ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Compte rendu

Mission d'information de la Conférence des Présidents « Bâtir et promouvoir une souveraineté numérique nationale et européenne »

Jeudi
15 octobre 2020
Séance de 9 heures

Compte rendu n° 5

SESSION ORDINAIRE DE **2020-2021**

Présidence de M. Jean-Luc Warsmann, *Président*

ASSEMBLÉE NATIONALE

Audition, ouverte à la presse, de M. Henri Verdier, ambassadeur pour le numérique

La séance est ouverte à 9 heures 05.

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. J'ouvre la séance.

M. Philippe Latombe, rapporteur. Nous sommes heureux d'accueillir aujourd'hui parmi nous notre ambassadeur pour le numérique, M. Henri Verdier. Monsieur Verdier, vous avez été nommé à ce poste en 2018 et votre mission consiste, je cite, à « *coordonner l'élaboration des positions de la France sur les questions internationales touchant la transformation numérique et à les promouvoir auprès de nos partenaires internationaux comme auprès des autres acteurs publics et privés* ». Notre mission d'information va, durant plusieurs mois, se pencher sur les moyens de bâtir et de promouvoir une souveraineté française et européenne. Nous souhaiterions connaître votre analyse de cette notion de souveraineté numérique, notamment la pertinence de l'échelon européen pour œuvrer à son développement. Nous sommes également intéressés par les conditions concrètes d'exercice de votre mission, les enceintes d'intervention, l'existence d'homologues dans les pays partenaires versus une spécificité typiquement française. La politique étrangère de la France en matière de numérique recouvre un grand nombre de questions essentielles telles que la cybersécurité, la neutralité d'internet, la protection des données personnelles, la lutte contre les *fake news* ou les discours de haine, le multilatéralisme ou encore la souveraineté européenne du numérique. Comment participez-vous à l'élaboration des politiques françaises sur ces différents sujets ? Et quelle est la coordination des différents services de l'État sur ces problématiques ?

Votre position contribue à la dimension croissante de l'action internationale de la France dans le domaine du numérique. Pouvez-vous nous rappeler sur quels principes généraux elle se fonde et les valeurs qui la guident ? Est-il de votre ressort d'assurer une cohérence au regard des multiples problématiques présentées et des divers canaux empruntés pour cette action ? Le numérique est en effet riche de sujets diversifiés présentant parfois des enjeux majeurs au regard de la place de la France sur la scène internationale, en particulier en matière de cybersécurité et de cyberdéfense. Dans ces domaines, la thématique de la souveraineté est prégnante puisqu'il s'agit de déterminer comment protéger les intérêts français de nouvelles menaces immatérielles et déterritorialisées. L'objectif est également de définir de nouvelles modalités de discussion avec nos partenaires, notamment européens, afin d'engager des actions concertées respectueuses de la souveraineté de chacun. Nous souhaiterions connaître la position de la France sur ce sujet, les enceintes de discussions autour de ces enjeux sécuritaires, ainsi que les partenaires privilégiés – l'Europe est-elle unie ? – et les principales négociations en cours dans les enceintes multilatérales.

La souveraineté numérique française et européenne est également confrontée, selon un mode sans doute moins conflictuel, à la montée en puissance d'acteurs privés qui prétendent imposer leurs normes et/ou disposent d'un pouvoir de marché les rendant souvent incontournables pour les consommateurs et les usagers. Comment, selon vous, la France et l'Europe peuvent-elles reprendre la main dans ces rapports nouveaux afin de ne pas être réduites à une situation seulement réactive, voire passive ? Nous pourrons ici évoquer les instances privées ou semi-privées où s'organise la gouvernance d'internet (pour l'attribution des noms de domaine par exemple). Nous pourrons discuter également des géants du numérique de plus en plus souvent prescripteurs, tant de nos modes de consommation que de

nos modes d'information. La crise que nous connaissons ne fait que renforcer ces tendances. Quelle réponse publique apporter, selon vous, au plan national, européen et international ?

Enfin, la défense de la souveraineté numérique passe également par une certaine autonomie matérielle et par la défense et la promotion d'une industrie du numérique européenne, compétitive et indépendante. Or, l'Europe souffre de départs d'industries stratégiques pour le matériel informatique qui constitue pourtant le sous-bassement du développement du numérique. La dépendance aux solutions technologiques extracommunautaires, logicielles comme matérielles, met-elle selon vous en cause l'autonomie européenne ? Comment contrer ces tendances et comment faire participer l'innovation et la recherche à une forme de réindustrialisation dans les nouvelles technologies, afin d'assurer une plus grande souveraineté européenne ? Pourriez-vous revenir sur cet aspect de la diplomatie économique qui pourrait s'attacher à votre mission ?

Je vous laisse la parole et vous remercie d'avance pour vos réponses.

M. Henri Verdier, ambassadeur pour le numérique. Je vous remercie pour le vaste programme que vous proposez. Je vais répondre aux différentes questions posées. Hier, nos équipes ont échangé sur la base d'un conducteur que je vous invite à suivre. Dans un premier temps, j'évoquerai la diplomatie numérique et les attributions de l'ambassadeur pour les affaires numériques et aborderai la notion de souveraineté numérique que la France propose à l'Europe.

Avec le recul historique, il apparaît que les acteurs de la révolution industrielle d'il y a trois siècles ont exercé une domination durable sur l'ordre du monde, pour son bien (le progrès) ou son mal (la domination). Aujourd'hui, nous assistons à une nouvelle révolution industrielle et certains pays savent que leur destin, dans les trois prochains siècles, se joue dans la maîtrise de cette technologie. La transformation des modes d'échanger, commercer, apprendre justifie selon moi cette appellation de nouvelle révolution industrielle. Nous assistons à une course à l'hégémonie. Vous avez, monsieur Latombe, évoqué la plupart des dimensions de la souveraineté numérique, nous les compléterons en chemin. Ces dimensions sont très concrètes. Lors de l'attentat terroriste de Christchurch, en Nouvelle-Zélande, Facebook s'est interrogé pendant des heures sur la définition de terrorisme. À l'époque, les États-Unis ne reconnaissaient pas encore le *violent extremism* d'extrême droite comme du terrorisme et aucune définition internationale consensuelle du terrorisme n'existait.

Je rappelle que 90 % des applications de nos smartphones ont accepté les conditions de service d'Android et Apple, peut-être de Facebook Connect et Paypal, et certainement de Google Maps. Ces applications peuvent donc subir, du jour au lendemain, des modifications de leurs conditions de service. Par exemple, Google Maps a, en 2018, changé les tarifs de son interface de programmation d'application (*Application Programming Interface-API*) en les multipliant par 100 pour certains utilisateurs. Lorsque j'étais que DSI (directeur interministériel du numérique et du système d'information et de communication) de l'État, j'ai vu à l'époque des sous-préfectures fermer des sites, car elles n'étaient pas en mesure de les financer à hauteur de 3 000 euros par an. Cette situation crée de la vulnérabilité et une asymétrie, puisqu'à tout moment, les plateformes telles que Facebook Connect, Paypal ou Google Maps, en savent plus que la start-up à l'origine de l'application. La start-up n'a donc aucune chance de renverser le pouvoir de force. Je prends comme autre exemple les élections américaines. Leurs campagnes sont structurées par la publicité ciblée. Certains candidats vont dépenser jusqu'à un demi-milliard de dollars pour utiliser une base de données présentant 50 informations pour 200 millions d'Américains. Ainsi, 3 000 à 4 000 messages cibleront différents profils. D'après les sociologues, cette fragmentation de la vie publique n'est pas sans rapport avec la montée de la violence. En Europe, la publicité politique est

encadrée, le financement des campagnes est limité et la vie privée protégée. Mais des forces privées sous-entendent que ce modèle est dépassé. Ces exemples illustrent le caractère très concret de problématiques qui relèvent du choix du peuple souverain, tant pour les campagnes politiques qu'au sujet de la vie privée ou de l'*open data*.

Venons-en au rôle d'ambassadeur pour les affaires numériques. La révolution numérique détermine désormais lourdement la prospérité et la souveraineté des États, car elle est devenue un objet géopolitique important qui caractérise les relations entre États. Le droit du conflit et le droit humanitaire doivent quant à eux faire place à la question cyber. Par exemple, la guerre commerciale entre la Chine et les États-Unis détermine très lourdement l'avenir de l'économie mondiale et du numérique. En outre, les pratiques d'ingérence territoriale deviennent l'arme du pauvre et se répandent rapidement. Nous reviendrons sur l'Appel de Paris ou sur le partenariat mondial pour l'intelligence artificielle qui sont des coalitions d'initiative française instaurées afin de créer du dialogue entre États et faire émerger des réponses et des solutions. La révolution numérique pèse sur les relations internationales et pourrait amener les États à détruire la liberté d'entreprendre ou la liberté d'accès à la connaissance qui sont propres à la révolution numérique. La France doit peut-être rappeler que la révolution internet est celle d'innovateurs et d'entrepreneurs et qu'elle doit beaucoup à sa composition décentralisée, peu contrôlée, hostile au monopole. La ligne de force de la France repose sur la défense d'un internet libre, ouvert, sûr et unifié. Une fragmentation en internets régionaux à l'échelle du monde doit être évitée, car elle constituerait une mauvaise nouvelle pour l'économie, mais également pour la paix mondiale. En effet, l'accès à des informations par bloc continental engendrerait un affaiblissement de la compréhension mutuelle entre espaces géopolitiques et un accroissement des tensions.

Le numérique est, pour toutes raisons, devenu un objet diplomatique. Lors de ma prise de fonction au Quai d'Orsay, j'ai tenté de cartographier le territoire de la diplomatie numérique en dessinant une boussole représentant le périmètre de la diplomatie numérique. Le rapport d'activité correspondant est en ligne sur le site du Quai d'Orsay. Au sein du Quai d'Orsay travaillent cinquante responsables de différents dossiers numériques. Quatre sont responsables des négociations sur le droit international dans le cyberespace, deux sont en charge des retraits de contenus terroristes, une jeune femme a inventé le visa Start up, d'autres responsables traitent de l'aide au développement, de la politique culturelle, de la promotion de la francophonie, *etc*. La première mission de l'ambassadeur pour les affaires numériques est de donner une cohérence à une diplomatie numérique inventée pour faire face à un certain nombre d'enjeux. Notre boussole présente quatre axes.

Le premier concerne les enjeux de sécurité, de cybersécurité (sécurisation des infrastructures), de lutte contre les contenus étrangers hostiles, voire des contenus terroristes ou pédopornographiques qui appellent des décisions internationales. La France souhaite séparer la question de la protection des infrastructures de celle de la régulation des contenus. Certains pays ont au contraire pour stratégie une doctrine globale de guerre informationnelle qui rapproche ces deux dimensions. Dans le domaine de la cybersécurité, la France est très présente dans les instances onusiennes, dans des dialogues bilatéraux avec des alliés ou non alliés, dans la régulation des contenus avec des pays européens ou non européens. Le dialogue reste encore à inventer avec les grandes plateformes. La France s'implique fortement dans la gouvernance d'internet qui concerne pas moins de dix-sept instances qui ont vocation à standardiser et normaliser. L'ambassadeur pour les affaires numériques tient le siège de la France à l'ICANN (*Internet Corporation for Assigned Names and Numbers*) en charge du nommage internet, à l'*Internet Governance Forum* (que la France encourage à réformer pour émettre des préconisations), à l'OCDE (Organisation de coopération et de développement

économiques), lorsque ce n'est pas Bercy, ainsi qu'au sein du G20, du G7 et d'un certain nombre d'institutions européennes.

Un deuxième axe de la boussole concerne les enjeux de diplomatie économique en lien avec le ministère de l'économie et des finances. Notre réseau diplomatique est au contact des French Tech. Le ministère de l'économie représente la France à l'OCDE dans les négociations sur la fiscalité du numérique. Il peut encourager des entreprises françaises dans leurs négociations avec de grands États. Enfin, dans le cadre de la diplomatie d'influence que j'appelle diplomatie de valeurs, la France défend depuis longtemps l'accès à la culture et à l'éducation, la liberté d'expression, la liberté de la presse, le développement des pays émergents, mais également, par exemple, la net-neutralité. Avec la révolution numérique, les politiques et les logiques d'action doivent évoluer, notamment pour défendre la francophonie ou réfléchir aux aides de l'Agence française de développement (AFD), et ce sans tomber dans la dépendance d'une grande puissance ni d'une grande entreprise. Nous accompagnons ces évolutions de politiques avec de beaux opérateurs tels que l'AFD ou l'Institut français.

Au centre de la boussole se trouve la fonction centre d'expertise. Nous sommes effectivement souvent la première équipe ayant la capacité technique pour effectuer des analyses sur la Libra (monnaie virtuelle), la blockchain (technologie de stockage et de transmission d'informations) ou l'IA (intelligence artificielle). Ces fonctions existent dans tous les pays homologues développés, mais elles sont rarement unifiées. En Allemagne, j'ai depuis quelques semaines une homologue directe qui est une ambassadrice numérique *at large*. Le *Tech Ambassador* danois était globalement sur le même périmètre, mais il envisageait de négocier avec les géants de la technologie quand la France les considérait non comme des États souverains, mais comme des forces économiques. Certes, de tels acteurs doivent faire partie de la solution, mais nous n'avons pas d'ambassade auprès des GAFA et ces derniers ont à New-York des bureaux commerciaux et non des ambassades. Hormis en Allemagne et en Suède, les compétences homologues sont fragmentées. Le réseau de la diplomatie cyber est pour sa part clairement identifiable. Il est composé d'ambassadeurs ou de hauts diplomates cyber et d'une représentation des pays dans la gouvernance d'internet. Cette dernière n'est pas toujours confiée aux affaires étrangères, elle peut relever du ministère de l'économie, de l'industrie, voire du ministère de l'intérieur pour les contenus à caractère terroriste.

Ce poste d'ambassadeur du numérique a une petite historicité. La diplomatie française était présente depuis une dizaine d'années dans la gouvernance d'internet et dans les sujets d'Open Gov (*Open Government Partnership*) et de cyber-négociation. Des responsables étaient en charge des différents dossiers. Puis, avec mon prédécesseur David Martinon, l'ambassadeur est devenu thématique, et nous continuons à muscler cette fonction. J'ai le privilège d'avoir une petite équipe de cinq collaborateurs, dont Louis-Victor de Franssu ici présent. Ils permettent de mettre en musique le travail des cinquante responsables du numérique au sein du Quai d'Orsay et d'avoir une approche matricielle. La lettre de mission que vous trouverez en ligne me donne la tâche de coordonner et représenter les positions françaises. Mais l'organisation du Quai d'Orsay est matricielle, avec éventuellement, pour chaque question numérique, un directeur géographique et un directeur thématique dont les apports sont importants. Notre travail consiste donc à sécréter une intelligence collective. Nous travaillons quotidiennement avec la direction de l'action stratégique et du désarmement, la direction des Nations unies, la direction générale de la mondialisation ou encore la direction de l'Union européenne. Le travail est conséquent à l'intérieur du quai d'Orsay, mais il est également interministériel pour chaque axe de la boussole.

Je travaille également au quotidien, selon les dossiers, avec le ministère de l'économie et des finances, le SGDSN (Secrétariat général de la défense et de la sécurité nationale), le SIG

(Service d'information du Gouvernement), le ministère de l'intérieur, le ministère de la justice, le ministère des armées et le ministère de la culture. Je suis disponible pour répondre à vos éventuelles questions à ce sujet. En tant qu'ancien directeur interministériel, j'ai découvert que la coopération des ministères régaliens était parfois plus fluide que les rencontres avec la DINSIC (direction interministérielle du numérique et du système d'information et de communication) dans le cadre de tâches plus civiles. Aujourd'hui, sous la houlette bienveillante du SGDSN, l'action interministérielle semble efficace sur les sujets de sécurité, de cyber, de retrait de contenu terroriste et de lutte contre les ingérences étrangères.

Abordons maintenant la question des enceintes privilégiées d'exercice de ces fonctions. La liste est longue et je transmettrai à la commission une liste exhaustive. De nombreux dossiers sont traités au sein de l'Union européenne comme les retraits de contenu terroriste ou le *Digital Services Act* (DSA) qui sera prochainement scindé en deux actes. Un plan de protection des démocraties est en préparation, un dialogue avec les grandes entreprises passe par le *European Internet Forum*, un groupe travaille sur les menaces hybrides, le service de l'action extérieure de l'Union européenne (SAE) avait souvent le leadership sur les questions d'ingérence, mais nous avons quelque peu modifié cette position. Ainsi, de nombreux enjeux sont traités au niveau européen. D'autres se jouent au sein de l'Organisation des Nations unies (ONU). Par exemple, le dialogue sur la cybersécurité et le consensus sur le droit international sur le cyberespace sont traités par deux groupes de travail. L'un est d'initiative américaine (groupe composé d'experts gouvernementaux) et l'autre est d'initiative russe (groupe à composition illimitée). Ayant observé que les deux groupes avaient fini par se paralyser, nous en proposons un troisième qui sera instauré une fois les travaux des deux groupes actuels finalisés. Le futur groupe de travail unique sera nommé *Program of action* et visera à changer les termes mêmes du débat sur le cyber.

La question de la gouvernance d'internet est très onusienne et nous avons participé aux différents IGF (*Internet Governance Forum*) et aux travaux lancés par le Secrétaire général des Nations unies. Nous pesons pour que l'*Internet Governance Forum*, enceinte multi-parties prenantes, soit renforcé, tranche sur ses propres débats et reconnaisse une place aux États. Si la culture de la *Permissionless Innovation* a bénéficié à internet, nous avons des responsabilités et des prérogatives en tant qu'État. Sans État souverain, la liberté individuelle est moindre, d'autant plus dans un monde de monopoles géants, de surveillance de masse et d'innovation débridée. Nous avons donc des choses à dire. Cette année, l'ICANN a failli prendre une décision qui nous a semblé grave, ce dont vous pouvez prendre connaissance en faisant des recherches sur la Toile. Malgré l'avis négatif quasiment unanime de ses membres, l'ICANN a voulu privatiser le .org et le vendre à un fonds d'investissement prêt à payer 1,5 milliard de dollars, sans pouvoir justifier de l'origine de ces fonds. Ce fonds pensait recruter l'ancien directeur de l'ICANN à l'origine de ce mouvement de privatisation. Le gouvernement français est la seule instance qui a souhaité stopper la démarche. À défaut de pouvoir recourir aux statuts, la France a usé de diplomatie en plaidant, justifiant, posant des questions et en se trouvant des alliés. Le procureur de Californie a joué un rôle clé en signalant que l'organisation qui depuis vingt ans était *non-profit* et donc ne payait pas d'impôts deviendrait sans doute, de par la vente envisagée, *for profit* impliquant le paiement d'arriérés sur vingt ans. Ce point a aussi contribué à empêcher cette vente. Certes, certains acteurs civils ne souhaitent pas que les États interviennent. Mais cet exemple montre que les procédures, la transparence et l'éthique ont été défendues par un gouvernement qui a agi non pas en tant qu'État auquel obéir, mais en tant qu'acteur du débat défendant des positions.

Nous travaillons beaucoup sur le sujet de la cybersécurité au sein de l'OCSE (Organisation pour la sécurité et la coopération en Europe). En outre, de nombreux travaux sont menés avec l'OCDE, en particulier un travail très intéressant sur la responsabilité du

secteur privé dans la cybersécurité. Nous en sommes un peu à l'origine avec l'Appel de Paris sur lequel je reviendrai dans un instant. Nous pensons qu'une sécurité durable ne sera pas créée uniquement avec du droit international. Un internet stable et sûr nécessite une montée en qualité des infrastructures et des services numériques qui sont de la responsabilité des entreprises qui les vendent. Nous travaillons également avec l'OCDE sur les rapports de transparence volontaire que nous nommons rapports d'auto-évaluation. Nous considérons que la réception d'un rapport annuel des entreprises concernant les réseaux sociaux ne suffit plus. Un échange de données est à construire afin de vérifier les éléments selon une approche consensuelle. Nous traitons d'autres dimensions de notre boussole au sein de l'Organisation internationale de la francophonie. Nous sommes présents à l'UIT (Union internationale des télécommunications) où se jouent des enjeux déterminants pour internet. Sur proposition de la société Huawei, un groupe de travail y a été créé pour un nouveau protocole TCP/IP que Huawei trouve plus rassurant, car il est plus clair, centralisé et mieux contrôlé.

Par ailleurs, nous menons des dialogues stratégiques serrés avec différents partenaires internationaux, les États-Unis, le Royaume-Uni, l'Inde, Israël, le Japon ou encore la Russie. Nous participons aux enceintes de discussions des entreprises d'internet telles que l'ICANN, l'IGF ou le GIFCT (*Global Internet Forum to Counter Terrorism*). Le GIFCT est la structure dont se sont dotées les entreprises de la Silicon Valley pour synchroniser les retraits de contenus terroristes une fois flagués. Je rappelle qu'après l'attentat de Christchurch, les tentatives de repostage ont la semaine suivante atteint le million sur Facebook et 400 000 sur YouTube. Une base de données et des outils sont nécessaires pour filtrer très rapidement les messages. Le filtrage se fait après flaguage par la police et retrait une première fois du post, afin d'empêcher sa republication. Suite à l'attentat de Christchurch, la France a plaidé pour et obtenu une réforme profonde de ce GIFCT qui a été doté d'une structure indépendante, d'un directeur dédié et d'un *advisory board* ouvert à cinq États et cinq représentants de la société civile.

Pour illustrer d'autres initiatives françaises, nous avons porté et négocié l'Appel de Christchurch, mon bureau est très présent sur ce sujet. Ainsi, des États, des entreprises et des représentants de la société civile s'organisent pour assurer le retrait des contenus terroristes en ligne. Je suis fier du travail accompli avec la Nouvelle-Zélande, car nous avons construit des règles d'États de droit. Cet Appel a engendré des résultats, notamment la réforme du GIFCT. Chacun a son rôle. Les États ne cherchent pas à supprimer des réseaux les contenus qui ne leur conviennent pas, mais à s'organiser pour détecter et signaler ces contenus. Les entreprises ont le devoir de les retirer en moins d'une heure et d'assurer la transparence. Enfin, la société civile veille à ce que les États légifèrent correctement et respectent les droits de la défense. Ces acteurs peuvent également aider à détecter les contenus terroristes. Aujourd'hui, le bilan est tout à fait positif, un équilibre a été trouvé.

L'Appel de Paris pour la confiance et la sécurité dans le cyberespace a été lancé en 2018. Cette organisation est devenue la plus importante en matière de cybersécurité, 78 États l'ont soutenue ainsi que des *local authorities* (incluant de grandes villes, l'État de Washington et l'État de Californie), 650 entreprises et 350 organisations non gouvernementales (ONG). Cet Appel permet d'illustrer l'unanimité internationale en matière d'application du droit international pour le cyberespace. Nos positions n'étant pas toujours majoritaires à l'ONU, il est précieux de pouvoir afficher le soutien d'entreprises et de la société civile. Ce fonctionnement a permis d'ouvrir un dialogue sérieux sur la responsabilité des acteurs systémiques, puisque la sécurité commence dans le design des solutions et les pratiques quotidiennes.

Bien sûr, la cybersécurité vise à empêcher des puissances étrangères de nous nuire. Mais, elle consiste également à expliquer aux fabricants d'objets communiquant que livrer des objets

ayant pour mot de passe par défaut « adminadmin » est tout simplement criminel. Les hackers savent que tous les utilisateurs ne vont pas changer leur mot de passe et ils en profitent. La divulgation responsable des failles est un autre sujet. Communiquer en conférence internationale sur une faille identifiée au sein d'une entreprise n'est pas un comportement intelligent. L'entreprise concernée doit avoir le temps de corriger la faille et d'implanter un patch.

La question de la souveraineté numérique, notamment européenne, est au cœur de ces problématiques, car notre souveraineté peut être menacée par des puissances étrangères, prise en otage dans des conflits continentaux ou encore menacée par des monopoles économiques. Laure de La Raudière le sait, j'ai créé ma première entreprise internet en 1995. À cette époque la France ne comptait que 15 000 internautes et Google et Facebook n'existaient pas. La révolution internet est porteuse d'émancipation, d'accès à la culture, de capacités de créer et d'innover. Les fondateurs d'internet évoquaient un *people empowerment,* soit un partage de puissance d'action. La souveraineté, pour favoriser ces capacités de créer, doit imposer des règles pour protéger les droits individuels qui sont connectés aux droits collectifs. Le ministre de l'Europe et des affaires étrangères, Jean-Yves Le Drian, s'est emparé de cet enjeu majeur qu'il porte. Vous trouverez en ligne son discours de Prague (décembre 2019) et son intervention à la conférence des ambassadeurs néerlandais (janvier 2020).

Nous pensons que la souveraineté française ne s'entend qu'en harmonie avec une souveraineté européenne. Un des grands combats est de convaincre nos partenaires européens que ce sujet est prioritaire et appelle une réponse politique. Parler de souveraineté numérique et de souveraineté numérique européenne n'était pas une évidence il y a trois ans. Les positions ont évolué. Peut-être la France a-t-elle trop souvent brandi l'étendard de la souveraineté pour défendre des entreprises, proches du pouvoir, en difficulté, ou une pulsion protectionniste. Nous en pâtissons aujourd'hui et devons en tirer les leçons. Toutefois, le fond de l'analyse demeure. Pour être souverain, un pays peut choisir le protectionnisme, derrière un *firewall,* ou l'hégémonie. La France propose une troisième voie qui est celle de l'autonomie stratégique pour prendre nos propres décisions sur la régulation de la vie privée, avoir une politique industrielle, décider d'une doctrine nationale de cybersécurité et interdire certains prestataires. Cette conception n'étant ni protectionniste ni hégémonique, elle ne rivalise avec aucun pays. La France peut ainsi être souveraine avec l'Allemagne ou l'Espagne. Elle peut également montrer aux partenaires en Afrique ou en Amérique latine que ce modèle permet des coalitions et des coopérations. Il est important d'entendre que ce récit de souveraineté est un récit d'autonomie stratégique. Durant ce cycle d'audition, des intervenants confondront peut-être la souveraineté avec l'intégration verticale d'une filière industrielle française. Or, un capital français n'est pas une garantie d'autonomie, car le cadre juridique ou technologique peut engendrer une privation de liberté de manœuvre. La possibilité de changer de prestataires peut tout à fait faire partie d'une stratégie de souveraineté.

Comme l'a dit Jean-Yves, Le Drian, la diplomatie française considère que pour atteindre l'ambition de souveraineté, quatre dimensions sont importantes. La première dimension est la sécurité et la cybersécurité. Vos travaux montreront que le sujet de la souveraineté est souvent né en marge de politique de régulation de la concurrence ou de politique industrielle, et a régulièrement tourné autour des questions de libre-échange et de protectionnisme. De fait, les problématiques liées à la sécurité, traitées au sein d'autres enceintes, sont souvent négligées. Pourtant, un pays qui risque d'être « débranché » en un claquement de doigts ne peut être considéré comme souverain. Un pays qui donne le code source de ses installations électriques à une puissance étrangère n'est pas non plus souverain. L'autonomie en matière de cybersécurité est pour nous la condition première de la

souveraineté. Dans ce domaine, de multiples progrès restent à faire par l'Europe pour se protéger. Circonscrire les discours de haine tout en respectant la liberté d'expression est délicat et impose d'interroger le *business model* de l'économie de l'attention et de la publicité personnalisée. Les *business models* des géants de la Tech doivent être confrontés, mais un État ne peut s'y attaquer seul. La cohérence et la réflexion sont pour cela de mise.

La deuxième dimension est la puissance de création. Dans le domaine du numérique plus qu'ailleurs, les inventeurs donnent le la. Personne n'aurait pensé à réguler le *search* ou les réseaux sociaux avant que ceux-ci n'existent. Les créateurs et les innovateurs sont toujours des forces, mais dans le secteur numérique, ils inventent les territoires mêmes de la régulation. Donc un pays qui ne crée rien est difficilement souverain. Une politique au service de l'innovation, au service de l'entrepreneuriat, au service de la croissance des entreprises est essentielle et indispensable. Je pense que nous partageons le constat d'une nécessaire économie du numérique. J'ajouterais que la puissance de création n'est pas l'apanage des entreprises. Les pays rayonnent et prennent aussi un *leadership via* leurs créations culturelles, l'impact de leurs intellectuels, le poids de leur recherche. En regardant une carte du monde, nous verrions que les pays disposant d'un écosystème numérique digne de ce nom ont notamment développé un cinéma national. En effet, ces pays pensent leur destin selon leurs valeurs et leur culture et ils ont le courage de choisir des chemins. Ainsi, la stratégie de puissance de création peut aussi passer par la culture et la recherche. La puissance californienne réside beaucoup à San Francisco, mais elle est également à Los Angeles. Et l'économie numérique de San Francisco a su profiter de l'industrie de contenus présente 800 kilomètres plus bas.

L'Europe s'est découvert la capacité d'être une puissance normative. Le règlement général sur la protection des données (RGPD) est, par exemple, devenu un vrai standard international. La Californie a adopté une loi de protection des données très similaire, le Mexique également, tandis que le Japon a obtenu un accord d'adéquation et que l'Inde finalise une loi de protection de la vie privée qui ressemble beaucoup au RGPD. Aujourd'hui, le plus grand marché mondial est constitué de consommateurs sous protection de type RGPD. Les entreprises européennes y gagneront un avantage compétitif puisqu'elles seront nativement prêtes pour le régime juridique le plus consensuel. Le Quai d'Orsay est convaincu que nous sommes capables de dupliquer cette force pour d'autres dossiers. Certains acteurs pensent que les États-Unis géreront les entreprises et l'Europe, la régulation. Une telle dissociation est impossible. Des intellectuels et des chercheurs doivent permettre d'imposer sa régulation. En France, l'histoire du RGPD date de quarante ans. Elle a débuté par la loi « informatique et libertés » grâce à des chercheurs qui ont étudié, testé, implanté, modifié. Au départ, la loi visait à se protéger de l'administration. La directive européenne y a ajouté la protection contre les entreprises. Cette histoire est longue, un secteur ne peut être régulé du jour au lendemain.

La puissance normative est importante, mais l'enjeu sera également de mettre fin à l'escalade des textes prétendant être d'application extraterritoriale. Certes, protéger nos citoyens passe par la revendication de l'application extraterritoriale de notre cadre juridique. Mais l'application extraterritoriale semble aujourd'hui instrumentalisée et l'incertitude juridique est croissante. Décréter l'application extraterritoriale d'un texte pour régler les problèmes n'est pas la panacée. Nous n'avons pas été les premiers à agir ainsi, mais ce n'est pas une excuse.

J'y ai fait allusion en début d'intervention, la plupart de nos start-ups produisent des applications pour smartphones. Elles doivent donc accepter les conditions générales d'utilisation et les data d'une demi-douzaine d'acteurs dont Facebook Connect, Paypal ou

Google Maps. Finalement, la quasi-totalité de l'économie numérique est fondée sur des ressources que nous ne contrôlons pas.

La situation qui en découle est une situation de dépendance et de servilité. Nous devons faire face à cet enjeu. Bien sûr, une stratégie industrielle est nécessaire, à taille européenne, même si l'histoire ne plaide pas en faveur de cette idée. Malheureusement, chaque réponse européenne prend finalement la forme d'une quinzaine de réponses et le consensus sur une entreprise ou un pays est difficile à trouver. La France pourra peut-être démontrer sa solidarité européenne dans le cadre de la bataille de la 5G, en soutenant des entreprises par exemple suédoises. Afin d'éviter que la situation ne se répète dans dix ans, des réflexions peuvent déjà être engagées sur la 6G, le *cloud*, l'informatique quantique ou l'intelligence artificielle. Par le passé, nous avons raté des occasions et nous devons en tirer des enseignements. L'économie numérique est caractérisée par le phénomène du *winner takes all*. Donc partir deuxième pour imiter le premier est déjà partir perdant. L'innovation numérique ne fonctionne pas ainsi. Le projet Gaïa-X (infrastructure européenne de données) me semble basé sur des prémices différentes, avec une construction d'interopérabilité et de synergies (et non un « acteur champion » sur décision étatique). La stratégie industrielle nous offre encore de belles opportunités.

Si l'autonomie des ressources sur lesquelles nous innovons impose une industrie européenne, des actions peuvent aussi être menées avec les communs numériques (*Digital Commons*), des logiciels libres tels que Open Street Map ou Wikipédia. Travailler sur des données libres est le meilleur moyen de garantir que ces données resteront accessibles. Cette position doit être une composante de la stratégie de souveraineté, afin de ne pas s'affaiblir. De plus, cet enjeu relève également de l'aide au développement. En effet, certains pays lorsqu'ils construisent leurs infrastructures hésitent entre une offre chinoise ou Facebook. Nous aimerions leur conseiller de construire un socle en *open source* avec une net-neutralité dont ils seront garants de l'indépendance. L'AFD commence à financer des partenariats publics pour favoriser l'émergence de communs dans les pays.

Pour conclure et avant d'échanger, je reviens sur les notions de souveraineté nationale et de souveraineté européenne. Historiquement, la France était méfiante, privilégiant la souveraineté nationale. Des voix fédéralistes plaidaient pour une Europe fédérale. Ce débat est politique, mais, opérationnellement, sur certains sujets tels que la cybersécurité, nous pouvons décider d'une troisième voie consistant à mieux travailler ensemble. En effet, la cybersécurité de l'Europe se fonde sur des agences solides dans différents pays et qui coopèrent très bien. Elles échangent des informations et savent quand c'est nécessaire déclencher des sanctions à l'échelon européen ou des réglementations renforçant la sécurité globale telle que la directive NIS (*Network and Information System Security*). Ces actions ne sont pas contradictoires, mais elles impliquent de changer les modes de fonctionnement. Le sujet de la souveraineté numérique permet d'évoquer la souveraineté interopérable. L'Allemagne ou les Pays-Bas souhaitent une souveraineté puissante et disposent d'agences fortes. Nous pouvons prévoir des critères communs très concrets, comme une échelle de gravité des attaques, afin de nous comprendre immédiatement. Ainsi, en fluidifiant les interactions, une puissance européenne peut se construire sans transfert de souveraineté. De nombreux sujets que nous avons évoqués nécessitent une coalition européenne pour faire poids au niveau mondial. La France a clairement un rôle leader. Le Président de la République organise le mois prochain à Paris le Forum de Paris sur la Paix (*Paris Peace forum*) et le sommet *Tech for Good* qui réuniront de grands patrons et de grands penseurs de la Tech. Nous sommes leaders, mais notre puissance de négociation découle de notre position européenne.

J'espère avoir répondu à vos questions et je suis à votre disposition pour échanger.

M. le président Jean-Luc Warsmann. Je vous remercie monsieur Verdier pour cette intervention tout à fait intéressante.

Je souhaitais vous relancer sur le sujet de l'extraterritorialité. Vous avez évoqué deux approches, une extraterritorialité pour des principes de base et un principe de comportement national avec des législations extraterritoriales. Cette seconde approche ne pacifie pas les relations internationales. Pourriez-vous approfondir ce point ou bien nous produire une contribution écrite dans les semaines à venir sur ce sujet qui est au cœur de nos problématiques ?

M. Henri Verdier, ambassadeur pour le numérique. Je produirai un écrit, car il me semble difficile d'approfondir ce sujet aujourd'hui au sein de cette mission. Je précise que la protection de nos citoyens, *via* le RGPD, ne vise pas que les entreprises européennes. Les libertés fondamentales de nos citoyens sont à protéger de toutes pratiques y compris issues d'un État ou d'une entreprise extraeuropéenne. La France est claire sur ce point. Néanmoins, nous avons constaté des abus de décisions extraterritoriales venant d'autres continents. Certaines nous sont même apparues comme des violations de notre souveraineté. Nous considérons que quiconque souhaite accéder à des données en Europe doit passer par l'État et non se servir dans les infrastructures européennes, et ce quel que soit le bien-fondé de son objectif. Nous maintiendrons fermement cette position. Mais il semble que certains textes soient interprétables et des pays s'adjugent ce droit notamment pour lutter contre le terrorisme ou la criminalité. Cette attitude n'est pas justifiable, car une coopération judiciaire peut être mobilisée. Aujourd'hui, dans de nombreuses enceintes se brandit facilement la menace d'application de mesures extraterritoriales. Cela peut parfois paraître légitime et fondé, mais nous devons dire à nos partenaires que faire une loi nationale et la décréter extraterritoriale ne peut être qu'un dernier recours, peu à même de régler les querelles. Nous tâcherons d'approfondir ce sujet et je solliciterai notre direction des affaires juridiques qui enrichira ces réflexions.

M. Philippe Latombe, rapporteur. J'aurais deux questions. La première est générale. Parmi nos collègues parlementaires (incluant le Congrès et le Sénat américains), nous observons les prémices d'une volonté de démanteler les géants du numérique présents sur leur territoire. Quelle est la position de la France et de l'Europe ? Sommes-nous plutôt favorables à un tel démantèlement ? Ou bien la complexité de l'action pousse-t-elle plutôt vers d'autres solutions telles que l'interopérabilité ? Vous l'avez évoqué, pouvoir porter ces données permettrait de se passer de ces entreprises. Comment se positionnent la France et l'Europe ? La seconde question est la suivante. L'application du RGPD a été un porte-étendard côté européen, mais la Cour de justice de l'Union européenne nous a rappelés à l'ordre à deux reprises avec l'invalidation du *Privacy Shield* et la confirmation de la jurisprudence *Tele2* la semaine passée. J'aimerais que nous revenions sur le *Digital Services Act* (DSA). Comment le mettre très clairement en place et éviter les incertitudes juridiques systématiques ? Quelle est la position de la France et son influence dans l'écriture du DSA ?

M. Henri Verdier, ambassadeur pour le numérique. La France et l'Europe n'ont pas de positions sur le futur de telle ou telle entreprise. Le contraire serait étonnant puisqu'une décision de démantèlement implique la justice et se fonde sur des fondements sérieux. En revanche, nous souhaitons éviter les abus de position dominante qui empêchent l'innovation. J'avais répondu à une entreprise de l'innovation numérique qui se plaignait que nous souhaitions justement d'autres entreprises de ce type, et non qu'elle soit en situation de monopole. Aujourd'hui, une réflexion complexe, largement portée par le ministère de l'économie et des finances, porte sur ces acteurs systémiques (*gate keepers)* qui déterminent lourdement les dimensions économiques et politiques. Les outils anciens caractérisant une position dominante ne sont plus toujours pertinents. Par exemple, une position dominante

dans le numérique peut venir de la possession d'un standard ou d'une donnée pivot incontournable.

Pour répondre à votre deuxième question, à l'intérieur du DSA nous interrogeons la régulation *ex ante* des plateformes à effet structurant. Le texte est européen, la France a apporté sa contribution à l'élaboration du texte et participera à sa transposition en trilatéral devant le Parlement. J'espère que nous serons tous capables, y compris le Parlement français, de soutenir les thèses défendues auprès de nos partenaires. En tant que responsable de la politique d'*open data*, j'ai vu de beaux textes, insuffisamment servis par le pouvoir de conviction de l'administration. Encore aujourd'hui, certains éléments suscitent de l'insatisfaction, mais cela pousse à avancer. Entre l'élaboration de textes clairs et leur application, un délai existe qui me semble normal. Le droit engendre un cycle judiciaire, fait de jurisprudence et d'approfondissements. Dans un monde idéal, tous s'aligneraient immédiatement sur un nouveau texte.

Mme Marietta Karamanli. Je vous remercie, monsieur l'ambassadeur, pour les éléments abordés. Je partage votre avis sur l'importance de la jurisprudence, essentielle en droit. Elle permet de bousculer et d'avancer. Vous avez évoqué le transfert des données personnelles entre l'Union européenne et les États-Unis. En juillet dernier, l'Union européenne a invalidé ce type de transfert en exigeant que les responsables du traitement des données évaluent eux-mêmes le niveau de protection des données dans le pays du destinataire. Pourriez-vous nous en dire plus sur les discussions sur ce sujet au niveau européen ? Il existe des mesures transitoires urgentes pour sécuriser l'activité des entreprises françaises et européennes dans ce domaine. Comment sécuriser aujourd'hui les transferts des données entre l'Union européenne et les États-Unis notamment au regard du transfert ultérieur des données des pays à des pays tiers ? J'avais souligné cette problématique dans un précédent rapport sur le sujet (datant de mai 2016), mais la crise sanitaire actuelle y ajoute un caractère d'urgence.

M. Henri Verdier, ambassadeur pour le numérique. Je ne saurais vous dire. Il faudrait poser la question à la direction générale des Entreprises (DGE) dont vous avez reçu le directeur. La Cour des comptes n'a pas interdit le transfert de données vers les États-Unis. Elle a fait tomber un régime de protection automatique et elle a rappelé qu'il appartenait à l'entreprise exportant les données de s'assurer qu'elle puisse garantir le respect et la protection de la vie privée. L'exportation de données n'a pas été interdite. La Cour a jugé en référence au droit, sans préjuger des conséquences. Des plans de prolongation de l'activité sont à déterminer. Toutefois, j'ai l'impression que certaines entreprises crient au loup plus fortement qu'il n'est nécessaire. Un grand réseau social a par exemple annoncé le risque d'une fermeture de son activité en Europe. Je pense pour ma part qu'ils vont rapidement trouver une solution adéquate.

Mme Laure de La Raudière. Je me demande si l'enjeu consistant à préserver un internet global face à des internets régionaux est réaliste. En effet, la Chine n'a pas d'internet global, mais son propre internet. Les États-Unis, en interdisant TikTok, livrent une réponse à l'internet régional de la Chine et, de toute façon, les Américains dominent le marché internet hors Chine. Quel est le bilan coûts-bénéfices de la doctrine d'un internet global ? Avec des internets régionaux, l'Europe pourrait appliquer clairement ses lois au niveau européen et établir des accords de coopération au niveau international. Je suis volontairement un peu provocatrice, car vous avez dit : « Il faut tout faire pour garder un internet global. »

M. Henri Verdier, ambassadeur pour le numérique. Je n'ai pas dit « tout faire », car mon carnet de chèques ne me le permet pas. Préconiser un internet libre, ouvert et unifié est une position clairement française. La fragmentation d'internet risque d'entraver la liberté d'expression, de limiter la compréhension mutuelle entre les peuples et de faire perdre

des points de croissance mondiale. Mais allons un peu plus loin. Comme je vous l'ai dit, j'ai créé ma première entreprise en 1985. À l'époque, les ingénieurs de France Télécom ne croyaient pas en internet et pensaient que son coût serait démesuré.

À titre personnel, je considère que la *Permissionless Innvoation*, grâce à un réseau ouvert et décentralisé a donné lieu à l'incroyable cycle d'innovations que nous avons connu. Elle a également permis l'émergence de réseaux sociaux et de géants qui ne sont pas internet. En effet, Facebook, Twitter ou TikTok consistent à entrer dans un espace privé avec un droit privé (régi par les conditions générales d'utilisation) et un design qui n'est pas basé sur la neutralité, la transparence ou la traçabilité. Au contraire, leur design est conçu selon le *business model* de l'économie de l'attention pour donner à voir aux utilisateurs des contenus et des publicités personnalisés visant à augmenter les revenus de l'entreprise. Un internet libre et ouvert ne contrevient pas à l'inspiration initiale des pères fondateurs. Il permet l'émergence d'acteurs dont il faut bien sûr réguler l'activité, mais qui démontrent le bien-fondé des principes fondamentaux.

Avons-nous une chance de gagner la partie ? Tout dépend du sujet. Internet comprend sept couches techniques différentes (les plus connus sont le protocole TCP/IP et le web). Je pense que cette base peut être conservée. Aujourd'hui, l'entreprise Huawei propose à l'Union internationale des télécommunications un nouveau protocole pour les TCP/IP. Certains pays ne l'accepteront jamais. Une autre bataille concerne la muraille dont s'entourent certains pays. Ils demandent ainsi à leurs opérateurs d'aller sur un DNS (*Domain Name System*) national qu'ils filtrent pour supprimer ce qui ne leur convient pas. Néanmoins, quelqu'un de débrouillard, muni d'un réseau virtuel privé (*Virtual Private Network*-VPN), pourra tout de même accéder à l'internet mondial. La censure instaurée concerne donc les masses, elle n'est pas définitive. Ensuite, dans les couches très hautes, des applications peuvent-elles être bannies ? L'Inde (et bientôt les États-Unis) a banni TikTok de l'App store. Les Indiens qui avaient TikTok l'ont toujours, mais de nouveaux téléchargements sont désormais impossibles. Cela peut faire partie d'une stratégie de négociation. Il n'y aura pas d'internet similaire partout avec les mêmes lois. Des stratégies de conflictualité et de protectionnisme vont se développer. L'essence et le cœur doivent être préservés et dans ce domaine, la bataille n'est pas perdue.

M. Pierre-Alain Raphan. Vous l'avez rappelé, le développement de la pratique de la donnée de l'intelligence artificielle devient une stratégie de domination des États dans les différentes régions du monde. Je m'interroge sur les impacts sur la démocratie au sens large et notamment la manière de s'informer. Les récents scandales, notamment celui de Cambridge Analytica, ont montré l'impact sur les libertés individuelles. En effet, l'*open data* est une stratégie très intéressante pour la protection des données en France et en Europe. Mais se pose la question des pratiques individuelles. Votre fonction d'ambassadeur du numérique implique-t-elle des relations fortes avec les ministères chargés de la jeunesse et des sports, le ministère de l'enseignement supérieur, voire le service national universel ? En effet, il me paraît important de mettre en place des programmes d'acculturation sur les grands enjeux du numérique et de diffuser des messages pour mieux se protéger individuellement de cette potentielle fuite de données via les smartphones (les géolocalisations sont quasi imposées) et des réseaux sociaux. L'interaction entre ministères permet-elle aujourd'hui une acculturation populaire sur ces sujets ?

M. Henri Verdier, ambassadeur pour le numérique. Je précise que je ne suis pas ambassadeur du numérique, mais ambassadeur, au sein du ministère des affaires étrangères, pour les affaires numériques. Je suis en charge des négociations internationales et de la politique extérieure de la France pour les affaires numériques. Je m'occupe moins fondamentalement de la politique nationale. Vous avez raison, la liberté individuelle, la

démocratie et la souveraineté sont interdépendantes. La souveraineté et la démocratie sont nécessaires pour protéger la liberté individuelle et la liberté individuelle est nécessaire pour protéger la démocratie et affirmer sa souveraineté. Cette interdépendance est sans doute nouvelle pour le numérique. Mais cela ne relève pas des attributions de l'ambassadeur pour les affaires numériques.

M. Philippe Latombe, rapporteur. Je vous soumets une dernière question que nous n'avons pas encore totalement abordée. Elle porte sur la taxation et la fiscalité des géants du numérique. Les négociations autour de la « taxe GAFA » échouent, sont relancées, échouent à nouveau. Que pouvez-vous nous en dire aujourd'hui ? Où en sommes-nous et quelles suites sont à donner ? Quelle est la position de la France à ce sujet et quels échos existent chez ses partenaires européens ? Je rappelle que la Cour de justice de l'Union européenne avait annulé une amende d'Apple.

M. Henri Verdier, ambassadeur pour le numérique. Ce sujet est en effet encore assez douloureux, car un dumping fiscal demeure entre les pays européens. La vraie question n'est pas une taxe GAFA. D'ailleurs, le ministre de l'économie et des finances a annoncé hier qu'il exercerait son droit de la prélever pour l'année 2020 puisque les négociations à l'OCDE n'avancent pas. La vraie question est celle d'une fiscalité numérique. Depuis des siècles, l'imaginaire fiscal considère que la valeur est prélevée sur le site de production, soit l'usine où se trouvent les salariés, avec une propriété intellectuelle provenant du bureau d'études de l'entreprise. Or, dans le numérique, la valeur relève du consommateur qui utilise le produit, reçoit la publicité, partage ses données et crée encore plus de valeur. Nous devons apprendre à prélever la valeur auprès des utilisateurs plutôt qu'auprès de la création. D'autant que certaines entreprises prétendent que cette création est tout entière de la propriété intellectuelle laquelle est tout entière localisée aux Bahamas. La fluidité numérique permet d'abuser de cette différence.

Depuis longtemps, la France porte ce sujet *via* le rapport « Colin-Collin », l'avis du Conseil national du numérique, les tentatives de portage à l'OCDE… Aujourd'hui, un groupe de travail constitué de représentants de cent vingt pays traite de ce sujet. La France ne vise pas une fiscalité des acteurs du numérique, mais une fiscalité du numérique, compatible avec l'économie numérique. Ce point est crucial. À défaut de prendre la valeur là où elle se crée, la base fiscale s'effrite et les acteurs en mauvaise santé sont affaiblis. Continuer à fiscaliser les perdants sans fiscaliser les gagnants revient à faire de la pression fiscale un handicap. Nous continuerons et nous finirons par l'emporter, car nous avons raison. Mais lors de telles négociations, chacun fait ses comptes. Les pays qui hébergent les géants du numérique ne sont ainsi pas favorables à une telle taxe. La France, souveraine, a donc décidé une taxe GAFA en attendant mieux. Cette taxe GAFA a été annoncée, puis suspendue dans l'attente de l'issue des négociations au sein de l'OCDE. Hier, Bruno Le Maire a annoncé l'échec de ce round des négociations et l'instauration d'un prélèvement de la taxe GAFA pour 2020. La taxe GAFA n'est pas la finalité. L'enjeu est que les systèmes fiscaux soient cohérents avec l'économie réelle actuelle.

La séance est levée à 10 heures 35.

Membres présents ou excusés

Mission d'information de la Conférence des Présidents « Bâtir et promouvoir une souveraineté numérique nationale et européenne »

Réunion du jeudi 15 octobre 2020 à 9 h 05

Présents. - Mme Marietta Karamanli, Mme Laure de La Raudière, M. Philippe Latombe, M. Pierre-Alain Raphan, M. Jean-Luc Warsmann

Excusées. - Mme Virginie Duby-Muller, Mme Danièle Hérin, Mme Nathalie Serre