ASSEMBLÉE NATIONALE

XIV^e LÉGISLATURE

Compte rendu

Office parlementaire d'évaluation des choix scientifiques et technologiques

Nomination de rapporteurs

Présentation de l'étude de faisabilité de Mme Anne-Yvonne Le Dain, vice-présidente, députée, et M. Bruno Sido, président, sénateur, concernant le risque numérique

Mercredi 16 avril 2014
Séance de

Compte rendu n° 50

SESSION ORDINAIRE DE **2013-2014**

Présidence de M. Bruno Sido, sénateur, *Président*

ASSEMBLÉE NATIONALE

Office parlementaire d'évaluation des choix scientifiques et technologiques

Mercredi 16 avril 2014

Présidence de M. Bruno Sido, Sénateur, Président

La séance est ouverte à 17 h 05

– Nomination de rapporteurs

M. Bruno Sido, sénateur, président.– Il nous revient de procéder à la désignation de deux rapporteurs sur deux saisines.

Tout d'abord, la saisine de la Commission des affaires économiques du Sénat relative aux « *Enjeux stratégiques des terres rares* ». J'ai reçu deux candidatures pour cette saisine : celle de M. Patrick Hetzel, député, et celle de Mme Delphine Bataille, sénateur. Y a-t-il d'autres candidatures ?

M. Patrick Hetzel, député, et Mme Delphine Bataille, sénateur, sont désignés rapporteurs de l'étude relative aux « Enjeux stratégiques des terres rares ».

La seconde saisine provient de la Commission des affaires sociales de l'Assemblée nationale et porte sur « *Le numérique au service de la médecine* ». J'ai reçu deux candidatures pour cette saisine : celle de M. Gérard Bapt, député, et celle de Mme Catherine Procaccia, sénateur. Y a-t-il d'autres candidatures ?

M. Gérard Bapt, député, et Mme Catherine Procaccia, sénateur, sont désignés rapporteurs de l'étude sur « Le numérique au service de la médecine ».

– Présentation de l'étude de faisabilité de Mme Anne-Yvonne Le Dain, vice-présidente, députée, et M. Bruno Sido, président, sénateur, concernant le risque numérique

M. Bruno Sido, sénateur, président.– Madame Anne-Yvonne Le Dain et moi-même avons l'honneur de vous présenter, aujourd'hui, l'étude de faisabilité d'un rapport sur le risque numérique (sécurité des réseaux informatiques, stockage des données personnelles ou industrielles et leur exploitation), à la suite de la saisine de l'Office effectuée par la Commission des affaires économiques du Sénat, le 26 juin 2013.

Comme vous le savez, le règlement intérieur de l'Office précise que les rapporteurs doivent d'abord procéder à une étude de faisabilité pour établir un état des connaissances sur le sujet de leur étude, pour déterminer des axes de recherche permettant d'obtenir des résultats pertinents dans les délais requis et, enfin, pour proposer les moyens nécessaires pour engager un programme d'étude.

C’est donc cette étude que nous vous présentons aujourd’hui, en vous rappelant que l’Office a le choix entre trois options : soit renoncer à poursuivre les travaux, soit suggérer à l’auteur de la saisine une nouvelle formulation, soit engager un programme d’étude en vue d’un rapport.

Mme Anne-Yvonne Le Dain, députée, vice-présidente.– Quant au champ des investigations à mener, vos rapporteurs ont donc suivi ce schéma pour, d’abord, établir un état des connaissances sur le sujet du risque numérique.

À cette fin, ils se sont reportés à l’audition publique qui avait été organisée par l’Office le 21 février 2013 sur « *Le risque numérique : en prendre conscience pour mieux le maîtriser ?* » et ont constaté que, si les grandes lignes avaient bien été tracées, toutes les questions n’avaient pu être abordées, que certaines des questions abordées méritaient d’être approfondies et que, enfin, seulement une année après cette audition, la réalité du numérique avait déjà largement évolué.

Pour illustrer cela, je m’en tiendrai à un exemple : l’utilisation accrue des nuages numériques pour stocker des données et proposer des services. Comme vous le savez, l’expression « nuage numérique » (*cloud* en anglais) renvoie au stockage de données informatiques de particuliers, d’entreprises, d’administrations, à l’extérieur de leur propre réseau informatique. Or, cette utilisation s’accroît à grande vitesse et plus vite que l’état des connaissances sur le sujet, ce qui n’est pas sans risque puisque le numérique est au cœur de notre société.

Vos rapporteurs se sont interrogés sur les axes de recherche à retenir à partir du moment où la Commission des affaires économiques du Sénat a souhaité que l’accent soit mis sur le risque numérique encouru par les entreprises, notamment à travers la sécurité des réseaux numériques utilisés par elles. Même ainsi délimité, ce thème de recherche est encore apparu très vaste à vos rapporteurs puisqu’il concerne le fonctionnement de la société dans son ensemble à travers des aspects techniques nouveaux et complexes.

Après quelques investigations, il est apparu pertinent de se concentrer sur les opérateurs d’importance vitale, terminologie officielle qui renvoie aux acteurs dont l’activité ne saurait être interrompue sans mettre gravement en péril le fonctionnement même du pays. La liste de ces opérateurs d’importance vitale est assez longue. C’est pourquoi vos rapporteurs ont jugé pertinent d’étudier particulièrement deux catégories de ces opérateurs, à savoir ceux du secteur des télécommunications et ceux du secteur de l’énergie. En effet, les télécommunications constituent, à la fois, l’infrastructure essentielle au cœur du numérique et un secteur économique en plein essor. Quant au secteur de l’énergie, il apparaît particulièrement emblématique pour caractériser la nécessité de continuité sans interruption de ses activités, notamment en raison d’une faille numérique compromettant le bon fonctionnement de ses installations. Il suffit de penser aux centrales nucléaires pour en être convaincu.

À ce stade de leur réflexion, vos rapporteurs ont pris la précaution de rencontrer le président de la Commission des affaires économiques du Sénat, M. Daniel Raoul, pour s’enquérir de l’adéquation entre le périmètre d’étude qui vient de vous être décrit et les préoccupations de la commission. Une telle délimitation a recueilli l’accord de M. Daniel Raoul.

M. Bruno Sido.– À propos de l'état des connaissances en matière de sécurité numérique, la première observation de vos rapporteurs à la suite de la quarantaine d'auditions exploratoires menées jusqu'à ce jour revient à constater l'insuffisance, voire les lacunes, de l'enseignement du numérique à tous les stades de la scolarité et dans la formation continue. Comme il leur est apparu que l'amélioration de cet état ne semblait ni facile ni immédiate, ils ont organisé, pas plus tard que ce matin, une audition publique en forme de table ronde sur l'éducation au numérique, avec une quinzaine d'intervenants extérieurs. Ouverte à la presse et aux membres du Conseil scientifique de l'Office, cette table ronde, particulièrement riche, a ouvert de nouvelles perspectives et montré que les investigations des rapporteurs en ce sens pourraient déboucher sur des recommandations constructives.

Au-delà de cette première conclusion d'évidence, les documents existants ont permis à vos rapporteurs de cerner quelques interrogations et d'apprécier à quel point les connaissances en ce domaine évoluaient avec rapidité. Aucun rapport parlementaire ou autre, ouvrage, compte rendu de colloque, publication ou article n'a semblé correspondre au thème même de l'étude proposée à l'Office par la Commission des affaires économiques du Sénat. Des investigations supplémentaires sont donc justifiées.

Dans un tel contexte, la synthèse des connaissances déjà disponibles, qui sera retracée dans une partie du rapport projeté, pourrait déjà combler une lacune. De plus, à en juger par les éléments déjà recueillis à ce jour, les recoupements d'informations résultant de cette synthèse devraient se révéler fructueux. Pour prendre un exemple, le rapport de l'Académie des sciences sur l'éducation au numérique mérite d'être mis en perspective avec les analyses de la Commission nationale de l'informatique et des libertés (CNIL), son guide de « *La sécurité des données personnelles* » ou encore avec le « *Guide d'hygiène informatique* » rédigé par l'Agence nationale de sécurité des systèmes d'information (ANSSI) ou son document intitulé « *Maîtriser les risques de l'infogérance* ».

De plus, des axes de recherche essentiels doivent être explorés. Il en est ainsi, par exemple, des normes internationales applicables dans le domaine du numérique où, à l'heure actuelle, une sorte de course poursuite est engagée entre les techniques, un règlement européen en cours d'élaboration pour compléter l'actuelle directive européenne applicable et la normalisation internationale largement impulsée par les États-Unis d'Amérique et, enfin, l'accord de partenariat transatlantique (APT) négocié depuis juillet 2013. Sur ce point précis, vos rapporteurs envisagent de se rendre à Bruxelles pour connaître l'état d'élaboration du règlement européen.

Mme Anne-Yvonne Le Dain.– En ce qui concerne la perspective de résultats pertinents à atteindre par l'OPECST, comme rappelé dès l'abord, l'étude de faisabilité a aussi pour objet de se demander si des résultats pertinents peuvent être atteints dans les délais requis. À ce stade, vos rapporteurs sont confiants puisqu'ils s'appuient d'abord sur l'audition publique de février 2013, organisée par l'Office, qui prolongeait elle-même le rapport de M. Jean-Marie Bockel, publié en juillet 2012 au nom de la Commission des affaires étrangères, de la défense et des forces armées du Sénat sur la cyberdéfense, et que, d'octobre 2013 à aujourd'hui, vos rapporteurs ont réalisé une quarantaine d'auditions.

Pour la suite, ils vous proposent d'organiser au moins deux autres tables rondes en plus de ce matin : l'une d'une journée sur les opérateurs d'importance vitale et la sécurité des systèmes d'information telle que proposée à ces divers acteurs et une autre sur le cadre juridique de la sécurité des réseaux du numérique, sans exclure des auditions individuelles complémentaires si le besoin s'en faisait sentir. Les auditions devant les rapporteurs seraient

donc combinées avec des auditions plus larges sous forme de tables rondes, ouvertes ou non à la presse suivant les cas, et pouvant être animées par des membres du Conseil scientifique de l'Office.

Pour mener à bien ce programme d'étude, vos rapporteurs ont constaté qu'il ne leur était pas indispensable de recourir à un groupe de travail à leur côté, compte tenu du fait que beaucoup d'aspects ont déjà été éclairés par les auditions rappelées précédemment.

Enfin, vos rapporteurs ont souhaité limiter au strict nécessaire leurs déplacements. À savoir quatre déplacements – dont deux déjà effectués – pour visiter des centres de recherche sur la sécurité du numérique et de ses réseaux : dans un premier temps à Élancourt puis, récemment à Nancy, au Laboratoire de haute sécurité de l'INRIA. Un troisième serait effectué à Rennes pour visiter le centre de recherche sur le numérique de la Direction générale de l'armement (DGA2) du ministère de la défense. Le quatrième, déjà évoqué, aurait pour destination Bruxelles. À la fois en raison du thème de l'étude, du temps imparti et de la nécessité de ne pas alourdir les dépenses de l'Office, vos rapporteurs ont exclu tout déplacement lointain à l'étranger, notamment aux États-Unis d'Amérique. En effet, si le numérique est particulièrement présent dans ce pays, il n'est pas évident d'y recueillir d'autres éléments d'informations que ceux disponibles à Paris grâce à des auditions ou en recourant précisément aux facilités que le numérique offre à la recherche d'informations.

Quoiqu'ayant renoncé à l'assistance d'un groupe de travail auprès d'eux, vos rapporteurs se sont déjà appuyé, et continueront de le faire, sur les membres du Conseil scientifique dont plusieurs ont été entendus. L'un d'eux, M. Daniel Kaufman, a animé les trois débats de la table ronde sur l'éducation au numérique qui a eu lieu ce matin même, au Sénat, Salle Médicis, et qui a donné lieu à un enregistrement vidéo.

Sans entrer dans les détails de ce que pourrait être le rapport à venir, vos rapporteurs attirent votre attention sur les premiers constats établis par eux, à savoir que la sécurité numérique actuelle est loin d'être garantie car de nombreuses failles existent dans les réseaux et les matériels, ainsi que dans la manière de les utiliser. À cet égard, il convient de souligner que les failles du numériques sont inévitables à chaque degré d'évolution de la technique. Elles sont multiples et révélées plus souvent par des erreurs – ou des pirates qui les exploitent – que par des analyses théoriques. Ces failles posent aussi la question de la confiance à accorder aux divers matériels utilisés. Chacun sait que les entreprises sont maintenant toutes largement dépendantes du bon fonctionnement des outils numériques auxquels elles recourent.

M. Bruno Sido.– Pour autant, ni la formation des personnes concernées, ni la fiabilité des matériels, ni la sécurité des réseaux, ni la connaissance des limites de la conjugaison de ces facteurs, ni l'actualisation à un rythme adapté des connaissances sur la vulnérabilité des réseaux ne sont au rendez-vous. Cela était déjà le cas il y a un an, et l'est encore davantage aujourd'hui avec le stockage des données et de services numériques dans les nuages.

À cet égard, vos rapporteurs soulignent qu'en matière de stockage de données numériques, quatre éléments sont essentiels pour leur sécurité : la confidentialité, l'intégrité, la disponibilité et la réversibilité. La confidentialité et la disponibilité sont des attentes évidentes des clients des nuages ; l'intégrité suppose le respect des données confiées et la réversibilité exige que le propriétaire des données puisse les récupérer au terme du contrat passé avec le fournisseur du stockage.

Ce simple rappel suffit à montrer que le cadre juridique du numérique doit être adapté au fur et à mesure des évolutions du cadre technique, ce qui conduit vos rapporteurs à insister sur l'importance d'une nouvelle détermination dudit cadre juridique approprié au secteur du numérique pour qu'il devienne possible d'attendre de réelles retombées économiques. À ce jour cela n'a rien d'une évidence. D'où, encore une fois, la nécessité de mener une réflexion pour s'engager dans cette voie.

En France, tant la CNIL que l'ANSSI aident à définir les limites du cadre juridique et technique, mais les recommandations de l'une comme de l'autre montrent qu'il est nécessaire de conjuguer les aspects techniques, juridiques, économiques et sociologiques pour obtenir le meilleur à la fois des matériels, des logiciels, des réseaux, des données et des services. À condition d'avoir nourri la réflexion des personnes au contact du numérique.

C'est pourquoi, à ce stade de leurs investigations, vos rapporteurs estiment que la synthèse des études existantes, des recoupements originaux et de nouveaux questionnements pourraient aboutir à d'utiles recommandations de l'OPECST pour promouvoir l'éducation au numérique tout au long de la vie, l'existence d'une souveraineté du numérique accrue et des moyens de parvenir à une sécurité numérique.

Ils vous proposent, en conséquence, de bien vouloir adopter la présente étude de faisabilité après avoir répondu aux questions que vous pourrez leur poser.

Mme Corinne Bouchoux, sénatrice.– Mes chers collègues, le thème de votre étude est une très bonne idée ; c'est un vrai sujet. Je voulais juste porter à votre connaissance quatre éléments. Le premier, c'est qu'une mission commune d'information sénatoriale sur l'accès aux documents administratifs et aux données publiques, dont je suis le rapporteur, va bientôt achever ses travaux. Elle nous a permis d'entendre un certain nombre de personnes dont on pourra vous communiquer la liste ; son rapport devrait paraître au début du mois de juin 2014.

Ensuite, une suggestion consistant à contacter les directeurs du master sur le numérique à Sciences-po – où j'étais d'ailleurs hier soir. Ce qui est intéressant à observer, c'est le choc des cultures et des générations, car vous avez dans la salle des étudiants pour qui nous sommes tous des dinosaures : ces étudiants font tous quatre choses en même temps ! Ils sont déjà des professionnels de l'expertise du risque numérique *in situ*. C'est intéressant car ce phénomène est peu perçu.

Troisièmement, l'an dernier, j'ai suivi la session nationale « Armement et économie de défense » de l'Institut des hautes études de défense nationale (IHEDN) et, sur les dix travaux de comité réalisés, au moins deux portaient sur votre sujet, dont un sur le nuage numérique et un autre sur les recherches menées par les industriels sur le numérique ; ce qui est en plein dans votre champ d'investigation avec vos recherches sur les industriels. C'est décidemment un très beau sujet que vous avez à traiter.

Enfin, même si, dans le cadre de la mission d'information, nous avons renoncé à aller à Londres, faute de temps, en revanche, s'est tenu, à Londres, un rassemblement de tous les lanceurs d'alerte : ils étaient vingt-sept du monde entier et ils sont en train de constituer une fondation. Le risque *versus* l'attaque, c'est ce qui nous intéresse. Ces lanceurs d'alerte seraient très intéressés de pouvoir témoigner devant des institutions. Pour le moment, aucune institution ne les a vus ; ce serait très fructueux pour l'Office.

Quatrièmement, j'attire l'attention des parlementaires sur le fait que l'IHEDN ne parvient pas à recruter de manière à refléter la diversité des familles politiques. L'an dernier, Mme Leïla Aïchi et moi-même avons suivi les sessions ; cette année, c'est une autre sénatrice écologique, Mme Kallioppi Ango Ela. Il faudrait vraiment, pour l'année prochaine, qu'il y ait davantage de biodiversité politique : trois écologistes en deux ans, ce n'est pas représentatif de la diversité du Parlement. Il est vrai que la charge de travail de ces sessions est très lourde car il s'agit de deux jours par semaine, plus des voyages.

Mme Catherine Procaccia, sénateur.– Le sujet d'étude de l'OPECST est passionnant. J'ai le sentiment que vous avez déjà beaucoup travaillé à travers toutes les auditions que vous avez menées. En matière de numérique, tout foisonne, comme je l'ai constaté à l'occasion de ma participation à la mission d'information que mène Mme Corinne Bouchoux. Je ne pensais pas qu'elle pousserait aussi loin ses investigations par rapport au numérique et à l'accès aux données. Par ailleurs, aujourd'hui, se tenait une conférence de presse à laquelle je n'ai pu assister qui portait sur le numérique et l'accès aux données personnelles.

De nombreux parlementaires se préoccupent du numérique. Il serait bon que vous arriviez à élaborer une synthèse de tous ces travaux, outre les vôtres, de telle sorte qu'on donne l'impression que le Parlement abonde dans le même sens et non pas que chacun se contente d'approches parcellaires. Si vous arriviez, à travers tous ces dossiers – sans compter les investigations que vous menez parallèlement –, à pouvoir élaborer une synthèse, ce serait très intéressant.

Vous avez évoqué aussi l'action de M. Jean-Marie Bockel qui a créé un groupe informel sur la sécurité numérique auquel je participe de temps à autre. Il y a presque trop d'initiatives, notamment depuis l'affaire Snowden. Mais, ce qu'a dit Mme Corinne Bouchoux à propos des dinosaures que nous serions me vexe un peu car j'avais le sentiment que les parlementaires étaient tout de même assez à la page sur ce thème. Beau sujet donc.

Concernant vos futures préconisations éventuelles relatives à l'éducation, force est de constater que l'éducation nationale est le monde le plus fermé aux évolutions. J'espère que vous ne parlerez pas dans le désert avec des recommandations la concernant.

M. Bruno Sido.– Je voudrais rendre à César ce qui lui appartient : M. Jean-Marie Bockel a réalisé un remarquable rapport. Notre synthèse devrait aller au-delà et déboucher ensuite sur des conclusions. En tout cas, il y a des problèmes à résoudre et un certain nombre de rappels à inscrire dans la loi, tout en sachant que c'est un secteur qui évolue terriblement vite. D'ailleurs, j'espère vous montrer tout à l'heure, à l'occasion d'une démonstration sur la vulnérabilité des outils numériques, ce qu'il en est ; c'est assez effrayant.

En complément, j'ai appris ce matin quelque chose d'encore bien plus effrayant : quand on suit une formation grâce à un cours ouvert et massif en ligne donnant lieu à une interrogation sous forme de questionnaire à choix multiple (QCM), il est possible de tracer le profil intellectuel détaillé de l'étudiant : celui-ci qui répond, celui qui hésite, celui qui se trompe… Ces divers profils d'étudiants sont ensuite vendus à des chasseurs de têtes. Or, ce profil peut marquer à vie un étudiant. Les enjeux sont donc tout à fait considérables.

Il reste à savoir s'il peut exister des parades à tous ces défis. J'en arrive à penser, mais peut-être à tort, que, si on n'arrive pas à trouver de parades au pillage informatique des données, notamment celles des entreprises où des milliards d'euros sont perdus – par

exemple, si vous passez la frontière chinoise avec un ordinateur et vous faites dérober tout ce qui est dans le disque dur – cela pourrait comporter, en germe, l'autodestruction de l'informatique puisqu'il deviendrait impossible de posséder des éléments confidentiels.

Dans un tel contexte, le rapport que l'on vous présentera risque probablement de devenir assez rapidement obsolète, mais évoquer les défis actuels et tenter d'y répondre apparaît tout de même utile.

Mme Anne-Yvonne Le Dain.– La notion de risque a déjà été évoquée l'an dernier lors de l'audition publique organisée par l'OPECST. Mais, depuis, est survenue l'affaire Snowden. Pour les données personnelles, il est certain qu'il s'agit de gros enjeux à considérer également comme des opportunités. De toute façon, les Américains vont continuer à agir comme par le passé.

Aujourd'hui, dans le cadre des négociations sur la protection des données personnelles, la Commission européenne se fait épauler par quinze experts américains, ce qui laisse songeur... Notre continent semble enclin à une certaine forme d'angélisme. Nous sommes les premiers clients des Américains ; ce sont des alliés mais, dans une alliance, les intérêts doivent être bien compris et cela consiste d'abord à se protéger. Il faut construire une force européenne et ne pas considérer que ce qui a été imaginé ailleurs ait vocation à devenir la norme partout.

La grande question qui se pose aujourd'hui est qu'un certain nombre de normes n'est absolument pas décidé par les États. Elles s'imposent à eux par l'usage que le monde professionnel accepte. Il en est ainsi des normes ISO. L'existence de ces normes sécurise, mais elles ne sont imposées par aucun système public ; c'est de l'auto-saisine puissante et efficace qui encadre l'accès aux données sur Internet, par exemple, à Facebook, à Twitter, *etc*. De même pour les noms de domaine, avec l'ICANN (*Internet Corporation for Assigned Names and Numbers*), pour lesquels, à partir d'une auto-saisine puis, au fil de l'eau, sur vingt ou trente années, il a été décidé que ce serait des « .org », *etc*. Cette association, basée aux États-Unis d'Amérique, envisage maintenant de déplacer son siège en Suisse. Mais cette nouvelle implantation helvétique va lui donner encore plus de légitimité apparente et un visage international.

L'évolution du monde va très, très vite. L'usage crée le droit et le droit peut parfois autoriser la suppression de certaines garanties. Pour autant, personne n'arrêtera d'utiliser des iPhones ! Le rapport évoquera aussi l'agilité sur Internet, l'éducation sur Internet, le droit qui s'y applique, européen ou international. Toutes ces choses importantes seront examinées mais le rapport ne pourra évidemment pas tout traiter.

M. Jean-Pierre Leleux, sénateur. – À propos de l'éducation au numérique, je dois préciser que l'éducation nationale n'est pas la seule concernée car les collectivités territoriales et le monde associatif sont également parties prenantes. Quant à la protection des données personnelles, c'est un vrai sujet, face à la sécurité des États. Envisagez-vous d'apporter une vision sur l'équilibre souhaitable, dans un État démocratique, entre la protection des données personnelles et les exigences des services de sécurité qui sont amenés à avoir des comportements intrusifs pour prévenir un certain nombre d'évènements graves et surveiller ce qui se passe sur l'ensemble des réseaux ?

Mme Anne-Yvonne Le Dain.– Nous ne pensons pas vraiment aborder cela ; nous pourrons le faire en partie, si nécessaire. Nous savons bien que chacun peut être surveillé ; certains le sont plus que d'autres. En France, le système police-justice fonctionne plutôt bien.

M. Bruno Sido.– Le problème est tellement vaste qu'il concerne aussi, outre les entreprises, les administrations – dont les services fiscaux –, la diplomatie et les aspects militaires. Nous nous bornerons à imaginer les effets qu'aurait déjà une intrusion informatique sur certains systèmes ou réseaux sensibles. C'est pourquoi, nous avons proposé au président de la Commission des affaires économiques du Sénat qui nous a saisi, M. Daniel Raoul, de nous limiter, au-delà de l'examen des problèmes généraux du risque numérique, à deux domaines d'investigations pour étudier la sécurité des réseaux numériques, à savoir celui des télécommunications en général – personne n'a oublié la panne d'Orange – et l'énergie parce que, par exemple, le réseau de transport de l'électricité exige un fonctionnement sans faille. Ni le domaine militaire ni celui du ministère de l'intérieur ne seront abordés.

Par ailleurs, nous ne nous rendrons ni aux États-Unis d'Amérique ni en Chine ni en Russie, où on ne nous montrerait que ce qu'on l'on aurait décidé de nous montrer. Même les opérateurs français considérés comme d'importance vitale ne nous diront pas tout.

Mme Corinne Bouchoux. – Cela semble une bonne idée de centrer le rapport de l'Office sur l'énergie et les télécommunications, car cela a le mérite de la clarté et de l'efficacité ; en effet, actuellement, au Sénat, deux missions sont en cours à la Commission des lois : l'une avec MM. Gaëtan Gorce et François Pillet sur la protection de la vie privée et des données personnelles et une autre, toujours avec M. Gaëtan Gorce, sur la gouvernance d'Internet, où la vie privée sera également prise en compte.

M. Jean-Yves Le Déaut, député, premier vice-président. –Je tiens également à vous féliciter pour votre étude de faisabilité sur un sujet qui est extrêmement complexe et comporte de multiples ramifications. Certes, il est impossible de tout traiter, mais les deux domaines choisis à titre d'illustrations ne suffiront peut-être pas pour aborder tous les cas de dysfonctionnements aujourd'hui constatés.

Je voudrais citer deux exemples : j'ai travaillé la semaine dernière sur ce thème au Conseil de l'Europe, où un bon rapport d'un de nos collègues allemands, député, vient de paraître sur la sécurité dans le cyberespace. Je vous encourage à entendre ce collègue, sur un sujet qu'il est possible de creuser encore davantage.

Ce que vous dites sur la normalisation est une bonne idée. Il faudrait également travailler sur la nécessité de créer une agence de labellisation internationale, en ayant comme objectif de savoir ce qu'un utilisateur doit maîtriser pour décider de recourir aux nuages numériques ; il s'agit de maîtriser et décider de la localisation de ses données, ce qui n'est pas le but d'un certain nombre de professionnels.

Même si c'est traité ailleurs, il faut aborder le fait que la gouvernance mondiale d'Internet est très insuffisante et parler de deux organismes, l'ICANN et l'IETF (*Internet Engineering Task Force*) – et il y en a d'autres. Il faut évoquer la mise en place d'une charte éthique internationale que les États, les associations de consommateurs et les consommateurs eux-mêmes s'engageraient à respecter.

Troisième point : les techniques sont au cœur de votre rapport. Aujourd'hui, il importe de rappeler qu'on est surveillé par des indicateurs de connexion, ou *cookies*, qui se trouvent dans la totalité des messages des ordinateurs que nous utilisons. Actuellement, ces indicateurs de connexion ont une durée de vie illimitée et, en général, on ne sait pas qu'ils existent. Or, il serait envisageable de limiter la durée de ces *cookie*s grâce à un texte international ; tous les experts le disent.

Un autre point de nature technique : ce que vous avez dit sur l'éducation est très juste mais il est important de pouvoir recourir à des personnes capables de maîtriser les éléments suspects. La question est de savoir qui doit les former : les États, les opérateurs d'accès à Internet ? Comment cette formation peut-elle se faire ?

Dernier point technique : l'identification certaine des interlocuteurs sur Internet. Aujourd'hui, les signatures électroniques existent, mais ce sont des systèmes compliqués. Or, il faudrait des systèmes simples pour l'utilisateur, afin de progresser sur Internet sans y être complètement pisté. Par exemple, comme beaucoup d'entre vous le savent, je suis président de l'Abbaye des Prémontrés à Pont-à-Mousson ; ce centre d'art et de rencontres culturelles, équipé d'environ soixante-dix chambres, est référencé sur les sites Booking et Wikipédia où j'étais allé vérifier ce qui était indiqué en tapant seulement « *Abbaye des Prémontrés* ». Cela m'a valu, par la suite, d'être sans cesse invité à aller dormir tout près de chez moi, le premier de ces sites ayant vu en moi un client potentiel.

Quand il s'agit d'autres types de données, cela prête moins à sourire ; il faudrait trouver des solutions techniques pour éviter de tels effets.

Enfin, je vous ferais une suggestion : au sein du Conseil scientifique de l'OPECST, plusieurs membres pourraient vous aider dans votre étude, s'ils ne l'ont déjà fait, au sein, ou non, d'un groupe de travail.

J'ai moi-même eu recours récemment à certains d'entre eux pour élaborer des amendements à Strasbourg. MM. Laurent Gouzenne, Daniel Kaufman ou, par ailleurs, M. Claude Kirchner de l'INRIA, vous permettraient d'être à la pointe des innovations techniques comme, par exemple, prendre, grâce au numérique, le contrôle d'un navire ainsi que me l'a montré une équipe de la DGA. Les trois ou quatre personnes retenues par vous vous aideraient dans la phase finale d'élaboration du rapport.

M. Bruno Sido.– Merci pour vos conseils, Monsieur le Premier vice-président.

En matière de risque numérique, on en découvre tous les jours et, ce qu'on découvre, c'est l'incertitude la plus absolue. Vous avez évoqué des complicités entre divers moteurs de recherche, mais qui pensera que Microsoft n'a pas de relations avec le gouvernement américain et la NSA (*National Security Agency*) ? Celui qui croirait cela se tromperait probablement. Pire encore, Intel devient la seule entreprise à fabriquer des puces informatiques. Qui peut penser qu'Intel n'est pas subventionné par le gouvernement américain et la NSA ? Personne. C'est ce que j'ai souligné lors d'une visite à l'Institut national de la recherche en informatique et en automatique (INRIA) en demandant à des chercheurs s'ils étaient certains de ne pas être espionnés dans leur recherche. Ils n'en savent rien et sont très prudents.

Encore ce matin, il nous a été expliqué qu'il était possible de prendre connaissance de tous les courriels, à moins de les crypter. Mme Anne-Yvonne Le Dain et moi-même croyons beaucoup au cryptage. Ce que j'ai retiré de la visite au laboratoire de haute sécurité de l'INRIA, c'est que certains chiffrages nécessitent un décryptage dont seuls certains ordinateurs très puissants sont capables au terme de deux cents à cinq cents années.

Enfin, j'attire votre attention sur le fait que, après le vote sur la présente étude de faisabilité, une démonstration nous sera proposée sur les vulnérabilités liées au numérique.

M. Jean-Yves Le Déaut.– Les rapporteurs ont entendu toutes les remarques exprimées. Nous allons passer maintenant au vote de l'étude de faisabilité.

L'étude de faisabilité est adoptée à l'unanimité.

Je signale à Mme Catherine Procaccia, qui est arrivée après le début de la présente séance, qu'elle a été nommée comme co-rapporteur pour l'étude sur « *Le numérique au service de la médecine* ». Il a été souhaité que vous vous entouriez d'un comité de pilotage et que vous présentiez les noms des personnes pressenties au président et au premier vice-président.

Mme Catherine Procaccia. – Je me réserve d'attendre la tenue de l'audition publique prévue prochainement pour, au vu de son contenu, imaginer comment pourrait fonctionner le tandem des rapporteurs sur ce sujet.

M. Bruno Sido.– Monsieur le Président, Mme Anne-Yvonne Le Dain et moi-même avons sollicité la Direction de la protection de la sécurité de la défense (DPSD) du ministère de la défense pour une démonstration de la vulnérabilité des outils numériques, qui va débuter dans quelques instants. J'ai donc le plaisir de convier à nouveau les parlementaires ici présents à y assister.

La séance est levée à 18 heures

Membres présents ou excusés

Office parlementaire d'évaluation des choix scientifiques et technologiques

Réunion du mercredi 16 avril 2014 à 17 heures

Députés

Présents. - Mme Anne-Yvonne Le Dain, M. Jean-Yves Le Déaut, M. Philippe Nauche
Excusés. - Mme Anne Grommerch, M. Alain Marty

Sénateurs

Présents. - Mme Delphine Bataille, Mme Corinne Bouchoux, M. Jean-Pierre Leleux, Mme Catherine Procaccia, M. Bruno Sido
Excusés. - Mme Chantal Jouanno, Mme Virginie Klès, M. Jean-Claude Lenoir