier pays d'entrepreneurs en Europe.

La difficulté qui subsiste, sur laquelle je travaillerai la deuxième moitié du quinquennat, tient au fait que nous avons du mal à lever des tickets importants. Je pourrais citer nombre de PME très réputées qui voudraient grandir, que ce soit dans le domaine de la santé, de la musique ou du transport, et qui cherchent des tickets à 100, 200 ou 250 millions d'euros, mais qui ne les trouvent ni en France ni en Europe et doivent s'adresser à des fonds américains. C'est une perte de souveraineté directe pour la France. Faciliter la levée de fonds pour des tickets supérieurs à 100 millions d'euros est donc, à mes yeux, une priorité absolue. Un excellent rapport m'a été remis par Philippe Tibi sur le financement de nos leaders technologiques français en France ; nous nous en inspirerons pour faire des propositions. Je ne me résigne pas à ce que nous financions des start-up pour qu'elles deviennent des champions américains plus tard.

Il faut aussi protéger nos technologies : il n'est pas acceptable qu'un géant de la robotique allemand comme Kuka, dans lequel des centaines de millions d'euros ont été investis, soit racheté par un géant chinois, qui bénéficie dès lors des meilleures technologies en matière de robotique. Je l'ai dit depuis le début du quinquennat, je refuse le pillage des technologies françaises. Aujourd'hui, un certain nombre de puissances étrangères ne s'intéressent plus seulement à des géants industriels comme Safran et Thales. Elles convoitent de plus en plus de petites start-up installées dans des villes de taille moyenne qui ont des technologies de rupture ou qui commencent à les mettre en place. Nous allons donc protéger un certain nombre de secteurs technologiques grâce au renforcement, prévu par la loi Pacte, du contrôle des investissements étrangers en France.

Je pense en particulier à trois secteurs technologiques directement liés à notre sécurité nationale : la cybersécurité, le spatial et l'intelligence artificielle.

La deuxième protection qu'il faut garantir au-delà des technologies concerne la protection des données. Les inquiétudes face au *Cloud Act* sont tout à fait fondées. Nous avons défini avec le Président de la République une réponse stratégique sur cette question en distinguant les types de données.

Il convient en premier lieu de protéger les données personnelles. Après le scandale planétaire de Cambridge Analytica, il est intolérable de voir, comme ce fut le cas il y a encore quelques jours, de grandes entreprises du digital enfreindre le règlement général sur la protection des données (RGPD). La Commission européenne doit donc être totalement

intransigeante sur ces questions et nous devons nous appuyer sur l'Union européenne pour protéger les données personnelles.

En deuxième lieu, nous devons protéger certaines données des acteurs économiques. J'ai eu de longs échanges avec l'ensemble des entreprises concernées afin de définir les données concernées. Certaines données économiques ne sont pas stratégiques et se chiffrent en millions, voire plus, et peuvent être stockées en libre accès ; ce serait donc un mauvais investissement que de vouloir les stocker de façon sécurisée. Des données plus sensibles peuvent être stockées chez des opérateurs américains, qui ont des capacités de stockage et surtout de valorisation dont nous ne disposons pas. Nous ne pouvons pas demander aux entreprises de ne plus stocker les données chez ces opérateurs si nous ne sommes nous-mêmes pas capables de leur offrir ces mêmes services de valorisation. Nous voulons donc que l'administration américaine ne puisse pas récupérer ces données sans que l'entreprise soit avertie et sans un minimum de contrôles. Or, dans le *Cloud Act*, n'importe quelle agence américaine - je ne parle pas de la justice - peut le faire. Nous souhaitons parvenir à un accord entre l'Union européenne et les États-Unis pour qu'aucune administration américaine ne puisse récupérer ces données sans l'accord explicite de l'entreprise, préalable ou non, l'accord préalable étant de loin la meilleure solution

En troisième et dernier lieu, on considère les données directement liées à notre souveraineté ou à nos intérêts fondamentaux, comme les données de prix sur des ventes d'avions, qui ne doivent pas être hébergées autrement que chez un hébergeur national ou européen. Nous voulons donc créer un cloud de confiance français d'ici à la fin de l'année 2019, en nous appuyant en particulier sur l'entreprise Dassault Systèmes. Il pourra stocker toutes les données stratégiques des entreprises privées ou publiques qui le souhaitent, avec toutes les garanties de sécurité nécessaires.

Concernant le projet de monnaie virtuelle Libra de Facebook, je l'ai dit à plusieurs reprises, notamment à l'occasion du G7 des ministres des finances à Chantilly, je ne puis accepter qu'une entreprise privée se dote de cet instrument de souveraineté d'un État qu'est la monnaie. Cela pose des problèmes de sécurité : Libra ne serait pas soumis aux instruments de lutte contre le financement du terrorisme que nous avons bâtis notamment avec le Groupe d'action financière (GAFI), et qui sont très efficaces et très contraignants. De plus, dans des États ayant une monnaie faible, Libra pourrait parfaitement se substituer à ces monnaies souveraines : en Argentine, dont la monnaie, le peso, a connu des dévaluations successives très fortes et une évasion monétaire majeure, ce serait sans aucun doute le cas. Libra présente enfin un risque systémique, Facebook n'est pas une PME avec 45 clients - il a 2 milliards d'utilisateurs.

Se pose cependant une véritable difficulté liée aux coûts de transaction internationaux, y compris à l'intérieur de l'Europe. Nous devons travailler dans deux directions, l'une privée, l'autre publique. La première,

c'est d'examiner la manière dont les banques privées, notamment françaises, peuvent parvenir à réduire les coûts de transactions financières, et je sais que certaines y sont prêtes. Par ailleurs, deuxième piste dont je me suis entretenu avec Mario Draghi et Christine Lagarde, il faut réfléchir à une monnaie digitale publique. Je proposerai, à l'occasion de la réunion des ministres des finances à Washington en octobre prochain, de lancer la réflexion sur ce projet, qui apporterait des réponses aux difficultés de coût et de rapidité de transaction. Certaines banques centrales au Royaume-Uni, ou en Suède, ont commencé à lancer des expériences sur ce sujet. Je pense qu'il serait bon que la Banque centrale européenne puisse se saisir de cette difficulté.

Au-delà du sujet du financement de l'innovation et de la protection de nos données et de nos technologies, notre troisième grande réponse réside dans la fiscalité. La France n'a jamais voulu viser quelque entreprise que ce soit, et certainement pas celles de nos alliés américains. Mais les champions américains du secteur digital ont simplement pris une avance par rapport à nous. Les taxer n'a jamais été le projet français ; le projet français, c'est de bâtir une fiscalité adaptée à la réalité économique du XXIe siècle. Or, au XXIe siècle, la valeur se crée sans présence physique sur le territoire. On ne peut donc pas continuer d'alourdir les taxes et impôts sur les entreprises ayant une présence physique sur notre territoire, sur les entreprises manufacturières européennes, car cela ruinera ces dernières au profit d'entreprises chinoises ou américaines implantées ailleurs. Pour des raisons tant d'intérêt national que de justice, je ne peux pas l'accepter.

Certaines entreprises de ce secteur - je ne citerai pas de nom, mais tout le monde voit desquelles je parle -, qui engrangent chaque année en France un chiffre d'affaires de plusieurs milliards d'euros et ont des dizaines de millions de clients français, ne paient, parce qu'elles n'ont pas de présence physique en France - peu de salariés, pas d'usine -, que quelques millions d'euros au titre de l'impôt sur les sociétés. C'est injuste et inefficace pour financer les biens publics.

Nous avons donc voulu combler ce vide fiscal, remédier à l'absence de juste taxation des entreprises n'ayant certes pas de présence physique en France, mais des clients, un chiffre d'affaires et des profits. La taxation de ces entreprises est un enjeu majeur de notre siècle.

Cela n'est d'ailleurs pas seulement vrai pour le numérique ; les profits des entreprises seront de plus en plus dématérialisés. Demain, la valeur d'une voiture résidera essentiellement, non pas dans sa carrosserie ou dans ses roues, mais dans les données qui alimenteront son système de guidage autonome. Il en va de même pour les boutiques de luxe, dont la valeur réside dans la marque, qui est intangible. Pour certaines entreprises manufacturières, comme Safran, la valeur réside non pas dans ses trains d'atterrissage, mais dans les données générées à chaque atterrissage et qui peuvent être revendues.

Tel est le projet de taxe numérique que nous portons depuis deux ans. Nous avons essayé de le faire adopter à l'échelon européen, et nous étions sur le point d'y arriver, mais quatre États s'y sont opposés - le Danemark, l'Irlande, la Suède et la Finlande. Vingt-quatre États y étaient favorables, mais la règle en matière fiscale étant l'unanimité, nous n'avons pas pu faire aboutir cette taxation. Il y avait pourtant une proposition solide de la Commission ; j'en déduis que nous devons rapidement passer, en matière fiscale, à la règle de la majorité qualifiée.

Ainsi, faute de solution européenne, nous avons conçu cette législation nationale, qui a d'ailleurs été adoptée à l'unanimité par le Sénat et l'Assemblée nationale ; preuve que la prise de conscience de l'enjeu stratégique de cette taxation, tant par les parlementaires que par les Français, est réelle. Je note en outre que des législations similaires sont en cours d'adoption dans d'autres pays, en Espagne, en Italie, en Autriche ou encore au Royaume-Uni, à la fois pour des raisons de justice et d'efficacité fiscale.

Les États-Unis nous ont menacés d'augmenter la taxation sur le vin français. Mais une décision souveraine a été prise et sera donc appliquée, à compter du 1er janvier 2019, aux grandes entreprises numériques, celles dont le chiffre d'affaires mondial est supérieur à 750 millions d'euros. Néanmoins, nous avons trouvé, avec nos amis américains, un accord de principe lors du sommet du G7 de Biarritz. D'une part, nous allons chercher, à l'échelon international, au sein de l'Organisation de coopération et de développement économiques (OCDE), une solution, qui se substituera, avant même sa ratification, à notre législation nationale. D'autre part, si les montants payés en 2019 au titre de notre taxation nationale sont supérieurs à ce qu'ils auraient été sur la base de la taxation internationale, les entreprises concernées toucheront un crédit d'impôt correspondant à la différence. Ainsi, dès lors que la taxation internationale sera adoptée, les entreprises taxées n'auront subi aucun écart d'imposition.

La stratégie française était donc la bonne, car, si les choses bougent aujourd'hui à l'OCDE, c'est parce que la France a adopté cette législation. En effet, les États-Unis craignent une seule chose : la multiplication de taxes nationales partout dans le monde. Les négociations sont difficiles, c'est vrai, mais elles avancent. Nous avons mis en place un groupe de travail France-États-Unis-OCDE afin d'aboutir à un accord international d'ici le début de l'année 2020.

Les choses sont donc simples et nous sommes très ambitieux. Le constat est évident : l'Europe a pris un retard considérable, et il faut le rattraper. Pour cela, notre politique est ambitieuse : il faut, pour garantir notre souveraineté numérique au XXIe siècle, des financements adaptés, une protection solide et une fiscalité juste. Le Président de la République et le Gouvernement s'y emploient depuis deux ans.

M. Gérard Longuet, rapporteur. - Nous voyons se dessiner dans votre déclaration une stratégie et des modalités liées aux responsabilités spécifiques de votre ministère, puisque vous avez développé, fort justement à mon avis, une politique favorable à l'investissement.

Je souhaite vous interroger sur votre stratégie. On pourrait en effet vous reprocher de supposer le problème déjà résolu. Vous voulez investir dans les technologies de rupture, mais la France est un pays de taille moyenne - le marché français représente 4 à 6 % du marché mondial -, et on ne connaît qu'*a posteriori* les technologies qui s'avèrent « de rupture », non *a priori* ; cela pose un problème d'allocation des ressources. Nous ne savons pas par avance ce qui va fonctionner auprès d'un public qui est mondial.

Vous avez évoqué trois sujets de rupture. L'intelligence artificielle est un très vaste sujet, qui fait appel à des moyens considérables. Nous avons, certes, des atouts en la matière, mais ceux-ci sont disputés par les grands acteurs. Il en va de même pour les nanotechnologies. Quant aux technologies quantiques, il ressort de nos auditions qu'un monde nouveau semble s'ouvrir, mais nul ne sait quand il émergera ni jusqu'où il ira. Pourriez-vous donc expliquer davantage ce concept de technologie de rupture ? En effet, Amazon ne représente pas par exemple à proprement parler une technologie de rupture, la technologie en elle-même est assez simple, il ne s'est agi que d'être le premier acteur.

Le capitalisme numérique pose en effet problème, car il repose sur une théorie simple : le gagnant prend tout. On finance pendant une période plus ou moins longue des structures qui perdent de l'argent, jusqu'à ce que celui qui est en position dominante devienne profitable, et alors il « prend tout ». Cette conception, fondée sur la poche la plus profonde, qui n'est, malheureusement pas la nôtre, nous permettra-t-elle de faire face au défi, dans un environnement où les entreprises dominantes rachètent de la technologie pour être sûres de ne pas être dépassées ?

Par ailleurs, le droit européen de la concurrence pose problème. Les acquisitions d'entreprises - start-up, licornes et autres -, qui visent à éradiquer toute concurrence, passent malheureusement sous la limite radar de la politique de contrôle de concentrations. Vous avez raison de croire à l'évidente nécessité d'avoir une stratégie dans une économie dématérialisée, mais on se heurte à la réalité d'une guerre par le financement. L'accès aux capitaux étant moins important en France qu'aux États-Unis, pouvons-nous réussir ? L'argument de la technologie de rupture est, je le répète, très convaincant, s'il n'a le défaut qu'on ne connaît qu'*a posteriori* les succès technologiques. Après tout, d'un point de vue technique, Facebook, ce n'est rien...

Je veux aussi vous demander une précision. Vous avez confiance, vous l'avez indiqué à de nombreuses reprises, en l'effet déstabilisateur des *blockchains*. Vous dites qu'il faut organiser en France ce système

déstabilisant ; cette piste est très intéressante, mais pourriez-vous être plus précis ?

Sur les véhicules autonomes, on mesure mal à quel point ce système est porteur de grands dangers pour l'économie mondiale du point de vue de la puissance concentrée. La menace d'une prise en main complète de tout un secteur d'activité - transport individuel, collectif, de marchandises - par une entreprise est très lourde, vous avez raison de le souligner.

Enfin, dernière question : jusqu'où peut-on aller pour aider à la localisation en France de l'hébergement des données, au moyen de la fiscalité ou des aides à l'investissement ? On a beaucoup investi dans le réseau - d'ailleurs, l'argent public finance ainsi des autoroutes que d'autres emprunteront et valoriseront-, mais le soutien à l'hébergement des données sur notre territoire est également nécessaire ; jusqu'où peut-on aller ?

M. Bruno Le Maire, ministre. - Commençons par une remarque politique. Dans les années 1960, la France est parvenue à initier des ruptures technologiques majeures et à prendre le leadership sur un certain nombre de technologies ; je pense notamment au nucléaire. Je ne crois pas à la possibilité de revenir à un État qui décide à la place des entreprises, mais nous pouvons, via un environnement fiscal et réglementaire favorable, susciter de nouvelles technologies de rupture dans notre pays, à deux conditions : cela doit venir des entreprises ou des chercheurs, et cela n'est possible qu'à l'échelle européenne. Nous n'y arriverons pas sans le relais de financements européens.

Je ne peux me résigner à l'idée selon laquelle notre avenir serait derrière nous. Nous avons manqué d'ambition, nous avons fait des erreurs, c'est vrai, mais nous pouvons reprendre la maîtrise des technologies de rupture. Prenons l'exemple du spatial : on me soumet de nombreuses notes indiquant que le lanceur renouvelable n'a aucune chance, qu'il ne faut surtout pas s'y engager, mais les États-Unis l'ont fait au moyen d'un appui public massif, et ils mettent ainsi nos lanceurs spatiaux en difficulté. Donc, cessons de regarder les trains passer et donnons-nous les moyens de maîtriser les technologies de rupture. Sinon, que ce soit dans le domaine du spatial, des biotechnologies, de l'intelligence artificielle, des véhicules autonomes ou des batteries électriques, nous perdrons tant notre puissance économique que notre souveraineté. Il est tout à fait possible de reprendre la main. La question est : comment ?

Je ne déciderai pas personnellement quelles sont les technologies de rupture pertinentes, je n'en sais rien, mais nous avons en France des ingénieurs, des chercheurs, des industriels qui, eux, le savent. Il faut s'appuyer sur notre réseau d'entreprises et identifier nos forces. Atos est l'un des leaders mondiaux en matière de calcul quantique. En matière de nanotechnologies, STMicroelectronics, située près de Grenoble, est parmi les meilleures entreprises du secteur et fournit ses composants à tous les grands

acteurs du numérique. En matière de biotechnologies, nous avons également des entreprises d'excellence. Appuyons-nous donc sur notre excellent tissu industriel.

En outre, le Fonds pour l'innovation de rupture repose sur des personnalités indépendantes, des chercheurs, des industriels, qui font eux-mêmes les propositions. Cela doit aussi correspondre à l'intérêt général et aux préoccupations sociétales. J'en donnerai trois exemples. Je pense, en premier lieu, à l'amélioration des diagnostics médicaux au moyen de l'intelligence artificielle, qui nous concerne tous. Les diagnostics seront plus rapides et plus sûrs ; c'est déjà financé par le fonds. Je pense, en deuxième lieu, à la certification des systèmes qui ont recours à l'intelligence artificielle ; le biais de sélection des algorithmes pose un problème démocratique : pourquoi M. Longuet, M. Montaugé et M. Le Maire reçoivent-ils chacun des nouvelles différentes sur leur téléphone ? Je pense, enfin, à l'automatisation de la cybersécurité : au lieu d'intervenir quand il y a eu une attaque ou de mettre à jour son système tous les deux mois, il faut une lutte automatique et permanente contre les attaques.

Je n'ai donc pas la prétention de définir quelles sont les technologies de rupture pertinentes ; le fonds est animé par des ingénieurs, des chercheurs et des industriels plus à même que moi de le faire. Il nous faut également nous appuyer sur notre réseau industriel existant et sur nos domaines d'excellence, dans lesquels on peut déjà créer des ruptures.

Cela dit, il y a encore des besoins importants de rationalisation en matière de soutien à l'innovation. Entre le programme pour l'innovation d'avenir, le Fonds pour l'innovation de rupture et le plan *Deep tech* de la Banque publique d'investissement (BPI), il faut rationaliser. Il existe trop de canaux de financement, ce qui nuit à leur efficacité.

En ce qui concerne le droit de la concurrence, je suis entièrement d'accord avec vous, monsieur le rapporteur. Le risque majeur provient du fait que la capitalisation boursière des géants du numérique dépasse largement le produit national brut de 90 % des pays de la planète. Il faut donc mieux sanctionner les comportements anticoncurrentiels et la prédation, et mieux contrôler les concentrations. Cela fait partie des sujets majeurs à porter à l'échelon européen au cours des années qui viennent : il faut renforcer le droit de la concurrence pour lutter contre les comportements prédateurs des géants du numérique. Cela passe aussi par la régulation des contenus, avec notamment la loi sur la manipulation de l'information et la proposition de loi sur le retrait des propos haineux.

Enfin, en ce qui concerne la régulation des plateformes, j'ai engagé des actions en justice contre Amazon, Google et Apple, pour des pratiques commerciales abusives. Obliger un client à installer sur son matériel tel ou tel logiciel, c'est abusif. Contractualiser avec des PME et résilier son contrat du jour au lendemain sans respecter le droit économique, c'est également

abusif. Or il incombe au ministre de l'économie de faire respecter l'ordre public économique, qui ne connait pas l'extraterritorialité et qui doit valoir pour tous. Du reste, ce que nous avons fait pour Facebook est efficace, et j'espère que cela conduira les entreprises concernées à changer leur comportement.

L'entreprise Amazon s'est beaucoup plainte de la nouvelle taxation et a elle annoncé qu'elle la répercuterait à la hausse sur ses PME clientes, mais j'espère qu'elle répercutera aussi la baisse de l'impôt sur les sociétés.

La blockchain est un dispositif électronique d'enregistrement partagé reposant sur un système de confiance mutuelle. C'est un projet très prometteur, dans lequel je crois et sur lequel nous pouvons être leaders. Nous avons défini un cadre juridique, prévu un financement et identifié trois secteurs industriels spécifiques, dont l'agroalimentaire et l'énergie. Deux députés travaillent particulièrement sur cette question : Jean-Michel Mis et Laure de la Raudière.

Vous le savez, les hébergeurs font l'objet de critiques en ce qui concerne leur consommation d'énergie, mais ce secteur est créateur d'emplois et de valeur. Nous avons donc tout intérêt à disposer d'acteurs nombreux et puissants en France. C'est pourquoi nous avons mis en place un avantage fiscal sur la taxe intérieure sur la consommation finale d'électricité (TICFE). Son taux est ainsi passé de 22,5 euros le mégawattheure à 12 euros. Notre objectif est de rendre ce secteur attractif ; c'est une question de souveraineté et de maîtrise des données, même si cette seule réponse n'est pas suffisante face aux législations extraterritoriales, dont nous parlions tout à l'heure. J'ajoute que nous avons demandé aux hébergeurs, en contrepartie et par souci environnemental, de nous faire des propositions en vue de réduire leur consommation d'énergie.

M. Patrick Chaize. - Monsieur le ministre, vous avez évoqué le lancement d'une réflexion sur la création d'une monnaie numérique publique, alors que des acteurs privés prennent déjà des initiatives. Ne risquons-nous pas d'arriver après la bataille ?

En ce qui concerne la taxe GAFA, ne pourrions-nous pas nous inspirer de ce qui existe pour d'autres réseaux comme les autoroutes - ne parle-t-on pas d'autoroutes de l'information ? -, c'est-à-dire mettre en place une forme de péage sur les débits transités, quitte à ce que la taxe nationale soit perçue via les opérateurs assurant ce transit ?

Enfin, vous avez parlé de vainqueur-vaincu et vous avez évoqué le risque d'utiliser des équipements étrangers, mais, en ce qui concerne les infrastructures, la France a choisi de faire appel au secteur privé. C'est aussi un sujet de souveraineté numérique. Vous le savez, je suis très attaché aux réseaux d'initiative publique. Or des arbitrages restent à prendre en ce qui concerne la fin du financement du plan Très haut débit : 3,3 milliards d'euros ont déjà été engagés, il manque entre 500 et 700 millions pour le compléter. Il

serait particulièrement dommage de ne pas laisser aux collectivités locales la maîtrise d'infrastructures qui participent de la souveraineté numérique. Quelles sont les intentions du Gouvernement pour financer le plan Très haut débit ?

M. André Gattolin. - J'aurai une première question de détail. Vous avez évoqué trois secteurs industriels identifiés par le Gouvernement en ce qui concerne la *blockchain*, mais vous n'en avez cité que deux. Quel est le troisième ?

Par ailleurs, vous avez dit au sujet des technologies de rupture que, sans le relais des financements européens, nous n'y arriverions pas. Or l'article 107 du traité sur le fonctionnement de l'Union européenne permet un certain nombre de dérogations en ce qui concerne les aides d'État. C'est par exemple dans ce cadre que deux projets importants d'intérêt européen commun (Piiec) ont été décidés, l'un dans le secteur de la microélectronique, l'autre dans celui des batteries de dernière génération. La France participe à ces deux projets. J'ai présenté avec plusieurs collègues de la commission des affaires européennes du Sénat un rapport d'information sur la question de l'intelligence artificielle, dans lequel nous proposions notamment de laisser la possibilité aux États de compléter les financements européens dans ces secteurs stratégiques. Pensiez-vous que ce type de levier soit judicieux ?

Enfin, en matière de cybersécurité, nous savons que le monde économique peut constituer une cible, en dépit du travail remarquable de l'Agence nationale de la sécurité des systèmes d'information (Anssi) pour accompagner les entreprises. Disposons-nous d'une évaluation du risque systémique en cas d'attaque globale sur un ou plusieurs grands acteurs économiques français ? Existe-t-il un plan de secours en la matière ?

M. Rachel Mazuir. -Certes, l'Europe est parfois divisée, mais elle n'en constitue pas moins un grand marché - on pourrait presque parler d'un marché de Cocagne pour les géants du numérique... Est-il encore possible de construire un ou plusieurs champions européens du numérique qui soient capables de concurrencer les acteurs américains ou chinois ?

M. Franck Montaugé, président. - Hier, cinquante procureurs américains ont lancé une procédure antitrust contre Google. La question de l'hégémonie de certains GAFA constitue donc bien une préoccupation aux États-Unis, alors que, dans le même temps, le droit européen de la concurrence empêche l'émergence d'acteurs de taille européenne ou mondiale. Il me semble indispensable que cette situation évolue. Quelle est la position du Gouvernement en la matière ?

Par ailleurs, la France a récemment quitté le *World Wide Web Consortium* (W3C). Le Gouvernement est-il toujours favorable à la multilatéralisation de l'Icann, l'*Internet Corporation for Assigned Names and Numbers* ? Il me semble que la présence de la France dans les organismes qui

contribuent à la gouvernance du monde numérique est particulièrement importante.

M. Bruno Le Maire, ministre. - En ce qui concerne la monnaie numérique publique, je souhaite que les choses avancent rapidement et nous devrions lancer la réflexion dont je vous parlais dès octobre prochain. En ce qui concerne Libra, je vous ai fait part de notre préoccupation, mais cela signifie aussi que nous agissons. Le rôle des ministres des finances du G7 est de prendre des décisions en la matière pour éviter qu'une monnaie digitale vienne concurrencer les monnaies souveraines.

Monsieur Chaize, vous avez parlé de taxe GAFA, je préfère parler de taxe « numérique », car cette taxe vise les activités digitales et ne s'applique pas qu'aux GAFA - elle concerne aussi des entreprises européennes et chinoises. Nous avons réfléchi à un dispositif qui ressemblerait à un péage, comme vous l'évoquez, mais ce serait techniquement compliqué. A partir, de là, trois solutions se dégageaient sur la taxation du numérique.

D'abord, ne rien faire et prendre acte de la perte d'une recette fiscale, ce qui serait finalement le plus simple. Pour moi, ce serait accepter un scandale : la réallocation des profits que les géants du numérique font sur des clients français au profit d'États dont le niveau de taxation est inférieur à celui de la France - je pense évidemment à l'Irlande. La situation actuelle est tout bonnement révoltante et nous devons y mettre un terme, car je suis convaincu que le moins-disant fiscal signifie la fin de l'Europe ! Je l'ai d'ailleurs dit très clairement à nos amis irlandais. J'insiste, c'est la convergence fiscale qui constitue l'avenir de l'Europe. Arrêtons de nous faire la guerre entre nous et ne renonçons pas à nos services et biens publics ! Le dumping fiscal ne correspond pas à l'idée que je me fais de la construction européenne et je me battrai pour une taxation minimale en Europe. Si un pays applique un taux réel d'impôt sur les sociétés inférieur à ce taux minimum, nous devons récupérer la différence. C'est une question de justice et d'efficacité. Vous l'aurez compris, cette première solution - ne rien faire - n'est pas la mienne !

La deuxième solution repose sur les prix de transfert. C'est un sujet technique, mais il s'agit au fond de négocier avec les entreprises concernées des accords bilatéraux pour qu'elles allouent une partie de leurs profits à l'État. Cette solution serait un premier pas, mais elle est difficile à mettre en place, dépend de négociations avec chaque entreprise et n'est pas, à mon sens, assez ambitieuse, car elle ne règle pas le problème de fond.

La troisième solution, celle sur laquelle nous travaillons, c'est un accord international au sein de l'OCDE. Établir une imposition pour une entreprise qui n'a pas ou peu de présence physique dans un État n'existe pas aujourd'hui. Toute la difficulté réside dans l'établissement du lien, ce qu'on appelle aussi le *nexus*, entre l'activité physique d'une entreprise dans un pays - centre de recherche, salariés, laboratoire, usine... - et son activité

commerciale ailleurs. Pour établir ce lien, nous travaillons sur trois critères : le niveau de profitabilité, le nombre de clients - certaines entreprises du numérique ont des millions de clients en France, mais seulement quelques dizaines de salariés... et les dépenses intangibles, comme le marketing. Finalement, cela ne concerne donc pas seulement les entreprises du numérique, mais toutes les activités qui n'ont pas de présence physique dans un État.

C'est ce choix que nous avons fait au sein de l'OCDE. Un tel dispositif entraînera une redistribution fiscale très lourde, de plusieurs milliards de dollars. Ceci nécessite une évaluation très précise, ce qu'a récemment mis en avant la Cour des comptes, mais c'est la seule solution de long terme pour taxer les activités digitales.

En ce qui concerne la 5G, la loi visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles a été promulguée le 1er août dernier. Je rappelle qu'elle ne vise pas un équipementier en particulier, mais bien à garantir le respect de notre souveraineté. Nous nous sommes ainsi dotés d'un nouvel instrument juridique de contrôle des équipements de télécommunication. Il faut savoir que la 5G est très différente de la 4G. La 5G n'est pas une simple amélioration de la 4G, elle opère une transformation systémique des réseaux, puisque les données sensibles sont stockées dans chaque antenne relais et non au coeur des réseaux. Cela justifie que nous nous dotions de moyens de contrôle renforcés.

M. Patrick Chaize. -Ma question portait en fait sur le plan Très haut débit et la manière dont le Gouvernement entend le financer.

M. Bruno Le Maire, ministre. - Je suis élu d'un territoire rural et j'ai été ministre de l'agriculture ! Je vous le dis donc très clairement : l'engagement du Président de la République d'assurer une couverture universelle de la France en 2020 et un très haut débit pour tous en 2022 doit être tenu. L'intendance suivra ! D'ailleurs, la question se pose d'abord en termes de déploiement, plus qu'en termes financiers. Nous avons déjà investi 3,3 milliards d'euros et le Premier ministre a annoncé en décembre 2018 une enveloppe supplémentaire de 620 millions d'euros.

Je reviens quand même un instant sur la 5G et j'insiste sur la rupture technologique qu'elle constitue. Les informations ne sont plus situées uniquement dans les coeurs de réseau, mais aussi dans les antennes relais, ce qui nous amène à renforcer les protections.

Le troisième secteur industriel qui a été identifié en termes de blockchain est la construction.

Au sujet de la politique européenne de la concurrence, les Piiec sont vitaux pour nous permettre de financer à hauteur raisonnable des projets qui ne sont plus à l'échelle nationale Pour les batteries électriques, la France a engagé 700 millions d'euros, l'Allemagne 1,2 milliard, la Pologne - elle est

spécialisée dans le retraitement des batteries - nous a rejoints et un financement européen complétera cette enveloppe. Plusieurs dizaines d'entreprises privées sont parties prenantes au projet et une première usine pilote devrait voir le jour, en France, l'année prochaine. Sur les nanotechnologies, nous avons mis 800 millions d'euros sur la table et l'Europe 100 millions. L'Europe financera le secteur des supercalculateurs à hauteur de 500 millions d'euros.

Au-delà des montants financiers, ce qui est important, c'est la rupture idéologique, qui était tant attendue. Si nous avions eu ces projets d'intérêt collectif européen il y a une quinzaine d'années, nous aurions aujourd'hui une industrie européenne du panneau solaire. À l'époque, le choix a été différent - ni aide d'État ni subvention -, si bien que nous importons massivement des panneaux solaires chinois, qui sont eux-mêmes subventionnés ! Cette fois, l'Union européenne fait le bon choix. Alors, est-ce trop tard ?

Il s'agit d'abord d'une question d'indépendance, notamment pour notre industrie automobile qui représente des centaines de milliers d'emplois en Europe. Je vous laisse imaginer le levier stratégique dont disposerait la Chine, si nous la laissions seule sur le segment des batteries... Nous serions dans une situation intenable. En outre, la maîtrise de la technologie des batteries ion-lithium, tant liquides que solides, nous permettra de nous assurer que leur retraitement est respectueux de l'environnement.

Je crois que nous devons faire la même chose avec l'intelligence artificielle. J'y travaille avec mon homologue allemand et nous ferons des propositions dans les mois qui viennent, sur le modèle de ce qui a été fait pour les batteries électriques.

La cybersécurité constitue naturellement une préoccupation majeure pour le secteur financier, le risque premier étant une attaque cyber contre les banques centrales. Dans le cadre du G7, nous avons procédé à un exercice de protection contre des attaques cyber sur les banques centrales et nous aurons un plan d'action à notre disposition à la fin de l'année 2019.

Monsieur Mazuir, je reprendrai votre expression, très juste, d'un marché de Cocagne pour les acteurs du numérique... Pourtant, nous devons avoir conscience que l'Europe n'est pas en position de faiblesse. Des erreurs ont été commises dans le passé ; par exemple, nous ne nous sommes pas assez intéressés à la question clé du financement, du capital-risque et nous nous sommes trop reposés sur des prêts. Mais nous sommes le marché le plus riche et le plus intégré de la planète avec 450 millions de consommateurs et je peux vous garantir que pour les acteurs du numérique nous sommes vitaux. De ce fait, si nous rassemblons nos forces, nous avons les moyens de peser dans les débats.

Est-il encore possible de construire des champions européens du numérique ? Je le crois, mais pas dans les secteurs déjà occupés. Nous ne

partons pas de rien ; certaines de nos entreprises sont des leaders dans leur secteur et nous devons les aider à grandir : OVH dans le cloud, Atos dans le calcul intensif, Dassault Systèmes, une entreprise extraordinairement performante en matière d'intelligence artificielle, etc.

Monsieur le Président, la réaction américaine que vous évoquez montre bien qu'il existe aux États-Unis un débat sur l'antitrust et les risques de concentration excessive de la part des champions du digital. Ce débat n'est pas seulement politique, il est aussi juridique, puisque des procureurs ont lancé des procédures contre Facebook et Google.

En ce qui concerne le retrait du W3C, c'est Orange qui a pris cette décision, pas l'État. Nous attachons évidemment une grande importance aux efforts de normalisation dans le domaine du numérique et, plus largement, de promotion des technologies françaises et européennes dans les secteurs clés. D'ailleurs, je souhaite que nous rénovions la stratégie française de normalisation. C'est un effort public et privé, dans lequel les entreprises doivent prendre leur part. C'est une question décisive.

Dernier point, je le redis, je suis persuadé que l'Europe ne disposera pas de grands acteurs dans le secteur du numérique si elle ne révise pas sa politique de la concurrence. Une nouvelle commission européenne est en train de se mettre en place. La France et l'Allemagne vont rappeler à nouvelle Présidente, Ursula von der Leyen, les propositions qu'elles ont déjà formulées et qui partent de trois idées simples : autoriser certains projets, quitte à mettre en place des contrôles *ex post* et à prévoir des ajustements au bout de quelques années pour maintenir un bon niveau de concurrence - procéder ainsi dans le dossier Alstom-Siemens, qui aurait pu devenir le champion mondial de la signalisation ferroviaire, aurait été beaucoup plus intelligent qu'une interdiction *a priori* -, retenir le monde comme marché pertinent, et pas seulement l'Europe, prévoir que le Conseil européen ou le Conseil de l'Union européenne puissent s'opposer à une décision de l'autorité de la concurrence, comme le Gouvernement peut le faire au niveau national en France et en Allemagne.

Ce point de l'ordre du jour a fait l'objet d'une captation vidéo qui est disponible en ligne sur le site du Sénat.