Conférence parlementaire
Cybersécurité, protection des données, intelligence artificielle : quels enjeux pour l'Europe ?

Organisée par le Sénat français, le Bundesrat allemand et le Sénat polonais

Jeudi 20 juin 2019

Sommaire

Allocutions d'ouverture

M. Jean BIZET
Sénateur de la Manche, Président de la commission des Affaires européennes du Sénat

Madame la Présidente,

Messieurs les Présidents,

Monsieur le Secrétaire général,

Monsieur le Directeur général,

Mes chers collègues,

Mesdames, Messieurs,

C'est avec grand plaisir que je vous souhaite la bienvenue ce matin au Palais du Luxembourg pour cette conférence parlementaire qui associe les secondes chambres d'Allemagne, de Pologne et de France.

Dans le cadre de la dimension parlementaire du « Triangle de Weimar », le Sénat français, le Bundesrat allemand et le Sénat polonais ont décidé d'organiser un cycle de trois conférences parlementaires portant sur les enjeux du numérique. Une première conférence s'est tenue à Varsovie, le 4 décembre 2017 ; elle était consacrée à la lutte contre les discours de haine sur Internet et à la cybersécurité. Une deuxième conférence a été organisée le 22 octobre 2018 à Berlin sur le thème de la lutte contre les Fake news.

Le Sénat français est très heureux d'accueillir aujourd'hui la troisième conférence qui s'intitule « Cybersécurité, protection des données et intelligence artificielle : quels enjeux pour l'Europe ? ».

Je me réjouis que le cadre soit ainsi dressé : d'abord, parce qu'il invite à croiser les enjeux technologiques qui s'attachent au développement d'internet, à la prolifération des données et aux progrès de l'intelligence artificielle, avec les enjeux politiques de sécurité et de protection, qui accompagnent l'entrée dans cette nouvelle ère technologique. Ensuite, parce que le sujet pose d'emblée la question au niveau adéquat, à savoir le niveau européen. En effet, la révolution industrielle que représente l'intelligence artificielle transforme nos économies et nos sociétés en profondeur et soulève des questions éthiques qui mettent en jeu le système de valeurs européen dans son ensemble. L'Union européenne compte désormais des dizaines de milliards de dispositifs numériques connectés, vulnérables aux défaillances techniques et aux virus et producteurs de quantité de données.

Les défauts de sécurité et le manque de transparence sur les algorithmes sont à l'origine de préjudices considérables pour les entreprises, en termes économiques ou bien évidemment de réputation, mais aussi de dommages pour les personnes, et soulèvent des questions délicates en termes de responsabilité. On peut citer le bug qui mit en échec le lancement d'Ariane 5 en 1996, l'autopilote « assassin » de Tesla, l'utilisation d'un système d'exploitation périmé qui permit au logiciel malveillant Petya de faire tant de ravages au National Health Service, ou encore le piratage par ultrasons des assistants numériques contrôlant tout dans les maisons intelligentes.

Dans ce contexte, une réponse européenne à multiples dimensions est nécessaire. Je dirais même que cette réponse est stratégique, dans un contexte où d'autres grands acteurs misent massivement sur ces nouvelles technologies.

L'Union européenne semble avoir pris la mesure de l'enjeu, à la fois sous l'angle de la cybersécurité qui fait l'objet de notre première table ronde et sous l'angle de l'intelligence artificielle que traitera notre seconde table ronde. Ainsi, en septembre 2017, la

Commission européenne a proposé un paquet de mesures pour renforcer la résilience de l'Union européenne dans le domaine de la cybersécurité. L'Acte européen pour la cybersécurité, définitivement adopté il y a tout juste deux mois, procure un cadre européen pour la certification de cybersécurité et renforce le rôle de l'Agence européenne chargée de la sécurité des réseaux et de l'information, l'ENISA, créée en 2004.

Ce règlement, qui est d'application directe dans les États membres, constitue une avancée déterminante pour l'autonomie stratégique européenne. Le Sénat français l'avait d'ailleurs soutenue par une résolution européenne de mai 2018, tout en faisant valoir l'importance que gardent aussi les agences nationales chargées de la cybersécurité, sur ce sujet de souveraineté.

Puis, en avril 2018, la Commission européenne a proposé une approche coordonnée avec les États membres pour tirer le meilleur profit des opportunités de l'intelligence artificielle. Cette stratégie repose sur trois piliers : un renforcement de la capacité industrielle et technologique de l'Union européenne, une préparation aux changements économiques et sociaux induits par l'intelligence artificielle, et la garantie d'un cadre éthique et juridique approprié pour créer un environnement de confiance et de responsabilité autour de cette technologie. Le Conseil a validé cette approche en juin 2018.

Parallèlement entrait en vigueur le 28 mai 2018 le RGPD (Règlement Général de Protection des Données), qui aura mis sept années à émerger. Négocié durant quatre années, ce règlement européen a été conçu autour de trois objectifs : renforcer les droits des personnes, responsabiliser les acteurs traitant des données et crédibiliser la régulation, grâce à une coopération renforcée entre les autorités de protection des données. Ce cadre législatif, venu se substituer aux 28 réglementations nationales, constitue désormais le plus haut standard mondial de protection des données personnelles de l'ère numérique. Je le précise fréquemment, l'Union européenne a une avance sur l'aspect éthique, et nous pouvons nous féliciter de ce succès.

La commission des affaires européennes du Sénat de la République française a été partie prenante dans ces évolutions : dès le 19 octobre 2017, elle a créé un groupe de travail pour se pencher sur l'enjeu de l'intelligence artificielle pour l'Union européenne. Ce groupe a élaboré un rapport au titre explicite, « Intelligence artificielle : l'urgence d'une ambition européenne ». Notre collègue André Gattolin aura l'occasion de vous présenter les résultats plus en détail, lors de la seconde table ronde de la matinée.

Mais je veux déjà insister sur sa conclusion principale : maintenant que l'Union européenne s'est mise en ordre de bataille juridique pour améliorer la cybersécurité et protéger les données, elle doit s'engager résolument, conjointement avec les États membres, dans le déploiement à l'échelle industrielle de l'intelligence artificielle.

L'Union européenne ne doit pas manquer ce rendez-vous. Elle a un immense potentiel en termes de talents et de recherche et de développement. Pourtant, elle le gâche sous nos yeux : comment expliquer qu'elle laisse les géants américains du numérique racheter ses jeunes entreprises innovantes ? Pourquoi d'importants marchés publics numériques, y compris en matière d'éducation, sont-ils attribués à des opérateurs américains et non européens, consolidant ainsi des positions dominantes ? Il est pourtant déterminant, pour favoriser le déploiement de l'innovation européenne en matière d'intelligence artificielle, de lui donner accès à un marché de taille suffisante : en effet, plus les données recueillies seront nombreuses, plus l'apprentissage des algorithmes se perfectionnera. L'interopérabilité que permet le transfert de données entre les opérateurs est également un élément essentiel pour assurer le succès des nouveaux écosystèmes, par exemple pour l'Espace numérique de santé.

Engager résolument l'Europe dans la compétition de l'intelligence artificielle signifie donc une mobilisation tous azimuts. Pour donner à l'Europe la maîtrise de son écosystème de données et lui permettre de tirer tout le bénéfice économique et social espéré de l'intelligence artificielle, il faut jouer sur plusieurs leviers :

D'abord la recherche et le développement : les atouts de l'Union européenne en ce domaine doivent encore être renforcés, notamment dans le cadre du partenariat public / privé sur la cybersécurité. Pour mobiliser autant de fonds, ce type de cadre est incontournable.

Ensuite, le développement d'une filière industrielle, ce qui passe par une présence accrue des États membres et des industriels européens du numérique dans le processus de certification pour imposer nos normes et formats de données ; cela passe aussi par une révision des règles de concurrence européennes, qui doivent concourir à l'ambition industrielle de l'Union au lieu de l'entraver. La commission des Affaires européennes du Sénat s'est d'ailleurs beaucoup penchée sur ce sujet. Les États-Unis comme la Chine savent, eux, manier l'arsenal des soutiens publics à leurs champions ; la politique commerciale elle-même de l'Union européenne peut aussi être un levier. L'Union européenne ne doit pas s'interdire d'envisager de se protéger en invoquant la clause de sécurité nationale, prévue à l'article XXI des accords de l'OMC, puisque l'organe de règlement des différends a eu récemment l'occasion d'en valider le bien-fondé. Le Président des États-Unis s'est d'ailleurs beaucoup intéressé à ce concept.

Enfin, il faut aussi mettre le prix dans ce projet de déploiement d'une intelligence artificielle à l'européenne. L'investissement dans les moyens de calcul dédiés à l'intelligence artificielle doit mobiliser à la fois les États membres et l'Union européenne. La Chine entend investir 59 milliards d'euros d'ici 2025 pour rattraper les États-Unis qui concentraient déjà en 2016 70 % des investissements mondiaux dans l'intelligence artificielle. L'Union européenne doit, elle aussi, se donner les moyens de ses ambitions, et c'est l'un des enjeux de la négociation en cours de son cadre financier pluriannuel. Le Sénat français défend la nécessité de valider l'intelligence artificielle comme un « projet d'intérêt européen commun », ce qui permettrait de fédérer les acteurs européens et de changer de braquet en termes d'investissement. À ce titre, j'ai déploré hier lors d'une réunion avec la secrétaire d'État aux Affaires européennes la modicité de l'investissement effectué en ce domaine qui ne représente que 1,11 %, ce qui est clairement insuffisant au regard des enjeux.

C'est à ces conditions que nous pourrons offrir au monde un modèle crédible d'intelligence artificielle, adossé sur une éthique en matière de protection des données conforme à nos valeurs : ce modèle européen peut constituer un avantage comparatif pour nos opérateurs numériques, en les différenciant de leurs concurrents chinois et même américains. Mais cette perspective prometteuse ne pourra voir le jour et ne sera crédible que grâce à la construction d'une véritable filière industrielle européenne autour de l'intelligence artificielle. Cela demande une détermination politique claire.

Une collaboration franco-allemande sur le sujet est déjà amorcée, et nous gagnerions à la compléter par des collaborations avec nos amis polonais. Nos trois assemblées réunies aujourd'hui peuvent ensemble donner une impulsion précieuse en ce sens. J'espère que nos échanges ce matin nous convaincront d'agir ensemble sur ce sujet décisif pour l'avenir de l'Union européenne.

Je me suis permis de rentrer dans les détails, car le sujet est vaste. Je laisse la parole à ma collègue Catherine Morin-Desailly, avec laquelle nous partageons une vision commune sur ces aspects.

Mme Catherine MORIN-DESAILLY

Sénatrice de la Seine-Maritime, Présidente de la commission de la Culture, de l'Éducation et de la Communication

Monsieur le Président de la commission des Affaires européennes, cher Jean Bizet,

Mesdames et Messieurs,

Je voudrais tout d'abord saluer nos collègues venus d'Allemagne et de Pologne pour réfléchir avec nous sur des questions ô combien essentielles. En outre, je salue également l'ensemble de ceux qui participent à cette rencontre.

Le thème d'aujourd'hui s'intitule *« Cybersécurité, protection des données et intelligence artificielle : quels enjeux pour l'Europe ? »*. Je note qu'il fait suite à une première conférence qui s'est tenue à Varsovie et était consacrée à la lutte contre les discours de haine sur internet, et à une deuxième conférence qui a eu lieu à Berlin sur le thème des *fake news*, « infox » en français.

Ce sont des sujets que nous connaissons très bien au Sénat, car nous les travaillons de longue date. Nous leur avons aussi consacré plusieurs discussions à la faveur des projets de textes de loi qui sont inscrits à l'ordre du jour par le gouvernement.

Je note entre ces trois thèmes à la fois une profonde cohérence et une unité naturelle.

L'unité se situe au travers de la question de notre souveraineté numérique. En réalité, c'est cette question qui est en jeu. L'enjeu pour nous, au lendemain des dernières élections européennes, est de nous réveiller définitivement et d'être capables de sortir d'une forme d'angélisme, de naïveté peut-être, ou bien d'une forme de morne résignation qui consisterait à nous dire que finalement tout est joué, que nous avons laissé passer le train des investissements possibles dans ces nouvelles technologies. Il est urgent de nous réveiller parce que nous sommes devenus une colonie du monde numérique.

Paradoxalement, l'Internet est né de ce côté de l'Atlantique, mais nous n'avons pas été capables dans les années quatre-vingt-dix, à la différence des Américains, d'investir dans les nouvelles technologies et nous avons laissé les Américains prendre le premier rang.

Dans le même temps, de l'autre côté du monde, les Russes et les Chinois ont construit leur propre écosystème dans ce domaine. Il est donc temps de sortir de cette tenaille qui nous place entre un modèle ultralibéral, qualifié parfois de « capitalisme de surveillance », et un modèle d'autocrature à l'instar de ce qui se construit avec le crédit social en Chine, les technologies étant au service d'une élite instaurant la surveillance généralisée.

Je crois que l'Europe, forte de ses valeurs, peut et doit même développer un autre modèle qui permettra la survie d'internet, aujourd'hui exposé à un risque de perte de confiance de la part de l'ensemble des internautes qui remettent de plus en plus en cause son intérêt en raison de tout ce qui se passe.

Je rappellerai ainsi que deux événements ont réveillé nos consciences.

Tout d'abord, l'affaire Snowden a révélé au monde le système d'hyper-surveillance mis en place par la NSA. Ensuite, le scandale de Cambridge Analytica, mis en lumière il y a quelques mois à peine, démontrant que nous sommes entrés dans une guerre froide de l'information.

Il est donc temps de réagir, car l'Internet est bel et bien devenu un terrain d'affrontement mondial, un monde d'hyper-surveillance et de vulnérabilité.

Au Sénat, Jean Bizet l'a évoqué, nous avons travaillé de longue date aux solutions qui pourraient être apportées dans une mission commune d'information menée en 2015. Il s'agissait de déterminer ce que pourrait apporter l'Europe dans cette gouvernance mondiale de l'Internet. Je dois dire que nos préconisations de l'époque sont toujours

d'actualité, voire encore plus depuis que tous ces scandales ont révélé l'urgence d'une réaction.

Nous avions conclu à la nécessité de développer une stratégie globale et offensive, dont Jean Bizet a tracé les quelques lignes. J'en rappellerai moi-même les caractéristiques principales.

Tout d'abord, il est indispensable de poursuivre notre travail en matière de protection des données. Certes, le RGPD existe, mais il a mis des années à pouvoir être voté, tout simplement du fait d'un lobbying outre-Atlantique qui a fait pression sur les dirigeants européens. En outre, en raison du caractère tardif de son entrée en vigueur, ce RGPD comporte plusieurs angles morts. Vous allez peut-être aussi travailler sur la question de l'Internet des objets, notamment à travers la question de l'intelligence artificielle et vous savez que ce domaine est en plein essor : il est donc urgent que l'ensemble des États européens se penche sur la question d'une certification qui nous offre la garantie de notre sécurité. Par conséquent, la question de la protection des données reste de toute première importance.

Des dispositions sont aussi à prendre en matière fiscale. Toutefois, comme le souligne fréquemment mon ami Bernard Benhamou, la fiscalité ne saurait constituer l'alpha et l'oméga d'une politique en faveur de la souveraineté numérique. En effet, nous devons également faire évoluer les règles de la concurrence.

Actuellement, les règles en matière de concurrence au niveau européen ne nous permettent pas de faire émerger des champions européens. De plus, elles agissent de telle manière que nos meilleurs talents et start-ups sont progressivement rachetés. En somme, nous assistons à une réelle hémorragie de tous ceux qui pourraient justement nous aider à ancrer en Europe un système numérique.

Des mesures conservatoires doivent aussi pouvoir être adoptées. Est-il normal qu'il ait fallu sept ans pour réussir à condamner Google pour abus de position dominante ? L'action entreprise fut certes courageuse et elle honore la commissaire Margrethe Vestager, mais il a été impossible, de par l'actuelle législation, de prendre des mesures conservatoires ? Pendant ce temps, les entreprises qui subissaient cette concurrence déloyale ont disparu. Il faut réagir à cela en changeant nos règles de concurrence.

Il faut aussi rouvrir la directive e-commerce. Je l'affirme, la meilleure manière de lutter contre les fausses nouvelles serait justement de conférer enfin un statut aux plateformes qui aujourd'hui ne sont ni redevables ni responsables de rien. Ce sera, selon moi, l'un des prochains chantiers de la Commission européenne. Le gouvernement français commence enfin à y réfléchir et à pousser cette idée, mais, je vous le dis, elle est tout à fait essentielle.

Concomitamment, l'Europe a besoin d'une politique industrielle puissante dans les secteurs clés et stratégiques que sont l'énergie, la santé, l'environnement, mais aussi dans le développement des outils cryptographiques qui seront le fer de lance demain des nouvelles vagues d'ubérisation des banques et du secteur prudentiel.

Il faut surtout une montée en compétence numérique de tous, car sans formation, sans éducation de toutes les tranches d'âge, de nos administrations, de nos politiques, nous ne pourrons pas prendre à bras-le-corps l'ensemble de ces sujets.

C'est sur toute une série de sujets qu'il faut avancer ensemble, ce qui passe aussi par une très grande exigence, comme nos amis allemands ont su le démontrer en réaction aux affaires Cambridge Analytica et aux « pratiques mafieuses » de Facebook. Je n'ai pas peur d'utiliser ce terme à l'instar de mon homologue et collègue britannique Damian Collins qui emploie aussi le terme de « gangster ». À travers l'exploitation des données, Facebook utilise à mauvais escient, cela a été démontré, ce qui relève de la propriété individuelle. En Allemagne, vous avez su prendre des mesures pour interdire l'agrégation des données à partir de Facebook, ce qui vise à permettre une meilleure protection de l'internaute.

Je ne crois pas une seconde au recours à l'autorégulation que proposent aujourd'hui les plateformes la main sur le cœur dans une soi-disant repentance ; je pense qu'il faut afficher la plus grande des exigences et des rigueurs pour faire en sorte que l'Internet, s'il veut survivre, soit régulé par la loi.

Outre-Atlantique, certains ingénieurs de la Silicon Valley, l'un des cofondateurs de Facebook lui-même Chris Hughes, évoquent aujourd'hui le nécessaire démantèlement de ces plateformes. En effet, elles sont devenues tentaculaires et hégémoniques, ce qui fait peser un risque sérieux sur nos démocraties, sur nos États nations. Par ailleurs, elles sapent tous les moyens de l'action publique, sans que rien ne soit fait.

L'heure est grave, il faut sortir rapidement d'une forme de complaisance. Je regrette qu'en France, on déroule le tapis rouge à Mark Zuckerberg qui vient, la main sur le cœur, dire que les plateformes vont s'autoréguler, je n'y crois pas une seconde.

Chers collègues, Mesdames et Messieurs, comme vous le voyez, nous sommes à la croisée des chemins, et il est plus que temps de reprendre en main notre destin numérique. Je vous remercie de votre attention.

Cybersécurité, protection des données, manipulation : approches comparatives en Allemagne, en France et en Pologne

Table ronde animée par Bernard BENHAMOU, secrétaire général de l'Institut de souveraineté numérique

En présence de :

M. Jean-Marie BOCKEL, Sénateur du Haut-Rhin, ancien ministre, membre de la commission des Affaires étrangères, de la Défense et des Forces armées,

M. Philippe BONNECARRERE, Sénateur du Tarn, membre de la commission des Lois et de la commission des Affaires européennes,

M. Olivier CADIC, Sénateur représentant les Français établis hors de France, membre de la commission des Affaires étrangères, de la Défense et des Forces armées,

M. Rachel MAZUIR, Sénateur de l'Ain, membre de la commission des Affaires étrangères, de la Défense et des Forces armées,

M. Łukasz MIKOŁAJCZYK, Sénateur, Vice-Président de la commission des Droits de l'homme, du respect des lois et des pétitions, Sénat de Pologne,

M. Till STEFFEN, Président de la commission des Lois du Bundesrat, Allemagne,

M. Kamil BASAJ, Safe Cybertrust Foundation, Pologne,

M. Christian DAVIOT, conseiller stratégie auprès du directeur général, Agence Nationale de Sécurité des Systèmes d'Information (ANSSI), Premier ministre,

Mme Frederike KALTHEUNER, Privacy International, Allemagne.

I) Propos préliminaires

Bernard BENHAMOU

Madame la Présidente,

Monsieur le Président,

Mesdames et Messieurs,

Chers invités,

Cela a été un grand plaisir d'avoir participé à l'organisation de ces travaux sur un sujet particulièrement intéressant et central dans nos sociétés. Madame la Présidente, vous avez rappelé l'urgence de ces questions. Je citerai une personne présente dans la salle qui insistait il y a vingt ans sur le « sentiment de pénibilité » ressenti par les utilisateurs lorsque les sujets liés à la cybersécurité étaient évoqués.

Ces thématiques ne doivent pas être abordées de la sorte. En effet, elles deviennent centrales pour la protection de ce que nous sommes, à la fois au niveau des États, mais aussi des personnes, car elles visent à protéger nos infrastructures mais aussi à éviter la marchandisation des données personnelles. Or ces attentes sont au cœur des valeurs portées par l'Europe. Le RGPD (Règlement Général de Protection des Données) est symbolique de cette approche, et nous est parfois même envié à l'étranger.

Pour autant, nous devons aller encore plus loin dans le traitement de ces questions. En effet, les menaces évoquées précédemment concernent l'ensemble des États et mettent en danger nos démocraties.

Certains ont pu évoquer le cas de la fusion entre Facebook et WhatsApp pour conclure à l'impuissance de la Commission européenne. Je rappelle que l'Europe avait déjà réussi à empêcher dans le passé une fusion entre des entreprises purement américaines, à l'instar de celle entre General Electric et Honeywell pour des turbines d'avion.

Ces questions doivent être appréhendées de manière pragmatique, en écartant tout sentiment de fascination technologique. En effet, il ne s'agit pas de questions qui se cantonnent à la sphère technologique. Elles s'inscrivent pleinement dans nos vies politiques, notamment lorsque des attaques extérieures visent à déstabiliser nos démocraties.

Face à cette menace, une réaction est nécessaire. La protection des données et la cybersécurité deviendront des marqueurs européens qui pourraient devenir autant d'avantages compétitifs si nous savons nous en saisir pour développer nos industries technologiques. Il faut donc cesser de les concevoir comme des freins au développement économique.

Madame la Présidente, vous évoquiez la tenaille entre le modèle libéral, le laisser-faire américain, et celui quasiment dictatorial de la Chine dans lequel chaque individu est noté et risque de perdre ses droits sociaux s'il dévie du « droit chemin » établi par les autorités chinoises. Notre objectif doit être de créer une troisième voie qui pourrait servir de base pour créer un nouveau modèle économique pour les technologies.

L'un des enjeux majeurs des temps qui viennent pour la France et l'Europe sera donc de permettre l'éclosion de cette troisième voie respectueuse des principes et des valeurs des Européens.

II) L'état des risques en matière de cybersécurité

Bernard BENHAMOU

Nous allons aborder cette première table ronde par un état des risques en matière de cybersécurité. Commençons notre tour de table par l'analyse de Monsieur Christian Daviot, conseiller à l'ANSSI.

Christian DAVIOT

Je tiens à préciser que je m'exprime ici en mon nom personnel, et non en tant que représentant de l'ANSSI.

Nous connaissons tous la nature des menaces qui existent. Elles sont énormément partagées et commentées. Je souhaite évoquer une menace bien plus dangereuse, de nature politique, qui se retrouve dans les trois pays représentés aujourd'hui. Hannah Arendt avait écrit que c'est dans le vide de la pensée que s'inscrit le Mal. Il me semble qu'il est urgent de réfléchir à la définition de certaines notions à l'aune du droit international. Ainsi, l'ONU avait précisé que le droit international s'appliquait à l'espace numérique. Toutefois, il n'existe aucune définition de ce territoire. L'Europe ne peut pas faire l'économie de cette réflexion, préalable nécessaire à toute définition d'une troisième voie.

Selon moi, la menace réside dans le fait de ne pas définir ces termes. Pour ce faire, les parlementaires et l'ensemble des acteurs de la société civile doivent s'associer à des experts pour évoquer ces notions et fixer un cadre clair. Le fait que personne ne travaille dans ce sens à l'heure actuelle constitue le plus grand danger.

Bernard BENHAMOU

Voyons désormais comment ces mêmes menaces sont perçues en Allemagne.

Till STEFFEN

Les menaces proviennent d'origines très différentes et le risque est de n'en retenir que certaines parmi elles. Quelqu'un a évoqué les grands groupes à l'instar de Facebook qui doit parfois être traité comme une organisation aux méthodes criminelles en raison de son pouvoir économique. Il me semble donc absolument nécessaire d'avoir ces échanges aujourd'hui.

Bernard BENHAMOU

Évoquons enfin l'angle de vue de nos voisins polonais sur les questions de cybersécurité et de protection des données.

Łukasz MIKOŁAJCZYK

C'est un sujet très important. Les attaques cybernétiques vont aller en augmentant avec le développement des menaces. Dans notre quotidien à tous, citoyens, administrations ou entreprises, la réalité virtuelle gagne en importance, ce qui élève d'autant le risque d'attaques et de manipulations.

Une autre menace découle de l'augmentation des capacités opérationnelles des organisations terroristes. Notre priorité doit donc être de renforcer nos capacités nationales de réponse. Un groupe de travail a été mis en place auprès du ministère compétent en Pologne, complété par des formations appropriées au sujet de la désinformation. Enfin, nous avons créé un site web pour informer les citoyens sur ces sujets.

III) La sensibilisation des utilisateurs aux risques en matière de cybersécurité

Bernard BENHAMOU

Dans quelle mesure les utilisateurs peuvent-ils être accompagnés au mieux par des mesures politiques d'encadrement ?

Philippe BONNECARRERE

À ce jour, il me semble que les citoyens ne sont pas suffisamment sensibilisés à ces questions. La situation ressemble à une course de vitesse entre le développement numérique d'une part et la multiplication des objets connectés et des réseaux d'autre part.

Le retard que nous avons eu à réagir est d'autant plus dangereux que le risque n'est pas physique. En matière numérique, nous ne percevons pas le danger, ce qui rend d'autant plus difficile le travail de sensibilisation.

En France, notre approche de ces sujets s'est jusque-là cantonnée à la sphère juridique. Cela s'est traduit par la mise en place du RGPD, par la suite complété par des mesures nationales. Cet arsenal de textes est certes nécessaire, mais il ne constitue pas une réponse suffisante.

Selon moi, il nous faut gagner le combat de la culture numérique. Je relève malgré tout quelques éléments prometteurs. À titre d'exemple, une option numérique sera mise en place dès l'an prochain au sein du baccalauréat. Il reste encore à former les professeurs à cette dimension nouvelle dans leur enseignement.

Cette culture doit être dispensée dès le plus jeune âge. Mon petit-fils de huit ans maîtrise l'aspect technique d'un mobile, mais est dépourvu de toute connaissance en matière de sécurité numérique. La culture numérique doit donc être appréhendée tant du point de vue technique que sécuritaire.

Bernard BENHAMOU

Quelles mesures d'accompagnement des citoyens ont-elles été adoptées en Allemagne ?

Frederike KALTHEUNER

Je tiens à souligner à quel point l'utilisateur est le maillon faible dans ce contexte. Par conséquent, il ne s'agit pas de lui faire supporter la responsabilité des problèmes de sécurité. En décembre 2018, nous avons analysé l'application mobile la plus populaire avec ses dix millions d'utilisateurs. Au terme de l'étude, il s'est avéré que plus de 60 % des données étaient partagées, en totale contradiction avec le RGPD.

Cet exemple démontre l'écart entre ce qui est affiché par l'Union européenne et la réalité des faits. Par ailleurs, ces questions sont intimement liées à la notion de justice sociale. En effet, beaucoup d'utilisateurs ne peuvent pas investir dans des appareils haut de gamme. En se reportant sur du matériel bon marché, ils s'exposent à des smartphones présentant plus de failles de sécurité.

En règle générale, ces problématiques échappent pour beaucoup à la conscience des citoyens.

Bernard BENHAMOU

Ces sujets doivent effectivement être abordés avec tous les régulateurs nationaux. Quels sont les angles d'accompagnement proposés en Pologne ?

Kamil BASAJ

Le besoin d'éducation ne pourra jamais être complètement assouvi. Le monde numérique se complexifie à une telle vitesse que le niveau de compétence requis pour le maîtriser augmente continuellement. Par exemple, l'utilisation croissante des systèmes interconnectés implique une formation des citoyens aux risques encourus d'un détournement malveillant de ces outils. L'État doit pleinement assumer sa responsabilité face à ces risques nouveaux.

Or, la cybersécurité ayant une portée transfrontalière, les actions menées doivent l'être conjointement. De même, il apparaît nécessaire d'alerter davantage les utilisateurs sur ces questions.

IV) La préparation des États européens face aux risques en matière de cybersécurité

Bernard BENHAMOU

Je vous remercie d'avoir souligné que les potentiels d'attaque n'en sont qu'à leur début et que leur essor semble inexorable avec le développement des objets connectés. C'est l'occasion de s'interroger sur la capacité des États européens à affronter ces enjeux. Quelles sont les évolutions législatives possibles pour encadrer ces domaines ?

Je note d'ailleurs que ceux-ci posent de réels problèmes pour la souveraineté des États ; pour illustrer mon propos, je citerai notamment le lancement de la nouvelle monnaie de Facebook, Libra. La création d'une monnaie par un opérateur privé soulève de nombreuses questions.

Qu'en pensez-vous, Rachel Mazuir ?

Rachel MAZUIR

Je constate que nous partageons tous des doutes et des espoirs face à ces questions. En France, la nécessité de traiter de ces sujets a été affirmée dès 2008 dans le *Livre blanc*

de la Défense nationale, puis en 2017. L'ANSSI a été mise en place en 2009. Cette agence est reconnue au plan international et son activité n'a cessé de croître.

Par ailleurs, la France s'est dotée d'un cadre législatif et réglementaire solide, notamment dans le secteur électronique. Ainsi, il est prévu l'obligation pour les opérateurs de télécom d'apporter leur concours dans la détection des attaques.

Le lancement de la 5G soulève de nouvelles questions. Dans l'objectif de préserver davantage la sécurité numérique, une proposition de loi sera soumise aux parlementaires dans quelques jours. Celle-ci contient certains axes totalement nouveaux au plan international.

Enfin, il me semble fondamental d'assurer la protection des réseaux interconnectés. Or le niveau de cybersécurité européen est directement lié au niveau de sécurité de chaque État. Il est donc essentiel de doter l'Europe de normes et d'objectifs communs pour être en mesure d'assurer un socle solide de cybersécurité dans tous les États membres.

Je conclurai par une citation : *« Le meilleur chef de guerre est celui qui la prépare et la gagne sans avoir à la faire. »*

Christian DAVIOT

Je précise que les capacités offensives et les capacités défensives sont strictement séparées dans notre modèle français. Ainsi, l'ANSSI est une agence uniquement dotée d'un rôle défensif.

Bernard BENHAMOU

Voyons désormais quel est le point de vue de l'Allemagne.

Till STEFFEN

Beaucoup d'éléments pertinents ont été rappelés. Je voudrais évoquer un point essentiel pour l'Europe. Les États membres reposant sur des systèmes démocratiques, ils dépendent de la confiance que leur accordent les citoyens. Or les campagnes de désinformation orchestrées depuis l'étranger tentent de déstabiliser nos États. Par exemple, des robots créant de faux comptes sur des forums ou des réseaux sociaux visent à faire croire à l'expression de certaines opinions. Nous devons en prendre conscience, car ces situations sont très dangereuses pour nos démocraties. En Allemagne, nous avons relevé plusieurs actions de ce type en provenance de Russie. Il est urgent de se protéger contre ces phénomènes.

Face à ces risques, nos débats démocratiques restent trop souvent cantonnés à la sphère nationale, notamment en raison des barrières linguistiques. Le risque de ce cloisonnement est de ne percevoir qu'une partie des débats menés dans les États voisins. Cela crée une porte d'entrée pour ceux ayant des intentions malveillantes à notre égard.

Toutes les préconisations évoquées ici ne pourront être mises en place qu'à la condition de conserver une approche démocratique de ces sujets. Nous devons renforcer le dialogue entre nous et mener des campagnes de sensibilisation auprès des citoyens.

Par ailleurs, il faut réfléchir à notre capacité à réagir face à ces campagnes particulièrement bien ciblées qui sont à l'origine de nombreux débats publics. La Commission européenne doit donc se doter d'outils adaptés pour affronter ces situations.

Bernard BENHAMOU

À ce sujet, je rappelle que pour le seul premier trimestre de l'année 2018, Facebook avait supprimé 583 millions de faux comptes, soit un quart de l'ensemble des comptes actifs. En effet, ces faux comptes étaient utilisés pour influencer l'opinion. À cette échelle, il ne s'agit donc plus d'artisanat, mais d'industrie lourde en matière de manipulation de masse. Quelle est sur ce point la position de la Pologne ?

Łukasz MIKOŁAJCZYK

Quand on évoque la cybersécurité, on ne peut pas espérer atteindre la sécurité totale. Il est nécessaire d'adopter des mesures déterminées face aux attaques, ce qui implique d'adapter la législation à l'environnement qui change. Chaque État dépend certes de sa propre infrastructure, mais aussi de l'infrastructure internationale.

Nous construisons peu à peu un système visant à développer nos capacités de réaction, mais une course de vitesse s'engage alors en permanence entre les menaces et les réponses que nous y apportons. À ce jour, tous les secteurs économiques présentent de grandes vulnérabilités. Il est donc nécessaire de développer nos capacités à lutter contre toutes ces menaces.

V) L'approche souhaitable de l'Europe dans le domaine de la 5G

Bernard BENHAMOU

Nous allons aborder un point qui a suscité de nombreuses tensions entre les États-Unis et la Chine. Il s'agit du cas de l'entreprise Huawei dont les produits ont été accusés de présenter des failles de sécurité introduites volontairement par le constructeur. Quelle doit être notre attitude face à ce type de situation alors même que la 5G en est actuellement à sa phase de déploiement ?

Jean-Marie BOCKEL

Il me semble pertinent d'aborder ce sujet à l'occasion de ce travail commun mené avec l'Allemagne et la Pologne. J'étais à une réunion de l'assemblée parlementaire de l'OTAN au cours de laquelle j'ai présenté un rapport sur les enjeux numériques et la cyberdéfense. Y a été évoqué le cas de l'entreprise Huawei. Cette question n'est pas nouvelle.

À titre personnel, j'avais un *a priori* prudent à l'égard de ce géant chinois, découlant de la doctrine française qui s'est forgée au fil des années. Elle invite à la fois à la prudence et à rester attentifs face au danger que certains produits fassent office de cheval de Troie. Il convient donc de trouver un bon équilibre entre une attitude purement naïve et une posture excessivement négative. Dans ce contexte, nous avons admis que Huawei pouvait se développer sous certaines conditions. De son côté, la Grande-Bretagne s'est alignée sur la position américaine qui avait décidé l'interdiction pure et simple de commercialisation. L'Allemagne a également adopté une position équilibrée. Il me semble qu'il en est de même en Pologne.

Dans cet environnement géopolitique confronté à certaines interdictions, que doit faire l'Europe ? Cette question suscite une autre question : qu'en sera-t-il du « *deal* » à l'arrivée, pour reprendre l'expression du Président Donald Trump ? Dans le cadre des négociations commerciales menées actuellement entre la Chine et les États-Unis, un *deal* est annoncé. La question est donc de savoir si l'entreprise Huawei en fera partie.

Je sais que l'ANSSI se pose les mêmes questions. Devons-nous adopter une vision identique à celle des Américains ou développer notre propre approche ? Dans le second cas, il faut évidemment appréhender cette question à l'échelle européenne. Seuls, nous ne serions pas en capacité à le faire face aux géants que sont les États-Unis et la Chine.

Bernard BENHAMOU

Sur ces questions très techniques, il est intéressant d'avoir le point de vue des experts en matière de sécurité. Je passe donc la parole à Christian Daviot.

Christian DAVIOT

Un texte de loi est actuellement en discussion en France. Personnellement, je constate que les positions adoptées en Grande-Bretagne, en Allemagne et en France sont subtiles, car elles ne visent pas un constructeur nommément.

De manière générale, nous devons rester vigilants face aux équipements. Dans le cadre des révélations de l'affaire Snowden, un constructeur américain avait été mis en cause. Cela démontre bien qu'il ne faut pas accorder une confiance aveugle à quelque industriel que ce soit.

Bernard BENHAMOU

Quelle est la position de l'Allemagne sur ce sujet ?

Till STEFFEN

Selon moi, le gouvernement allemand n'a pas une attitude assez ferme. Il reste prudent, ce qui provoque certaines incohérences dans sa démarche. Nous avons ainsi décidé d'autoriser le déploiement de la 5G tant que nous ne serions pas dépendants des produits Huawei.

Or, sans aller jusqu'à affirmer que seuls les produits européens sont autorisés en Europe, nous devrions tout de même apporter une alternative européenne dans le domaine des infrastructures. Cette réponse doit être au même niveau que l'exemple d'Airbus. Pour mémoire, quand Airbus avait été mise en place, se posait aussi ce problème de monopole pour l'entreprise Boeing.

Nous devons donc soutenir ce type de démarche, qui implique évidemment des compétences et des moyens adaptés, mais aussi une coopération entre les agences européennes et les agences nationales.

En mutualisant nos efforts, il sera possible de nous doter d'armes appropriées face à ces problématiques.

Bernard BENHAMOU

À ce propos, la France et l'Allemagne ont décidé de coopérer en vue de mettre en place une alternative européenne. À défaut, cela engendrerait une vulnérabilité accrue de l'Europe. Qu'en est-il de la Pologne ?

Łukasz MIKOŁAJCZYK

Bien entendu, la Pologne partage l'objectif de sécurité qui est affirmé ici. Nous sommes actuellement dans une phase de consultation des opérateurs de télécom qui sont des partenaires à part entière. La question du déploiement de la 5G doit être traitée pleinement, car à terme la 5G pilotera tous les systèmes et accélérera le développement du numérique.

Je partage l'idée que la réponse doit émaner de l'Europe entière.

Frederike KALTHEUNER

Cette question renvoie à celle de la domination des États-Unis et de la Chine et suppose avant tout de définir quelles sont les innovations souhaitables, au lieu de la réduire aux problématiques de concurrence.

À titre personnel, je voudrais recentrer ce débat sur les droits individuels qui sont ceux qui pâtissent en premier lieu de ces risques. L'Union européenne doit s'évertuer à développer une stratégie plus axée sur la protection des données. À ce titre, elle ne doit pas se diriger vers les modèles américains et chinois qui se cantonnent aux aspects concurrentiels.

VI) Les capacités offensives de l'Europe dans les cyberguerres potentielles

Bernard BENHAMOU

Parmi les différentes perspectives se pose la question d'une guerre potentielle qui prendrait appui sur l'attaque de nos infrastructures numériques. Dans ce contexte, nous allons plus particulièrement nous interroger sur nos capacités offensives. En effet, passé un un certain point, résister devient une stratégie insuffisante, qui doit être complétée par des actions offensives. Pour évoquer cette question, écoutons le point de vue d'Olivier Cadic.

Olivier CADIC

Je tiens d'abord à affirmer que nous sommes actuellement en guerre. Cela me désole, mais il faut prendre conscience que les temps ont changé. La dernière déclaration de guerre officielle d'un État européen date de 1982 et émanait du Royaume-Uni contre l'Argentine. Pour autant, les Russes testent chaque jour nos systèmes de défense. Par exemple, ils ont cherché à brouiller nos systèmes de communication dans la Marine.

Quant à elle, la Chine a clairement affirmé que son objectif était de dominer le monde d'ici 2050 et elle considère que nos systèmes démocratiques sont dépassés. De l'autre côté, les Américains considèrent le monde comme un territoire qu'ils doivent dominer sur le plan économique.

Au-delà des États, il existe des organisations criminelles et des groupes terroristes qui cherchent à atteindre la réputation des démocraties. Parfois même, la cible visée présente un caractère vital, à l'instar de l'attaque récente contre nos systèmes d'approvisionnement en eau.

Je disais que votre présent est notre passé. Lorsque nous commentons l'actualité, elle est déjà révolue. Ainsi, la Libra a été commentée cette semaine alors même que cette monnaie est un projet développé par Facebook depuis des années. Cela démontre que nous sommes perpétuellement en retard.

Face à ces enjeux, la mise en place de capacités offensives est la moindre des choses. Ainsi, la ministre de la Défense a annoncé en début d'année que la France allait se doter de moyens offensifs. Ces techniques ont d'ores et déjà été utilisées à l'encontre de Daech.

Le cœur de notre système est visé. Je citerai les trolls qui visent le compte Twitter du Président de la République. Cela fait d'ailleurs des années que je réclame la mise en place d'un vaccin électronique pour contrer ce type d'action.

Par conséquent, nous sommes confrontés à des défis tels que nous ne pourrons les relever seuls. La seule solution est donc une union entre tous les États membres, ce qui suppose au préalable de définir des priorités.

Bernard BENHAMOU

C'est effectivement un sujet sensible. Qu'en est-il de la doctrine allemande sur ces questions ?

Till STEFFEN

Ce qui a été décrit est juste. Nous sommes confrontés à des situations bien plus dangereuses que dans des guerres traditionnelles. Pendant ma jeunesse à Francfort, plusieurs scénarios de réponse nous préparaient à une éventuelle attaque de chars russes.

À ce jour, les menaces liées à une attaque Internet sont susceptibles de provoquer des dégâts potentiels bien plus grands. L'exemple de l'attaque du système d'approvisionnement en eau le démontre.

De surcroît, la menace peut à la fois venir d'une organisation criminelle, d'un groupe terroriste ou d'individus isolés. Pour autant, je reste prudent lorsque nous évoquons la stratégie d'une contre-attaque. Il est certes possible de repousser les attaques quotidiennes qui se présentent par millions, mais si nous décidons de riposter, comment identifier la cible ? Comment être certain de viser juste ? En effet, un doute subsiste toujours quant à l'origine de l'attaque, ce qui implique de rester vigilant au risque d'un effet domino dangereux.

Olivier CADIC

Se doter de capacités offensives présente l'avantage que le camp d'en face se sente également menacé. En outre, si nous restons cantonnés à un système purement défensif, nous sommes exposés au risque qu'il ne fonctionne plus.

L'exemple de Huawei est éloquent : nous avons accepté la commercialisation de ses produits, alors même que la réciproque n'est pas appliquée en Chine. Selon moi, cette attitude est suicidaire et démontre que le modèle chinois pose problème. Je pose la question : à quel moment déciderons-nous de changer notre comportement ?

Jean-Marie BOCKEL

Les capacités offensives de la France sont récentes. L'évolution notable est qu'il existe désormais une doctrine d'emploi. À l'époque, j'avais pris connaissance des systèmes offensifs de manière confidentielle. Si la confidentialité attachée à ces techniques ne me paraissait pas problématique, je restais perplexe quant à l'absence de doctrine d'emploi.

Par ailleurs, ces techniques ne produisent leurs effets dissuasifs que si elles s'accompagnent de réelles actions. Je me réjouis que nous soyons passés du « faire sans dire » au « faire en annonçant la couleur ».

Reste le point sensible de l'échelle des systèmes offensifs. Selon moi, ce domaine se prête davantage à des coopérations bilatérales qu'à un système plus large. En effet, plus les États sont nombreux à s'engager dans ce type d'action, plus les vulnérabilités de chacun sont accentuées.

La politique de défense doit donc permettre en premier lieu une montée en puissance de chacun. Cela implique de concilier la souveraineté nationale avec une action conjointe.

Bernard BENHAMOU

Comment ces sujets sont-ils traités par la Pologne ?

Łukasz MIKOŁAJCZYK

Il s'agit effectivement d'un sujet sensible et traité comme tel par la Pologne. Je suis tout à fait d'accord avec les propos précédents. Nous devons agir de concert aux niveaux national et international. De plus, il faut créer les conditions d'une coopération entre les plateformes internet et la sphère sociale. Cela impliquera la mise en place de partenariats public / privé qui permettront de contrecarrer toute action de désinformation. À terme, la sécurité en sera améliorée.

VII) Le rôle de l'Union européenne dans le domaine de la cybersécurité

Bernard BENHAMOU

Nous allons évoquer la dernière partie de cette première table ronde. Quel pourrait être le rôle de l'Union européenne dans la cybersécurité ? Cette question suscite de nombreux débats. Quels sont vos commentaires à ce propos, Philippe Bonnecarrère ?

Philippe BONNECARRERE

Nous espérons tous que l'Union européenne pourra assumer complètement son rôle dans ce domaine. En effet, la menace n'est pas limitée territorialement. Nos États sont tous perméables et interdépendants. Aussi serait-il inopérant de traiter ce sujet exclusivement au plan national.

Nous sommes dotés de certaines dispositions réglementaires, à l'instar du RGPD. De même, l'Union européenne a mis en place une Agence dont le rôle progresse peu à peu : l'Enisa.

Pour autant, l'Union européenne doit développer son action sur un plan culturel en instaurant chez les citoyens des automatismes de sécurité. Il faut dégager des réponses adaptées aux risques numériques.

Par conséquent, il me semble que notre combat doit être de basculer d'une réponse purement juridique à une réponse globale en la matière. Bien entendu, cette évolution demande un certain temps.

Bernard BENHAMOU

Quelle est l'attitude de l'Allemagne dans ce domaine ? Quelles sont ses préconisations ?

Till STEFFEN

Dans mon approche du sujet, j'essaie toujours d'inclure la dimension européenne. Cette question nous interroge tous en tant que décideurs politiques. Il est fondamental que nous surmontions nos divergences politiques, au lieu de les aggraver. Ensemble, et non les uns contre les autres, nous pourrons relever ces défis nouveaux.

Cette approche conjointe doit également valoir pour la réglementation. Au sujet du RGPD, l'Allemagne avait refréné la France au sujet de la coopération entre les différentes agences de sécurité. Ce type de comportement doit être combattu. Il faut que nous fassions tous des efforts au risque de ne pas être en mesure de résoudre ces problèmes.

Bernard BENHAMOU

Merci de cette franchise. Un dernier mot de Łukasz Mikołajczyk à propos de l'action européenne.

Łukasz MIKOŁAJCZYK

L'Union européenne présentant un énorme potentiel technique, scientifique et humain, il est nécessaire d'y puiser. Tout ce qui a été évoqué est juste, nous devons coopérer sur ces sujets à l'échelle européenne. Pour ce faire, il faut rechercher un consensus qui permettra de dégager des solutions communes dans l'Union européenne. Les actions menées par les entreprises doivent également être intensifiées et prendre une dimension européenne.

L'intelligence artificielle : quels enjeux éthiques, industriels et politiques ?

Table ronde animée par Bernard BENHAMOU, secrétaire général de l'Institut de souveraineté numérique

En présence de :

M. André GATTOLIN, Sénateur des Hauts-de-Seine, membre de la commission des Affaires européennes, auteur d'un rapport d'information sur « une stratégie européenne pour l'intelligence artificielle »

M. Gérard LONGUET, Sénateur de la Meuse, ancien ministre, Président de l'office parlementaire d'évaluation des choix scientifiques et technologiques, rapporteur de la commission d'enquête du Sénat sur la souveraineté numérique

M. Konstanty RADZIWIŁŁ, Sénateur, ancien ministre, Sénat de Pologne

M. Till STEFFEN, Président de la commission des Lois du Bundesrat, Allemagne

M. Anthony COLOMBANI, Fédération française des télécoms

M. Wojciech ORLIŃSKI, journaliste polonais

I) La nécessité d'établir une stratégie éthique propre à l'Europe

Bernard BENHAMOU

Force est de constater qu'à l'heure actuelle, l'Europe n'occupe pas la place qui devrait être la sienne sur l'intelligence artificielle. Certains d'entre vous ont d'ailleurs pu travailler sur ces questions.

Nous ne pouvons pas nous réjouir de voir les meilleurs cerveaux européens partir travailler pour des entreprises américaines ou chinoises. Cette question concerne tout autant l'opinion publique. Enfin, l'intelligence artificielle jouera un rôle dans l'ensemble des secteurs économiques et sociaux, ce qui implique de la placer au cœur de nos réflexions politiques.

Nous allons commencer avec André Gattolin. Que pensez-vous des actions et politiques publiques dans ce domaine ? Jusqu'où doivent-elles aller ? Plusieurs débats ont eu lieu au sujet de la bioéthique. Faut-il faire de même pour l'intelligence artificielle ?

André GATTOLIN

Je le pense. Les travaux de Cédric Villani mettent l'accent sur l'importance de définir une éthique dans le domaine de l'intelligence artificielle. Cela me semble effectivement indispensable. La Commission européenne a commencé à appliquer sa feuille de route sur ce sujet dans le but de traduire la vision particulière de l'Europe à ce propos et afin qu'elle soit conforme à notre modèle démocratique.

Nous autres Européens avons une théorie légiste issue de la construction philosophique et politique de ce continent. Cela induit une attention toute particulière tant au respect des libertés individuelles qu'au droit des peuples et des nations. Dans ce contexte, le monde de l'intelligence artificielle doit être à même et de garantir le respect de l'ensemble de ces libertés.

Pour autant, il me semble qu'il ne faut pas mettre en place une législation trop contraignante qui aurait pour effet de restreindre le développement de l'intelligence artificielle sur le terrain économique. Notre approche doit donc être équilibrée.

II) L'instauration d'un débat démocratique sur les questions d'intelligence artificielle

Bernard BENHAMOU

Nous assistons à un déploiement considérable des assistants personnels intelligents qui font naître de nouveaux risques pour leurs utilisateurs. À ce jour, 20 % des Américains en sont équipés. Dans ce contexte, que pensez-vous de la nécessité d'un débat démocratique sur ces questions ? Serait-il utile ?

Till STEFFEN

Tout à fait. Nous avons besoin d'un débat public. Je constate une grande confusion dans l'opinion à l'heure actuelle, ce qui me paraît très risqué. Un groupe de travail au sein de mon parti traite des programmes informatiques. L'un des experts a remarqué que la notion d'intelligence artificielle avait succédé à celle de logiciel ; l'écueil serait de qualifier d'intelligence artificielle tout logiciel difficile à comprendre et plus largement d'employer dans le débat public des mots-clés inappropriés aux situations. Plus personne ne semble comprendre quels sont les sujets évoqués.

Par ailleurs, nous devons assumer nos responsabilités face aux produits mis sur le marché. Plus de transparence est également nécessaire au sujet des services liés à ces outils nouveaux.

Enfin, je note que les débats concernant le cadre réglementaire, d'une part, et l'éthique, d'autre part, doivent être nettement distingués. Or, à ce jour, seul le débat sur la réglementation a lieu, ce que je déplore.

Bernard BENHAMOU

Quelles seraient les pistes d'amélioration en la matière dans ce cas ? Monsieur le Ministre, qu'en pensez-vous ?

Gérard LONGUET

Je souligne tout d'abord que le Parlement français est tout à fait en mesure d'établir un état des lieux sur ce sujet, et a su le prouver toutes les fois où tant le Sénat que l'Assemblée nationale en ont formulé le besoin.

Il nous faut trouver un chemin vraisemblable entre les deux positions excessives que nous rencontrons trop souvent : d'une part, celle consistant à considérer l'intelligence artificielle comme un moyen de déposséder l'être humain de son autonomie ; d'autre part, celle qui consiste à minorer son importance, la réduisant à un simple système. D'un côté, il s'agit d'un scénario apocalyptique, alors que l'autre tend à banaliser l'intelligence artificielle. Notre regard doit donc trouver le juste milieu entre ces deux voies.

J'ai toujours eu beaucoup d'admiration pour la démocratie allemande qui repose sur les principes de décentralisation et de scrutin proportionnel. En France, ces deux principes nous sont totalement étrangers. Cela conduit malheureusement les citoyens à abandonner leur responsabilité individuelle dans la participation au débat public. Peu à peu, les seules questions publiques débattues se réduisent à s'intéresser au nom du prochain responsable politique.

Or les débats relatifs à l'intelligence artificielle se sont écartés de la sphère politique et partisane, non pas en raison de leur difficulté, mais plus du fait de la perception que la décision sur cette matière repose sur le pouvoir exécutif.

Bernard BENHAMOU

Peut-être que les systèmes d'intelligence artificielle pourraient modifier les débats en raison des perspectives nouvelles d'influence sur les populations.

Gérard LONGUET

À ce propos je voudrais faire une remarque : l'analyse des électeurs n'est pas nouvelle. Ce qui est innovant, c'est la capacité à donner des informations plus détaillées.

Bernard BENHAMOU

Qu'en est-il de ce sujet en Pologne ?

Konstanty RADZIWIŁŁ

Ce débat est passionnant, mais bien plus complexe que celui de la première table ronde. En effet, il contient des questions centrales pour notre avenir, qu'il faut aborder avec beaucoup de pédagogie. L'opinion publique se figure souvent des robots se retournant contre l'être humain, devenant incontrôlables.

Cette vision caricaturale doit être combattue. Cet outil que constitue l'intelligence artificielle doit être mieux appréhendé. Il nous faut évidemment mettre en garde nos sociétés sur certaines formes d'intelligence artificielle, afin que les citoyens soient sensibilisés à certains risques.

Toutefois, l'intelligence artificielle est en mesure de nous apporter des bénéfices incroyables, notamment sur le plan de la santé. Il en est de même avec les voitures autonomes ou la gestion des villes. Pour autant, ces outils ne doivent pas être pris en compte comme de banals produits. L'Union européenne essaie de poser un cadre dans la directive relative à la responsabilité du fait des produits, mais cela n'est qu'un début.

Mis entre des mains malveillantes, cet outil peut se transformer en arme, tant individuelle que de destruction massive. Cela implique de traiter cet outil avec précaution, comme nous nous y employons avec certains secteurs sensibles du type nucléaire.

III) La perspective d'une définition éthique propre à l'Europe

Bernard BENHAMOU

Nous allons poursuivre avec les questions éthiques. Que pourrait décider l'Europe pour dessiner son propre chemin ? À ce sujet, Anthony Colombani pourrait nous éclairer dans la mesure où il travaille dans le secteur des télécoms.

Anthony COLOMBANI

Sur la nécessité de choisir une voie intermédiaire, l'Europe peut et doit même le faire. Elle a déjà commencé à mettre en place des lignes directrices excellentes sur ce sujet, par exemple la réglementation qui vise à interdire les armes létales autonomes. Il faut admettre que la régulation concernant la vie privée entraînera une limitation des progrès.

Pour autant, nous devons concevoir l'éthique comme une condition de l'acceptation sociale de l'intelligence artificielle, plus que comme une barrière. À défaut, cela ne fonctionnera pas. En effet, si la population prend conscience que l'intelligence artificielle porte atteinte à la vie privée, elle se dressera contre. Un cadre éthique est donc absolument nécessaire au développement de cette industrie. C'est un enjeu civilisationnel qui se trouve devant nous. D'ailleurs, les questions philosophiques font partie prenante des recherches actuellement menées par les développeurs de très haut niveau.

Bernard BENHAMOU

Abordons maintenant la vision allemande sur cette question.

Leonie BEINING

J'approuve également les directions que prend l'Union européenne actuellement. Nous devons garder à l'esprit que les technologies sont mondialisées. À ce titre, différents pays développent leur propre ligne de conduite et l'Europe doit se doter de la sienne. En particulier, il apparaît essentiel de décider de la manière dont les normes seront transposées dans les États membres.

Je citerai le cas de la Chine qui officiellement adopte un cadre de protection de la vie privée, même si, en réalité, nous savons tous que ces questions ne trouvent pas d'application effective.

Bernard BENHAMOU

Abordons maintenant la vision polonaise des enjeux éthiques liés à l'intelligence artificielle.

Wojciech ORLIŃSKI

Cette conférence est très intéressante. Elle démontre un certain consensus à propos de la nécessité d'une régulation. Jusqu'à récemment, cette vision était peu partagée par l'opinion publique polonaise. Et il me semble que les générations suivantes jugeront cette attitude de la population comme une erreur immense.

Cela démontre à quel point il existe des divergences entre les différentes réglementations nationales. Cela constitue même un argument pour certains États étrangers, qui mettent en avant cette faiblesse de l'Europe.

Selon moi, nous devons nous orienter dans trois directions. Tout d'abord, soyons en mesure de déterminer si nous parlons avec un homme ou avec un robot. Dans le second cas, gardons à l'esprit qu'il ne s'agit pas toujours d'actions malveillantes. Ensuite, l'utilisation de l'intelligence artificielle ne doit pas exonérer l'utilisateur de sa responsabilité. Enfin, la transparence doit être la règle au sujet des algorithmes.

Par ailleurs, nous devons toujours être en mesure d'exercer des recours. C'est ce qui différencie un régime démocratique d'un régime totalitaire. A l'heure actuelle, nous avons le sentiment que le monde de l'Internet échappe à cette possibilité d'exercer des recours. Cela doit évoluer.

IV) La question de la transparence face aux algorithmes des industriels

Bernard BENHAMOU

La question de la transparence a été posée a de nombreuses reprises, notamment autour de Facebook. Je citerai les conséquences des modifications des algorithmes de Facebook et leur impact sur le nombre de personnes qui échangeaient à propos des « Gilets jaunes ». A l'heure actuelle, devons-nous imposer la transparence aux grandes plateformes quant à leurs algorithmes ? Monsieur le Ministre, quelle est votre position sur ces sujets ?

Gérard LONGUET

En toute honnêteté, nous ne sommes pas assez mûrs pour définir le point d'équilibre entre le respect de la propriété intellectuelle et l'impératif de protection des données. Or les dérives possibles des algorithmes, notamment dans le milieu de la santé, placent ce sujet au cœur des débats.

Je confirme que l'intelligence artificielle est un atout fantastique pour la santé, dans la mesure où elle rend possibles l'émission et le traitement de données de manière inédite.

Toutefois, nous pourrions aboutir à un système qui se retournerait contre l'intérêt général et aurait des effets néfastes tant pour la recherche médicale que pour le bien-être des patients.

En référence à l'époque où j'étais ministre des Postes, j'illustrerai ce risque par une comparaison : les dérives que j'évoque seraient comparables à un service postal gratuit, mais dans lequel l'utilisateur autoriserait le facteur à prendre connaissance du courrier. Au vu du nombre de données collectées, l'enjeu économique est énorme.

A l'heure actuelle, notre maîtrise de ces sujets est clairement insuffisante. Les évolutions économiques réduisent le choix de plusieurs entreprises entre s'adapter ou disparaître. En toute hypothèse, les débats menés au sein du Parlement européen me semblent tout à fait intéressants, dans la mesure où ils privilégient la notion de liberté à celle de régulation.

Bernard BENHAMOU

Doit-on pour vous imposer aux plateformes la transparence au sujet des algorithmes utilisés, selon la vision allemande ?

Till STEFFEN

À ce jour, l'Union européenne et l'ensemble de ses États membres se sont trop limités à l'adoption de normes inadaptées. Facebook doit être soumis aux lois antitrust, au même titre que les autres entreprises. Nous devons donc sérieusement envisager la mise en œuvre des contrôles que vous évoquez. Ce domaine économique doit nous impliquer de la même manière que les autres.

Bernard BENHAMOU

Comment se positionne la Pologne sur cette question ?

Konstanty RADZIWIŁŁ

Il me semble que nous avons commis l'erreur de faire confiance à la main invisible pour réguler ce marché. Cette croyance a pu être encouragée par plusieurs industries.

Ainsi, dans le domaine de la santé, les systèmes prédictifs pourraient être dévastateurs s'ils sont utilisés par des assureurs ou des employeurs.

S'agissant de Facebook, je me rappelle qu'une représentante de cette société était présente lors de notre conférence à Berlin. Lorsqu'elle a qualifié l'activité de son entreprise de publicitaire, l'ensemble de la salle a réagi. Or voilà qu'aujourd'hui cette même entreprise annonce le lancement d'une cryptomonnaie. Que devons-nous conclure de ses intentions réelles ? Est-ce là un moyen de collecter encore plus de données ?

Je voudrais d'ailleurs évoquer un autre exemple, celui du robot ménager commercialisé par Lidl. Certains utilisateurs y ont découvert un micro. L'enquête diligentée à la suite de cette information n'a toujours pas permis d'expliquer sa présence. Certains ont supposé qu'il s'agissait d'une mise en place en vue d'une future version connectée du robot.

Ces cas concrets nous démontrent que nos adversaires sont nombreux et que nous devons leur porter toute notre attention. Le marché ne saura pas s'autoréguler. Le cas de la Chine m'inspire une anecdote. À l'époque du régime totalitaire polonais, nous demandions quelle était la différence entre une démocratie et une démocratie socialiste. La réponse était de dire que c'était la même différence qu'entre une chaise et une chaise électrique.

Cette situation est dramatique, en réalité. D'ailleurs, la grande absente de nos débats est la Russie. Parfois, la menace principale ne vient pas des pays producteurs de technologie, mais de ceux qui l'utilisent à mauvais escient.

Bernard BENHAMOU

Le cas de ce robot ménager a aussi concerné le marché français puisqu'il était commercialisé dans l'ensemble des États européens.

Leonie BEINING

Il me semble nécessaire de nuancer la question de la transparence. Sans aller jusqu'à connaître le code source, le citoyen devrait être en mesure de savoir qu'une décision a été prise par le biais d'un algorithme. De même, il serait important d'être informé des critères utilisés dans le processus de décision.

V) Les faiblesses de l'Europe en matière d'intelligence artificielle

Bernard BENHAMOU

Nous avons beaucoup évoqué les cas de la Chine et des États-Unis. Revenons à l'Europe pour nous intéresser à ses faiblesses. Nous assistons au départ de nombreux talents qui partent dans des entreprises étrangères. Quels seraient les moyens pour remédier à cette situation regrettable ? Que pouvez-vous commenter de cette situation, André Gattolin ?

André GATTOLIN

L'école mathématique française est effectivement reconnue dans le domaine de l'intelligence artificielle. Tariq Krim avait produit un excellent rapport sur cette question. Les conclusions qu'il tirait restent entièrement d'actualité. Il démontrait comment les meilleurs cerveaux français partaient en Californie. Il y a quelques années, un précédent gouvernement a aggravé cette tendance en plafonnant un système d'aide à 2,5 fois le SMIC, ce qui a limité la capacité à réagir des entreprises françaises face à cette tendance.

Bernard BENHAMOU

Cela nous interroge sur les actions à mener dans le cadre des lois antitrust.

André GATTOLIN

Absolument. Je citerai le cas de l'entreprise Skype qui est en train de mourir du fait que l'entreprise qui l'a rachetée souhaite privilégier son propre système de messagerie interne.

Nous devons aussi formuler d'autres propositions dans le domaine de l'innovation. Avec nos capacités, des domaines entiers restent inexploités. Par exemple, celui de l'agriculture pourrait donner lieu au développement de nombreux systèmes de « smart farming ». Il en est de même dans la gestion des ressources halieutiques. Soyons créatifs, ne restons pas dans une logique de reproduction de ce qui existe déjà.

La question de l'imposition des bénéfices réalisés par les entreprises du numérique est au cœur des débats en cours dans le cadre du G 20. Si les Américains n'y sont pas hostiles, ils exigent malgré tout que cela concerne l'ensemble des entreprises.

Bernard BENHAMOU

Quels seraient les autres outils qui nous permettraient un développement dans ces domaines ? Qu'en pensez-vous, Leonie Beining ?

Leonie BEINING

La question doit être posée sous l'angle de la politique industrielle. Le talent, le matériel et les données constituent les trois ingrédients de l'intelligence artificielle. À ce titre, ils méritent davantage d'investissements. Nous devons donc faire en sorte que l'Europe coopère plus pour que puissent émerger des idées nouvelles.

Je m'oppose à une approche purement pessimiste de la situation qui ne met l'accent que sur le retard de l'Europe. Nous devons développer une vision différente, une troisième voie. De plus, il nous faut être fiers des accomplissements réalisés, à l'instar du RGPD qui est un succès réel.

Nous avançons certes lentement, mais cette lenteur est le prix d'une réelle réflexion. Les questions doivent également être tournées vers l'avenir. Ainsi, une étude démontre le bilan catastrophique de l'intelligence artificielle au niveau de son empreinte écologique. Nous devons accentuer notre attention sur ces questions.

Bernard BENHAMOU

Comment la Pologne envisage-t-elle la capacité de rebond de l'Europe ?

Wojciech ORLIŃSKI

En tant que journaliste, ma parole est totalement libre. Je suis un citoyen polonais et à ce titre, ces débats me surprennent. En effet, lorsque la Pologne a intégré l'Union européenne, nous avions l'impression que les États membres occidentaux détenaient toutes les réponses à toutes les questions. Désormais, en étant nous-mêmes consultés sur ces sujets, notre impression est étrange.

Certes l'Europe a mis du temps à régler certaines questions : sept ans ont été nécessaires à la fois pour faire aboutir le RGPD, mais aussi pour conclure le procès visant Google. Pour autant, ces processus ont abouti. Si aux États-Unis les procédures semblent plus rapides, force est de constater qu'il n'y existe ni RGPD ni condamnation de Google. Par conséquent, la troisième voie portée par l'Europe me semble donc tout à fait efficace.

Les propos tenus par Till Steffen sont très pertinents. Effectivement, nous devons mettre en place un champion européen dans ces domaines, tel qu'Airbus dans le sien.

Qu'est-ce que l'intelligence artificielle concrètement ? Des compétences en matière de calcul et des volumes de données. Les GAFA détiennent les deux. Aucune autre entreprise ne peut y prétendre à ce jour. Les perspectives de développement ne manquent pas et l'Europe doit y tenir tout son rôle.

Bernard BENHAMOU

Nous prenons conscience que la maîtrise environnementale pourrait participer à ce processus.

Anthony COLOMBANI

L'état d'esprit qui ressort de nos débats est positif en ce qu'il démontre une réelle volonté d'avancer. Je tiens à souligner que toute l'intelligence artificielle ne se limite pas aux États-Unis et à la Chine. Beaucoup d'exemples sont situés en Europe.

Bernard BENHAMOU

Pour autant, la partie destinée aux consommateurs est essentiellement basée aux États-Unis.

Anthony COLOMBANI

Certes, mais notre vision du sujet doit être globale. Selon moi, nous devons envisager certains allègements de réglementation et anticiper davantage les impacts de l'intelligence artificielle.

VI) La mise en œuvre d'une politique de valorisation des talents

Bernard BENHAMOU

Nous assistons à un phénomène de déperdition des talents. L'Europe est devenue un terrain de shopping pour le recrutement de nos cerveaux les plus brillants. Parfois, les salaires sont quintuplés, voire décuplés, sans même évoquer le cas des chercheurs au CNRS. Comment pouvons-nous endiguer ce phénomène ? Quelles seraient les pistes qui permettraient d'inverser cette tendance, André Gattolin ?

André GATTOLIN

C'est effectivement préoccupant. Historiquement, notre vision libérale nous a empêchés d'aider nos entreprises. Nous avons alors mis en place divers systèmes horizontaux tels que les crédits d'impôt. Il me semble qu'un système vertical est nécessaire. L'exemple de Google est éloquent : cette entreprise a pu décoller quand l'administration de la Défense l'a intégrée. Par ailleurs, il faut que l'Union européenne mette en place une politique industrielle.

Pour ce faire, il faudrait créer un Conseil européen de l'innovation. Notre modèle actuel doit donc être radicalement modifié pour inverser la tendance.

Questions de la salle

Bernard BENHAMOU

Nous allons désormais répondre aux questions de la salle.

De la salle

J'aimerais en savoir plus sur la notion de « blockchain ».

Ces débats sont très intéressants, et j'ai eu plaisir à les écouter. Toutefois, le développement de l'intelligence artificielle semble laisser de côté les territoires plus difficiles d'accès géographiquement, à l'instar des Antilles.

Wojciech ORLIŃSKI

Ce thème est très complexe, je l'évoque souvent avec des étudiants. Les blockchains peuvent constituer des leviers de développement pour une start-up. Elles sont traitées différemment selon les États. À ce sujet, l'Europe doit se positionner.

S'agissant des DOM-TOM, je comprends votre sentiment d'isolement.

Bernard BENHAMOU

Je tiens à préciser que l'ensemble de nos débats est filmé. À ce titre, nos amis d'outre-mer pourront aisément retrouver la vidéo sur le site web du Sénat.

Anthony COLOMBANI

À titre personnel, je voudrais évoquer le cas de la Corse, très similaire à celui des Antilles. Il faudrait s'inspirer de certains pays qui ont parié sur des choix de formation de très haut niveau sur le numérique, comme l'Italie. Beaucoup d'étudiants italiens sont recrutés par les GAFA à leur sortie de cursus.

De la salle

Je suis avocate dans le domaine des nouvelles technologies. Après vous avoir écouté, je note une envie générale de légiférer sur toutes ces questions. Or notre cabinet traite de projets sur le long terme pour lesquels il serait crucial de connaître les évolutions

réglementaires à venir afin d'accompagner au mieux nos clients. Avez-vous des précisions à apporter quant au calendrier des réformes ?

Konstanty RADZIWIŁŁ

Je ne peux pas m'exprimer sur la situation française. Au niveau communautaire, je pense que l'unique domaine sur lequel nous avons légiféré est celui de la responsabilité du fait des produits. Nous allons effectivement travailler sur d'autres aspects, pour autant il est impossible d'annoncer un calendrier.

Clôture : quelles réponses de l'Union européenne ?

M. Jean BIZET

Sénateur de la Manche, Président de la commission des Affaires européennes du Sénat

Le Président du Sénat, M. Gérard Larcher, n'a malheureusement pas pu assister à cette conférence en raison de ses engagements. Il m'a toutefois chargé de vous transmettre le message suivant.

Mesdames et Messieurs les Présidents,

Mesdames et Messieurs les Parlementaires,

Mesdames et Messieurs,

Je me félicite de l'organisation de cette troisième conférence en format « Triangle de Weimar » et je vous remercie de votre présence au Palais du Luxembourg.

Je remercie en particulier nos invités allemands et polonais, notamment M. Till Steffen, Président de la commission des Lois du Bundesrat, et MM. Łukasz Mikołajczyk et Konstanty Radziwiłł, membres du Sénat de Pologne, ainsi que mes collègues sénateurs pour leur présence et leur participation active.

C'est en 2016 que nous avions lancé, avec le Maréchal du Sénat de Pologne, M. Stanislaw Karczewski et le Président du Bundesrat de l'époque, M. Stanislas Tillich, l'idée d'organiser un cycle de trois conférences parlementaires en format « Triangle de Weimar ».

La première conférence s'est tenue à Varsovie le 4 décembre 2017 et était consacrée à la lutte contre les discours de haine sur internet.

La deuxième conférence a été organisée à Berlin le 22 octobre 2018 et portait sur le thème de la lutte contre les Fake news.

Cette troisième conférence qui se tient à Paris est donc la dernière et elle nous permet de dresser un bilan et de tracer des perspectives.

Nous avons souhaité placer cette troisième édition sous le signe de l'Europe avec l'intitulé suivant : « cybersécurité, protection des données et intelligence artificielle : quels enjeux pour l'Europe ? »

En effet, nous considérons que pour faire face aux défis soulevés par la cybersécurité et l'intelligence artificielle, seule une réponse à l'échelle de l'Europe serait à la hauteur des enjeux.

Et, dans ce cadre, nous avons la conviction que la France, l'Allemagne et la Pologne peuvent jouer un rôle utile d'aiguillon vis-à-vis de nos partenaires européens et des institutions européennes.

Face à la multiplication des cyberattaques, à des fins de criminalités, d'espionnage ou de sabotage, la cybersécurité représente un enjeu majeur de sécurité nationale.

Depuis les rapports Romani et Bockel, le Sénat a joué un rôle précurseur dans ce domaine, en appelant de ses vœux à une prise de conscience des enjeux soulevés par la cybersécurité et à un renforcement des moyens pour lutter contre cette menace.

La commission des Affaires étrangères, de la Défense et des Forces armées du Sénat a notamment veillé, lors de l'examen de la dernière Loi de programmation militaire, à conforter les moyens de l'ANSSI.

Le Sénat est aussi un gardien vigilant de la protection des données, tant au niveau national, qu'au niveau européen, grâce à sa commission des Lois et à sa commission des Affaires européennes.

Avec l'arrivée des objets connectés, la protection des données va devenir sans doute un enjeu essentiel pour la préservation de l'équilibre entre la sécurité et les libertés individuelles.

La multiplication des discours de haine, de l'antisémitisme, du racisme, de la désinformation et de la manipulation sur Internet et les réseaux sociaux, représente aussi un défi pour nos démocraties.

Depuis les affaires Snowden et Cambridge Analytica, nous connaissons les dangers de la manipulation et de la désinformation pour le fonctionnement même de nos démocraties.

Le Sénat a beaucoup travaillé sur la question de l'adaptation de notre droit au numérique, notamment au sein de la commission des Lois et de sa commission de la Culture de l'Éducation et de la Communication, pour parvenir à un meilleur équilibre entre la liberté d'expression sur Internet et la lutte contre la haine.

L'Assemblée nationale et le Sénat seront d'ailleurs amenés à se prononcer prochainement sur une proposition de loi inspirée de la législation allemande qui vise à renforcer l'obligation pour les opérateurs des plateformes de retirer les contenus illicites dans un délai de 24 heures sous peine de lourde sanction financière.

L'intelligence artificielle soulève des enjeux essentiels, démocratiques, juridiques, éthiques et industriels, notamment sur la transparence des algorithmes. Au travers de l'Office parlementaire d'évaluation des choix scientifiques et technologiques, le Sénat a souhaité suivre attentivement ce sujet et contribuer aux réflexions sur l'adaptation de notre cadre législatif.

Qu'il s'agisse de la cybersécurité ou de l'intelligence artificielle, seule une réponse à l'échelle européenne serait à la hauteur des défis, comme le montrent les travaux conduits par la commission des Affaires européennes du Sénat.

Enfin, le Sénat a créé, en avril dernier, à la demande du groupe Les Républicains, une commission d'enquête sur le thème de la souveraineté numérique. Celle-ci a commencé ses auditions et devrait remettre ses conclusions en septembre. Face aux géants américains ou chinois, il s'agit d'éviter que l'Union européenne devienne « une colonie du monde numérique », pour reprendre le titre d'un rapport d'information du Sénat.

Sur tous ces sujets, une approche comparative entre la France, l'Allemagne et la Pologne est particulièrement opportune. Je pense notamment aux enjeux de sécurité soulevés par le déploiement de la 5G, et la nécessité d'une coordination au niveau européen.

Nos trois pays peuvent aussi jouer un rôle utile au sein de l'Union européenne pour apporter des réponses communes à ces défis. Et je suis persuadé que les Parlements nationaux, et les Chambres hautes en particulier, peuvent y contribuer.

À l'occasion de la XXe session de l'Assemblée des Sénats d'Europe, qui s'est tenue à Paris, du 13 au 15 juin, nous avons d'ailleurs signé avec le Président du Bundesrat, M. Daniel Gunther et le Maréchal du Sénat de Pologne, M. Stanislaw Karczewski, une déclaration conjointe. Dans cette déclaration, nous avons notamment convenu :

- *de continuer à échanger des expériences et des bonnes pratiques,*
- *de poursuivre le dialogue entre les parlementaires, les experts, les professionnels et les représentants de la société civile,*
- *d'étudier des mesures législatives visant à sensibiliser la société aux risques cybernétiques en particulier pour les plus jeunes.*

Nous avons donc posé aujourd'hui la troisième pierre, mais l'édifice est loin d'être achevé. Il nous faudra poursuivre notre travail à l'avenir pour faire vivre l'esprit de Weimar. Je vous remercie pour votre attention.

À titre personnel, je vous remercie de votre présence et de votre attention, ainsi que pour la qualité des débats.