

A S S E M B L É E      N A T I O N A L E

X V <sup>e</sup>      L É G I S L A T U R E

# Compte rendu

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

- Audition, ouverte à la presse, de M. Julien Nocetti, docteur en sciences politiques, chercheur associé à l'institut français des relations internationales (Ifri) et enseignant-chercheur en relations internationales et études stratégiques aux Écoles de Saint-Cyr Coëtquidan..... 2

Jeudi

11 mars 2021

Séance de 14 heures

Compte rendu n° 40

SESSION ORDINAIRE DE 2020-2021

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



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

*La séance est ouverte à 14 heures.*

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

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

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

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

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

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

**M. Julien Nocetti, docteur en sciences politiques, chercheur associé à l'institut français des relations internationales (Ifri).** Je vous remercie de m'avoir invité à m'exprimer sur ces enjeux que vous venez d'esquisser, qui sont absolument passionnants, éminemment complexes, très évolutifs et qui mobilisent votre mission d'information. En guise de préambule, je me permets de préciser que je dirige aussi, depuis peu, la chaire Cybersécurité de Rennes School of Business, au sein de l'une des plaques territoriales de la cybersécurité en France.

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

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

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

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

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

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

Nous observons, par ailleurs, que l'enjeu de la souveraineté numérique est parfois exploité, par les États que j'ai mentionnés, à des fins stratégiques et de politique étrangère. Il est d'ailleurs frappant de relever, soit dit en passant, que certains médias russes – que nous connaissons bien depuis 2017 – n'ont aucun complexe à instrumentaliser ce sujet de la souveraineté numérique, ou plutôt l'absence de souveraineté numérique en Europe, avec en contrepoint les différents scandales d'espionnage qui ont émaillé la vie politique et stratégique européenne depuis une dizaine d'années. La souveraineté numérique est donc une thématique qui est aussi exploitée à nos propres dépens, et nous devons nécessairement prêter attention à cette dimension dans l'élaboration de doctrines et pour peser dans ce domaine.

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

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

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

produites sur le continent européen transitent, à un moment, par le territoire américain. Je pense que c'est un paramètre que nous devons bien mesurer.

Au-delà du cas américain, nous devons bien appréhender l'évolution extrêmement rapide de cette notion de souveraineté numérique et des enjeux qu'elle charrie. En 2021, la souveraineté numérique est très différente de la souveraineté numérique que nous commençons à appréhender en 2010 ou en 2014, un an après l'affaire Edward Snowden. À l'époque, lorsque l'on évoquait la notion de souveraineté numérique, les débats se focalisaient essentiellement sur une seule question : qui contrôle Internet ? Aujourd'hui, les enjeux sont extrêmement différents, puisque la question dépasse le champ numérique traditionnel – infrastructures, Internet, web, etc. Par conséquent, nous devons urgemment élargir notre propre focale en y incluant les technologies critiques. L'intelligence artificielle, la 5G et l'informatique quantique ne peuvent pas être occultées de notre conception de la souveraineté numérique, tout comme l'enjeu de l'approvisionnement en composants critiques, sur lequel je reviendrai dans quelques instants. Je pense également à la maîtrise d'algorithmes sensibles. Ces problématiques sont d'une très grande complexité lorsqu'elles s'intercombinent. Je vous laisse donc imaginer à quel point toute ambition de souveraineté numérique est vertigineuse.

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

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

Comme vous l'évoquiez, l'Europe cumule des faiblesses déjà bien identifiées en matière de souveraineté numérique, qu'il s'agisse de facteurs internes ou externes. En interne, citons l'insuffisante intégration du marché numérique, les problématiques de financement de l'innovation, les divergences politiques entre États membres, etc. À l'extérieur, l'Europe

s'expose de plus en plus à des stratégies de puissance prédatrices et éprouvées. J'ai déjà évoqué, dans le cas des États-Unis, une longue tradition combinant puissance financière, puissance technologique, mais aussi attraction des GAFAM – par le biais d'un écosystème extrêmement performant – et extraterritorialité du droit américain. Du côté de la Chine, la célérité et le centralisme de la prise de décision, conjugués à une absence totale de considérations éthiques en interne, expliquent pourquoi cette spécificité chinoise parvient à acquérir quelques avantages en matière stratégique, au détriment de l'Europe.

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

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

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

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

Pour en revenir à votre première question relative à la définition de la souveraineté numérique, je rappellerai d'abord que beaucoup s'y sont déjà essayés, et que je ne suis donc

pas certain de pouvoir y apporter une contribution fondamentalement nouvelle. Néanmoins, en lien avec cette logique d'interdépendances, la souveraineté numérique pourrait consister à pouvoir choisir nos interdépendances. Par cette formule, je sous-entends l'idée de choix, de stratégies, de moyens, de capacités, mais également l'idée que nous évoluons dans un contexte global d'interdépendances. Nous devons bien mesurer que certaines approches de la souveraineté numérique édictées ou martelées au cours de la dernière décennie ont pu parfois sembler cantonnées à des logiques nationales extrêmement réductrices, sans doute caricaturales, qui occultaient complètement le fait que notre monde demeurerait extrêmement globalisé et soumis à des logiques d'interdépendances, en dépit des formes de nationalisme technologique auxquelles nous avons pu assister du côté chinois comme du côté américain.

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

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

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

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

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

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

Du côté américain, la situation est paradoxale. Certains acteurs comme Qualcomm, Apple et Intel jouissent d’une forme de leadership sur certaines parties de la chaîne de valeur des semi-conducteurs, en particulier dans leur design. En revanche, les Américains ne maîtrisent pas l’ensemble du spectre et dépendent de chaînes de valeur tout à fait globalisées, comme je l’indiquais précédemment. C’est d’ailleurs pour cette raison que le géant américain Nvidia a tenté, l’été dernier, de racheter le britannique ARM, qui est extrêmement avancé dans la construction de semi-conducteurs. L’accord a semble-t-il capoté pour diverses raisons. Néanmoins, cette tentative montre bien que les Américains sont devenus extrêmement susceptibles sur cet enjeu des semi-conducteurs et cherchent à mettre certains de leurs alliés sous pression, notamment en Asie. Je pense notamment à Taïwan, qui revient en force dans cette géopolitique des technologies, et qui héberge notamment la société TSMC, leader mondial de la fonderie et de la production de ces composants. Durant sa présidence, Donald



Trump a cherché à relocaliser, sur le territoire américain, précisément en Arizona, une partie de la production de TSMC. J'ignore si l'accord sera ou non maintenu par l'administration Biden, mais force est de constater que cet enjeu fut véritablement, durant plusieurs années, au centre de l'agenda bilatéral sino-américain et des tensions géopolitiques en matière de technologies.

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

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

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

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

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

Avec Joseph Biden, nous devons nous attendre, malgré une volonté d'apaisement qui sera recherchée avec la Chine, à une politique du coup pour coup sur ces questions de cybersécurité, et à une stratégie de représailles systématiques contre ces velléités chinoises de tester les États-Unis. Nous le savons, les Américains sont amplement testés depuis quelque

temps. Nous en avons vu la première manifestation avec l'attaque dirigée contre SolarWinds, qui fut pour partie attribuée à la Russie, tandis que certains acteurs chinois auraient également effectué quelques intrusions au sein des systèmes compromis. Je pense également à cette attaque subie par la Floride, dont les systèmes d'approvisionnement en eau auraient été compromis par l'intervention de pirates informatiques. Plus récemment, nous avons tous en tête l'attaque dirigée contre Microsoft Exchange par le biais de pirates chinois.

Aux États-Unis, cette tradition d'attributions publiques des attaques relève aussi d'une logique d'envoi de signaux : envoyer des signaux de dissuasion et/ou de coercition et empêcher que tel ou tel acteur ne se livre à des attaques répétées et plus conséquentes en termes de dégâts. S'il est probable que cette tendance se poursuive aux États-Unis, reste à savoir si cette systématisation des attributions se répercutera, à long terme, chez les alliés européens. Au Royaume-Uni, on observe depuis quelque temps une forme de mimétisme et d'alignement, avec de multiples cyberattaques attribuées à la Russie. Le reste de l'Europe est, quant à lui, marqué, sur ce plan également, par des divergences de politiques et de conceptions sur l'attribution ou la non-attribution de cyberattaques. À ce stade, aucun consensus ne semble véritablement se dégager. L'un des points fondamentaux suscitant le plus de débats est d'ailleurs l'enjeu du « *hack back* », ou piratage en retour, qui confère aux acteurs privés un rôle important en matière de représailles. Ce sujet ne fait absolument pas consensus et se prête parfois aux chamailleries des différents États européens au sein des enceintes de discussion communautaires.

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

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

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

**M. Philippe Latombe, rapporteur.** En lien avec ma précédente question, comment situez-vous les Anglais, qui ont quitté l'Union européenne ? Sur cet échiquier mondial, la petite plaque qu'est le Royaume-Uni se rapprochera-t-elle plutôt des Américains ou se

maintiendra-t-elle plutôt dans notre environnement ? Je pense notamment à la protection des données, sachant que le Règlement général sur la protection des données (RGPD) ne sera plus applicable au Royaume-Uni à partir du 1<sup>er</sup> juillet 2021. Les Britanniques doivent ainsi décider, avant le mois de juin, quel modèle adopter en matière de protection des données. Conserveront-ils l'ancien modèle du RGPD ou entameront-ils une transition vers le modèle américain ? Ce sujet peut-il être source de difficultés ? Sait-on si le Royaume-Uni aurait fait des émules auprès d'États membres qui souhaiteraient se rapprocher des Américains ?

**M. Julien Nocetti.** Il s'agit d'une question relativement sensible. Avant le Brexit, la diplomatie numérique britannique était assez pléthorique, et le Royaume-Uni était sans doute l'acteur européen le plus consistant dans ce domaine, sans doute par mimétisme vis-à-vis du partenaire américain, mais aussi par connaissance de ces thématiques et par une plus grande maturité sur ces enjeux et sur la défense des intérêts britanniques en la matière. Cette consistance était particulièrement visible sur la plaque bruxelloise, avec des intérêts britanniques – notamment en matière de commerce et de protection des données – sagement défendus par les officiels de la Couronne, mais aussi une habileté à fonctionner en réseau avec des sociétés de conseil – ou autres – extrêmement efficaces dans la défense de ces intérêts et des approches promues par les Britanniques. Tout ne disparaîtra pas avec la transition et le départ du Royaume-Uni des instances communautaires, puisque le pouvoir britannique disposera toujours d'experts et de relais à Bruxelles.

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

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

**M. Julien Nocetti.** C'est un point intéressant, dans la mesure où cette idée de troisième voie – sur laquelle je travaille actuellement – n'est pas nouvelle. Si l'on en retrace la généalogie, cette notion de troisième voie est surtout mise en avant depuis l'affaire Edward Snowden. À l'origine, certaines propositions politiques ont pu sembler farfelues ou décalées. En 2013, la proposition d'Angela Merkel de mise en place d'un Schengen de l'Internet avait suscité une série d'incompréhensions politiques à différents niveaux, avant d'être balayée d'un revers de main par les Américains. Je songe également aux stratégies d'évitement d'une

ultra-dépendance aux câbles sous-marins contrôlés par des sociétés américaines. La question n'est donc pas nouvelle, puisque ces propositions pouvaient être envisagées, à l'époque, comme une forme de troisième voie permettant à l'Europe de se positionner entre cette vision très libertarienne à la californienne – bien que soutenue par le pouvoir fédéral – et cette vision techno-autoritaire à la chinoise.

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

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

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

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

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

Quoi qu'il en soit, des niches d'excellence sont nécessairement à prendre du côté européen. Dans certains domaines comme la cybersécurité, l'identité numérique ou l'algorithmie, l'Europe dispose de savoir-faire de pointe et de pépites, avec des expertises personnelles et collectives – centres de recherche, laboratoires, start-up – extrêmement pointues. De fait, pour répondre indirectement à votre question, l'Europe pourrait se montrer plus proactive en assurant la défense et la protection de tels acteurs face à des stratégies prédatrices extrêmement classiques. Nous devons investir des niches d'excellence susceptibles de réduire notre dépendance à d'autres acteurs extra-européens, tout en nous donnant la capacité de protéger nos propres acteurs. Comme l'actualité l'a récemment montré, certains acteurs majeurs de la cybersécurité ont été rachetés par des concurrents étrangers. Différentes pistes doivent donc être explorées dans ce domaine.

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

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

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

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

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

**M. Julien Nocetti.** La question est évidemment très vaste. J'évoquais précédemment le concept d'autonomie stratégique et sa réappropriation partielle par la « bulle bruxelloise », par le biais de certaines initiatives technologiques et numériques. Or ce concept est bien issu du contexte stratégique français. De fait, cette idée d'autonomie stratégique numérique a pu être perçue, par certains États européens à Bruxelles, comme une volonté française d'être, sinon hégémonique, du moins beaucoup plus présent dans le débat, quitte à essayer d'en imposer les termes. Certains de nos partenaires européens le ressentent ainsi.

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

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

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

De fait, la diplomatie de la conférence conduite par la France traduit aussi une stratégie d'affichage qui n'est pas toujours suivie d'effets. Cet aspect de notre politique pourrait donc être plus soutenu et plus efficient, sachant que la diversité des enjeux traités

dans ces multiples initiatives et événements requiert des moyens qui, parfois, font aussi défaut à l'ensemble de l'appareil diplomatique français.

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

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

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

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

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

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

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

**M. Philippe Latombe, rapporteur.** France Digitale a attaqué Apple en justice pour des pratiques anti-concurrentielles, arguant du fait qu'il est impossible d'échapper à son monopole, étant entendu qu'Apple est propriétaire à la fois du système d'exploitation et de la plateforme d'achat des applications. Parallèlement, des questions sur la taille des GAFAM commencent à émerger aux États-Unis. S'agit-il d'une question qui se pose réellement ? S'agit-il simplement d'une menace de circonstance ou s'agit-il d'une voie dans laquelle même les Américains devront rentrer ?

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

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

Cela dit, l'enjeu le plus saillant sur lequel ces acteurs pourraient être attaqués est celui du respect de la concurrence, que le législateur américain a toujours à cœur, suite à des décennies de pratiques déjà éprouvées dans ce domaine. Il ne serait pas surprenant qu'un acteur comme Facebook, aussi majeur soit-il, finisse par être scindé, pour des raisons



concurrentielles, mais aussi politiques, en plusieurs entités, sachant que ce sujet fait l'objet de discussions répétées au sein même des États-Unis. En tout état de cause, cette possibilité ne relève pas du simple fantasme.

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

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

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

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

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

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

**M. Philippe Latombe, rapporteur.** Devons-nous chercher à agréger des acteurs pour leur permettre d'atteindre une taille critique ? Dans la compétition de demain, pourrions-nous

survivre avec des entreprises de taille intermédiaire (ETI) face aux grands groupes construits par nos concurrents – j’emploie à dessein le terme « *concurrents* », et non le terme « *adversaires* » ? Je précise que ma question couvre aussi bien le volet économique que la logique de stratégie d’influence.

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

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

**M. Julien Nocetti.** Comme je l’évoquais dans mon propos liminaire, nous devons bien mesurer l’accélération phénoménale à laquelle nous avons été confrontés depuis à peine dix ans. En l’espace de quelques années, la décennie 2010 a été marquée par le franchissement de certaines étapes vertigineuses en matière de numérique et de technologies. Ce rythme effréné va-t-il se poursuivre à horizon de cinq ou dix ans ? De la réponse à cette question dépendront un certain nombre de paramètres.

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

Bien que nous ayons tendance à occulter ce paramètre socio-économique, nous devons le suivre de manière très stratégique et très politique dans les cinq à dix années à venir, sachant que ces changements technologiques suivent un rythme très vélocé, qui plus est avec une extension du champ numérique. Je mentionnais précédemment l’ampleur prise par les questions et les enjeux de l’intelligence artificielle, des réseaux 5G déployés à grande échelle, qui impliqueront des enjeux de libertés fondamentales à l’ère numérique, des enjeux de surveillance – que nous avons malheureusement pu mesurer depuis la crise sanitaire – et des enjeux stratégiques, au sens où les grands acteurs de cette planète technologique n’auront aucune pudeur à s’affranchir des règles de bon comportement et défendront leur propre pré carré et leur propre stratégie. Je ne le dis pas pour m’inscrire dans une posture pseudo-réaliste, mais pour tenter de dessiner une lecture qui se distancie d’une certaine forme d’ingénuité par

rapport à ces enjeux. Nous sommes bien dans une logique de rapports assez bruts, et tous les phénomènes que nous pouvons observer depuis quelques années seront nécessairement amplifiés dans les années à venir. Il s'agit donc d'acquérir une compréhension extrêmement fine de ces enjeux, en particulier – c'est l'objet de votre commission et de vos travaux – de ces enjeux de souveraineté extrêmement puissants.

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

**M. Julien Nocetti.** Je répondrai en deux temps, en tenant compte des deux dimensions que vous avez évoquées. Je mets de côté la Chine, sur laquelle je reviendrai dans quelques instants, pour commencer par ce premier enjeu plus sociétal. *In fine*, un développeur de San Francisco partage davantage de points communs avec un fondateur de start-up de Bangalore, un capital-risqueur de Londres ou un hacker de Saint-Petersbourg qu'avec ses propres concitoyens du Midwest américain. Bien entendu, il s'agit de l'exemple américain, qui est très particulier. Néanmoins, les mêmes fractures territoriales, urbaines et géographiques sont à l'œuvre en France, ainsi qu'au Royaume-Uni, où les fractures sont encore plus marquées qu'en France. Ces fractures sont profondément travaillées par le numérique, par notre dépendance au numérique et par l'emprise de certains acteurs, à commencer par Amazon. C'est un paramètre sur lequel je souhaite mettre l'accent.

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

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

En outre, la Chine est épisodiquement marquée par l'émergence de contestations. Il est difficile d'y voir parfaitement clair, mais le pouvoir chinois fait parfois face à des foyers de contestation liés à une crise écologique, un accident ferroviaire, sans compter les événements très particuliers de Hong Kong, dont l'impact fut retentissant. En tout état de cause, le

numérique sert aussi aux citoyens chinois, qui ont développé une forme d'ingéniosité en tentant de contourner les mots et termes censurés, et qui emploient tout un vocable dédié afin de contourner cette grande muraille et ce pare-feu à la chinoise, dont le caractère monolithique est effectivement indéniable. Ne sous-estimons donc pas les réponses et les capacités de mobilisation des populations chinoises face aux initiatives très verticales de Pékin.

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

*La séance s'achève à quinze heures trente.*



### **Membres présents ou excusés**

**Mission d'information sur le thème « Bâtir et promouvoir une souveraineté numérique nationale et européenne »**

Réunion du jeudi 11 mars 2021 à 14 heures

*Présents.* – MM. Philippe Latombe, Denis Masségli, Jean-Luc Warsmann

*Excusées.* – Mme Frédérique Dumas, Mme Nathalie Serre