ASSEMBLÉE NATIONALE

XIVe LÉGISLATURE

Compte rendu

Office parlementaire d'évaluation des choix scientifiques et technologiques

Mercredi 28 janvier 2015
Séance de 16 h 30

Compte rendu n° 61

SESSION ORDINAIRE DE **2014-2015**

Présidence de M. Jean-Yves Le Déaut, député, *Président*

ASSEMBLÉE NATIONALE

Office parlementaire d'évaluation des choix scientifiques et technologiques

Mercredi 28 janvier 2015

Présidence de M. Jean-Yves Le Déaut, député, président

La séance est ouverte à 16 h 40

– **Informations relatives à l'OPECST**

M. Jean-Yves Le Déaut, président de l'OPECST. – Notre collègue députée **Anne Grommerch** a décidé de démissionner de l'OPECST. Nous le regrettons, mais nous souhaitons que le groupe UMP de l'Assemblée désigne rapidement un remplaçant qui puisse venir nous apporter son concours.

Notre collègue Dominique Orliac, députée, nous a indiqué qu'elle ne se sentait pas en mesure d'assurer son poste de suppléante au **Comité économique, éthique et social du HCB**. Dans ces conditions, je propose son remplacement par M. Gérard Bapt, qui avait fait acte de candidature chronologiquement après elle.

Nos auditions du lundi 24 novembre sur **le survol des installations nucléaires par des drones** méritent d'être éditées, je pense, en retenant comme conclusion la synthèse que j'avais présentée le mercredi 26 novembre devant vous, ainsi que le débat nourri qui s'en était suivi. Je soumets donc à votre accord le dépôt d'un rapport reprenant tous ces travaux.

Les candidats, parmi les membres de l'OPECST, ne se bousculent pas pour le **prochain partenariat avec l'Académie des sciences.** Deux jumelages se sont mis en place à l'initiative de scientifiques qui ont pris l'attache de leur député (Mme Martine Martinel et M. Jean-Luc Bleunven). Je propose donc d'élargir la recherche de volontaires et d'adresser des courriers aux présidents des commissions pour qu'ils nous proposent des candidats.

– **Présentation des conclusions de M. Jean-Louis Touraine, député, et Mme Corinne Bouchoux, sénatrice, relatives à l'audition publique du 22 mai 2014 sur « *Les adjuvants vaccinaux : une question controversée* » ;**

M. Jean-Yves Le Déaut, président de l'OPECST. – Nous en venons aux conclusions relatives à l'audition publique du 22 mai 2014 sur les adjuvants vaccinaux et en particulier sur la question controversée des sels d'aluminium.

Cette audition publique a été organisée suite à une saisine de la commission des affaires sociales du Sénat. Les conclusions seront soumises à la discussion et à l'approbation de l'Office.

Mme Corinne Bouchoux, sénatrice, co-rapporteure. – L'Office parlementaire a organisé le 22 mai 2014, une audition publique sur les adjuvants vaccinaux et en particulier sur le débat controversé autour des sels d'aluminium incorporés aux vaccins. Bien qu'ils permettent d'accroître considérablement l'efficacité des vaccins, les sels d'aluminium comporteraient des effets néfastes sur la santé.

Jean-Louis Touraine et moi-même avons co-présidé avec rigueur cette audition publique. Au vu de l'emballement médiatique précédent et des divergences profondes entre les intervenants, le bon déroulement du débat n'était pourtant pas *a priori* acquis. De plus, la présence d'intervenants se présentant comme victimes de pathologies a ajouté une dimension humaine au débat, qui ne pouvait alors être traité exclusivement d'un point de vue scientifique.

En dépit des craintes initiales, le débat s'est relevé être apaisé, contradictoire et transparent. L'un des orateurs M. Christopher Exley, professeur de biochimie à l'Université de Keele au Royaume-Uni, a d'ailleurs félicité l'Office pour l'organisation d'un tel débat, ce qu'il estime impossible dans son pays.

L'audition publique avait fait suite à la saisine de Mme Annie David qui présidait alors la commission des affaires sociales du Sénat. De nombreuses associations l'avaient sollicitée auparavant, afin qu'une étude soit réalisée, notamment sur la polémique autour d'une pathologie assez récemment découverte : la myofasciite à macrophages. Bien que cette pathologie fasse l'objet d'études depuis plus d'une vingtaine d'années et qu'elle semble maintenant reconnue, la communauté scientifique n'est toujours pas parvenue à un consensus sur l'existence ou non d'une causalité entre cette pathologie et les sels d'aluminium.

M. Jean-Louis Touraine, député, co-rapporteur. – Étant donné l'éloignement des positions initiales, nous avons été agréablement surpris par le climat dans lequel se sont déroulées les deux tables rondes. Les uns faisaient état d'effets adverses des vaccins considérables et sous-estimés. Les autres rappelaient leurs bienfaits indiscutables, et estimaient excessives les réserves émises par les opposants. Les tables rondes sont parvenues à faire dialoguer ces parties. Le débat s'est maintenu dans le domaine rationnel du rapport entre l'efficacité et les effets adverses.

L'ensemble des intervenants a consenti à ce qu'il n'y ait pas de remise en question du bienfait évident en santé publique et individuelle des vaccinations largement répandues. De même, ils ont accepté la possibilité d'effets adverses à ne pas négliger, en étant conscients de la nécessité de mieux les identifier afin d'en approfondir l'étude.

La première table ronde portait sur les effets des adjuvants vaccinaux, en interrogeant la communauté scientifique, puis un panel d'acteurs plus élargi. Rapprocher le dialogue entre les adversaires et les défenseurs de cet adjuvant a été fructueux.

Le point de vue des adversaires de l'utilisation de l'aluminium dans les adjuvants a notamment été développé par le Professeur Romain Gherardi de l'hôpital Henri Mondor à Créteil. Il fait état dans les biopsies de la présence d'aluminium au niveau du site de l'injection quatorze ans après l'administration d'un vaccin. Contenu à l'intérieur des macrophages, l'aluminium peut migrer au niveau cérébral. Les conséquences de cette présence d'aluminium peuvent être le développement d'une pathologie baptisée la myofasciite à macrophages. La définition des caractères cliniques de cette maladie est confuse, puisque les symptômes sont relativement courants : douleurs musculo-articulaires,

troubles cognitifs, asthénies. Une symptomatologie qui peut être provoquée par de nombreuses autres pathologies. Pour autant, ces symptômes pourraient être en relation avec cette administration d'hydroxyde d'aluminium comme adjuvant.

Les défenseurs ont quant à eux indiqué que la plupart des vaccins étaient inopérants sans adjuvants. Déjà un élève de l'Institut Pasteur, M. Ramon avait démontré l'inefficacité du vaccin contre la diphtérie avec l'anatoxine diphtérique seule, le simple ajout d'hydroxyde d'aluminium le rendant performant. Il en avait été de même pour le vaccin antitétanique. Si bien que l'hydroxyde d'aluminium était considéré à l'époque comme indispensable à l'efficacité des vaccins.

Il est curieux de constater que de nombreuses décennies plus tard, un tel postulat persiste. En définitive, peu d'études recherchent d'autres possibilités d'adjuvants ayant une efficacité comparable. D'autres adjuvants sont utilisés chez l'animal, mais ne peuvent être administrés chez l'homme. Des propositions ont été faites sur la recherche de nouveaux adjuvants, mais elles n'ont pas été suffisamment poursuivies, si bien que l'hydroxyde d'aluminium demeure aujourd'hui l'adjuvant utilisé le plus couramment.

Face à cette multiplicité des points de vue, il importe de ne pas accepter *a priori* la totalité des arguments des parties. Il ne s'agit ni de jeter le discrédit sur les vaccins du fait des adjuvants, ni de laisser dire des choses fausses sur les pathologies provoquées par l'aluminium, mais bien d'encourager les recherches dans ces deux domaines.

En effet, un échange pendant le débat a mentionné les démences et autres encéphalopathies avec troubles neurologiques provoquées par de grandes quantités d'aluminium dans le cerveau humain. Il est vrai que l'on peut en déceler des quantités considérables dans le cerveau de personnes dialysées avec de l'eau riche en aluminium, provoquant d'importants troubles neurologiques. Néanmoins, les doses administrées comme adjuvants sont infiniment inférieures. La quantité susceptible de migrer du point d'injection d'un vaccin au niveau cérébral est encore beaucoup plus faible. De sorte qu'on ne peut comparer les conséquences provoquées par les sels d'aluminium comme adjuvants vaccinaux avec des pathologies provoquées par des facteurs à doses considérablement supérieures.

Il n'empêche que des pathologies mineures telles que ces troubles associés à la myofasciite à macrophages méritent d'être étudiées et singularisées, afin qu'elles puissent sortir de la confusion actuelle.

À l'instar des maladies auto-immunes, il importe de mener des études épidémiologiques rigoureuses, pour pouvoir affirmer ou non une causalité liée à l'administration de vaccins. En effet, de nombreux vaccins sont, dans la pratique, administrés aux âges d'apparition fréquente de ces maladies. Par exemple, l'utilisation du vaccin contre le papillomavirus, administré aux jeunes filles adolescentes pour les protéger des risques du cancer de l'utérus, a été accusé de provoquer des maladies auto-immunes telles que des scléroses en plaques. Or, les études épidémiologiques démontrent une incidence équivalente d'apparition de ces maladies auto-immunes dans les groupes vaccinés et non vaccinés.

En administrant les vaccins à des âges inférieurs où la propension à apparaître de ces maladies est plus faible, les doutes légitimes relatifs aux effets néfastes des vaccins pourraient s'en trouver atténués.

Mme Corinne Bouchoux. – La deuxième table ronde, que j'ai présidée, concernait les pistes à envisager pour l'avenir, qu'il s'agisse de la pertinence d'un moratoire ou de la recherche d'alternatives aux adjuvants. Le débat s'est déroulé également dans la sérénité.

Afin d'assurer le bon déroulement du débat, nous avions demandé aux intervenants qui le désiraient d'indiquer s'ils étaient eux-mêmes vaccinés, et s'ils avaient fait vacciner leurs enfants, l'objectif étant de souligner qu'il ne s'agissait pas d'une posture anti-vaccin. La totalité des intervenants ont accepté.

La question relative à la pertinence ou non d'instaurer un moratoire a provoqué un désaccord. Les partisans et les opposants à la mise en place d'un moratoire se sont exprimés, en présentant les rapports bénéfices-risques. Bien qu'elle n'ait pas été tranchée, cette question a pu être évoquée de façon modérée.

Je considère que l'intérêt de cette table ronde a été de réussir à créer un dialogue constructif, et ce de façon sereine.

Par la suite s'est posée la question des vaccins sans adjuvants. Comme l'a rappelé Jean-Louis Touraine, l'efficacité des vaccins devenant alors moindre, la balance risques-bénéfices penche alors dans le sens du risque, ce dernier pouvant être maintenu sans les avantages apportés par les adjuvants.

Le dernier point sensible abordé a été celui des alternatives à l'aluminium. Faut-il trouver une solution alternative à l'aluminium ? Et dans ce cas, quelles seraient les solutions envisageables ?

Le débat a alors porté sur le phosphate de calcium comme adjuvant éventuel. Ce dernier ne comporte cependant pas des avantages équivalents à l'aluminium, tout en générant également des risques. Le point de vue du laboratoire Sanofi nous a été longuement explicité par l'un de ses représentants. Dans la mesure où les résultats relatifs au phosphate de calcium sont contradictoires, Sanofi a décidé de ne pas poursuivre les recherches. Sanofi n'a cependant pas apporté de réponse à la question sur la pertinence de relancer ou non le phosphate de calcium, pour offrir un choix aux patients. En effet, les associations de victimes réclament le droit de pouvoir choisir ou non l'administration de l'aluminium. Ce débat n'a pour autant pas été prolongé.

Enfin les aspects économiques ont été évoqués. Le président de l'association Entraide aux malades de myofasciite à macrophages (E3M) a abordé la question de l'achat des vaccins de l'Institut Pasteur par Mérieux, afin de voir si la rentabilité financière n'avait pas fondé le choix d'un vaccin plutôt qu'un autre. Ce débat s'est néanmoins clos rapidement, du fait des positions diamétralement opposées, entre celle du représentant de Sanofi et celle de l'association E3M.

Un autre argument de nature économique a été à nouveau soulevé par le professeur Yehuda Schoenfeld de l'Université de Tel-Aviv, reprochant aux laboratoires de ne pas investir suffisamment dans la recherche de nouveaux adjuvants.

Malgré ces nombreuses divergences -exprimées de façon mesurée- les intervenants sont toutefois parvenus à un certain nombre de points de consensus.

Il en est de la nécessité d'intensifier la recherche. Malgré la crainte irraisonnable des citoyens, il faut répondre à leurs méfiances en augmentant les recherches sur les effets de l'aluminium, afin de prévenir une baisse éventuelle de la vaccination. Il est important de prévenir tout regain d'une sorte de désobéissance civile qui a eu lieu pendant la campagne de vaccination contre la grippe H1N1. La deuxième demande de recherche porte sur la myofasciite à macrophages, et l'amélioration du diagnostic de cette maladie, impliquant une modification dans l'enseignement de la médecine.

D'autre part, les échanges ont fait ressortir la demande de financer la recherche de manière que l'expertise soit la plus indépendante possible, c'est-à-dire financée par des fonds publics. Ensuite, les intervenants se sont accordés pour proposer que les recherches soient pour approfondies dans un cadre pluridisciplinaire.

Le dernier point d'accord propose d'améliorer l'efficacité du système d'alerte concernant les pathologies liées à la maladie myofasciite à macrophages, dans la mesure où aucun remède n'existe actuellement. Néanmoins cela pose le problème de la suite à donner à cette alerte. La mise en place d'un système de déclarations sur le site de l'Agence nationale de sécurité du médicament et des produits de santé (ANSM) nécessiterait d'instaurer un accompagnement des victimes.

C'est tout à l'honneur du Parlement et de l'Office d'avoir réussi à réaliser ce débat dans de telles conditions. Je vous renvoie aux comptes rendus des interventions qui rendent compte des différents points de vue exprimés. Le problème n'est pas forcément résolu, mais l'audition a répondu à une réelle attente d'écoute et d'intéressement à ces problématiques que l'on a pendant longtemps écartées car elles dérangeaient. L'Office a su adopter une posture différente, en proposant un débat contradictoire et démocratique, là où des logiques concurrentes ont pu s'affronter : celle des victimes qui recherchent une causalité à leurs maux, celle des laboratoires, et celle de la santé publique qui est de vacciner la population. A l'aune du siècle, les vaccins ont tout de même sauvé beaucoup plus de vies que provoqué des aléas. Toutefois mes chers collègues, ce discours fondé sur un raisonnement en probabilités statistiques n'est pas satisfaisant pour les victimes.

M. Jean-Louis Touraine. – J'approuve entièrement la présentation de Corinne Bouchoux. Le fait que l'on ait pu tenir cette audition dans la sérénité démontre que l'Office arrive à entendre des parties qui, au départ, n'ont pas forcément pour habitude de dialoguer, et dont les positions sont initialement fortement arrêtées. Des personnes qui nous avaient presque dissuadés de tenir cette audition ont reconnu qu'elle avait permis l'établissement d'un dialogue. La conclusion a été bien résumée par Corinne Bouchoux.

Les laboratoires mènent une recherche pour établir des vaccins contre les maladies conséquentes. Néanmoins cette recherche comporte des manques : les maladies peu solvables ne font pas l'objet d'un tel investissement. L'aide de la puissance publique est donc essentielle.

En ce qui concerne les adjuvants, je considère que la recherche ne sera pas faite de façon majeure dans les laboratoires. Actuellement, l'utilisation de l'aluminium est efficace et leur garantit des résultats positifs. Les adversaires sont un groupe en définitive minoritaire, dont la voix ne porte pas au-delà de leur cercle, n'empêchant pas la commercialisation des vaccins. La prise de risque serait alors trop importante d'investir dans la recherche d'autres adjuvants, dont on ne connait pas encore les inconvénients. Les laboratoires ne vont pas

substituer un risque connu et minime à un risque inconnu. Il importe donc que la puissance publique prenne en charge cette recherche.

De même, la puissance publique doit encourager les études dans les sciences humaines, à propos de l'acceptabilité sociale de la vaccination, mise à mal lors de nombreux épisodes : H1N1, hépatite B, papillomavirus. Le discours sur la santé publique, postulant que 80% de la population soit vaccinée pour qu'une maladie ne se propage pas, ne fonctionne plus aujourd'hui. L'acceptabilité parait plutôt reposer sur la balance avantages-risques au niveau individuel. Ces questions doivent être analysées par des organismes publics de recherche, pour maintenir l'adhésion au projet vaccinal.

M. Gilbert Barbier, sénateur. – Il est regrettable que dans notre pays des études épidémiologiques ne soient pas réalisées. La référence à des publications étrangères, de fait obligatoire dans ce domaine, est alors contestable par la force des choses.

Un autre problème relatif à la myofasciite à macrophages qui est actuellement très confus concerne l'imputabilité devant les tribunaux. Il est difficile de savoir comment cette affaire va être tranchée au niveau juridique ; c'est un problème de société qu'il faudra évoquer.

Enfin, le fait que la recherche dans ce domaine repose essentiellement sur les laboratoires et les entreprises, provoque immédiatement des suspicions d'intérêts économiques lorsque l'on fait référence à leurs travaux. Il importe que la recherche publique s'engage davantage, afin de crédibiliser ou de contredire les travaux des laboratoires.

M. Jean-Yves Le Déaut. – Je voudrais d'abord féliciter les deux rapporteurs. Si l'Office l'accorde, nous publierons le compte-rendu de l'audition suivi de ses conclusions développées ici, qui sera transmis à Alain Milon, président de la commission des affaires sociales du Sénat. Il nous indiquera alors s'il y a lieu de donner suite à cette étude.

Corinne Bouchoux et Jean-Louis Touraine ont fait état d'un certain nombre de points de consensus : intensifier la recherche sur des sujets comme les sels d'aluminium, développer la recherche publique, améliorer le système d'alerte ou au moins le mettre en place.

Il me parait nécessaire d'insister sur ce que Jean-Louis Touraine a souligné précédemment, à savoir qu'on ne peut démontrer l'absence d'effets d'un adjuvant ou d'un vaccin, sans rapporter cet effet aux bénéfices escomptés de cette vaccination. Je viens de recevoir une lettre d'une association qui demande la liberté de choix dans la vaccination. L'acceptation de la liberté de choix dans la vaccination diminue l'efficacité de la vaccination. Une partie de la population n'étant plus vaccinée, les risques de contamination s'accroissent.

Dans ces domaines de la santé, la notion de bénéfices-risques est, à mon avis, une notion plus importante que la seule notion de la précaution.

M. Jean-Louis Touraine. – Il ne peut y avoir en ce domaine la moindre liberté. Elle amènerait à pénaliser des enfants du fait d'idées particulières des parents. Le taux de vaccination de la rougeole, une maladie qui peut être mortelle, est aujourd'hui inférieur au seuil de protection de la population. Il est dangereux de laisser encourager cette propension à refuser la vaccination.

M. Jean-Yves Le Déaut. – Je constate que l'Office parlementaire adopte ces conclusions. A la demande de Catherine Procaccia, sénatrice, nous pouvons proposer à Alain Milon que les conclusions soient présentées par Jean-Louis Touraine et Corinne Bouchoux devant la commission des affaires sociales du Sénat et de l'Assemblée nationale.

M. Daniel Raoul, sénateur. – Tout rapport devrait être présenté devant la commission du Sénat ou de l'Assemblée nationale qui est à l'origine de la saisine.

– Examen du rapport d'information de Mme Anne-Yvonne Le Dain, députée, et M. Bruno Sido, sénateur, premier vice-président de l'OPECST, sur le risque numérique ;

M. Jean-Yves Le Déaut, député, président de l'OPECST. – Nous avons déjà eu une discussion sur ce sujet le 17 décembre dernier et nos collègues rapporteurs ont souhaité disposer d'un peu plus de temps pour arriver à une version qui intègre la réorganisation des recommandations et qu'ils ont aussi pu améliorer. Ce projet a été mis en consultation, comme c'est la règle, quarante-huit heures avant la réunion de ce jour.

Cette version n'a pas tout intégré. J'ai moi-même retravaillé encore ces deux derniers jours sur quelques améliorations de forme, mais on dispose maintenant d'un document qui contient des recommandations très importantes. Il me semble nécessaire que, conformément aux options prises dans le cadre de l'étude de faisabilité, vous proposiez de modifier l'intitulé puisque vous avez opportunément choisi de cibler votre étude.

Je voudrais tout de suite vous féliciter, en englobant dans ces félicitations le conseil technique que vous avez reçu. Car ce document, avec ses recommandations, pose bien le problème. .

Une brève vidéo sur la sécurité numérique, très récemment élaborée par le Cigref à destination des entreprises, est alors projetée dont le message consiste à attirer l'attention sur le fait que : « *100 % des entreprises protègent leurs données ; logiquement très peu d'entre elles ont dû connaître une faille de sécurité lors des douze derniers mois… de fait, oups ! 73 % ! Comme quoi, on n'est jamais trop prudent. Chaque seconde, notre environnement déborde d'activités, des gens comme vous et moi qui, chaque jour, génèrent des millions de données sensibles en envoient et en reçoivent, les partagent aux quatre coins du monde. Mais qui veille sur tout ça ? Qui peut agir pour éliminer les risques ? Et si c'était vous ?* ».

M. Bruno Sido, sénateur, premier vice-président de l'OPECST, rapporteur. – Mme Anne-Yvonne Le Dain et moi-même avons aujourd'hui le plaisir de vous présenter le projet de rapport sur le risque numérique dont vous nous avez confié l'élaboration et dont la vidéo qui vient d'être projetée illustre en quelques minutes la problématique en ce qui concerne les entreprises.

C'est à partir d'une **saisine de la commission des Affaires économiques du Sénat** que nous avons entrepris **une étude de faisabilité** adoptée par l'Office le 16 avril 2014.

Cette saisine faisait elle-même suite à une **journée d'auditions publiques** organisée conjointement par l'OPECST et la commission des Affaires étrangères et de la Défense du Sénat au mois de février 2013. Ce jour-là, l'audition publique avait été scindée en deux parties, l'une relative au risque numérique militaire et l'autre au risque numérique civil.

Au début de nos investigations, nous comptions donc réaliser notre rapport en approfondissant la seule question du risque numérique civil. Mais il nous est rapidement apparu que, en matière de risque numérique, **la distinction entre le civil et le militaire était artificielle**, compte tenu justement de la nature du numérique qui est présent partout.

Au terme d'**une centaine d'auditions** comprenant trois journées d'auditions publiques et des déplacements à Bruxelles et en province, notamment pour visiter le centre de haute sécurité de la Direction générale pour l'armement et le laboratoire de haute sécurité de l'INRIA, vos rapporteurs ont établi **une douzaine de constats** sur la situation de la sécurité numérique et procédé à **trois choix** pour mener à bien leur étude.

Au début de celle-ci, nous avons pris soin de rencontrer le président de la commission des Affaires économiques du Sénat, M. Daniel Raoul, aujourd'hui de retour à l'OPECST ce dont nous nous réjouissons.

Nous lui avons indiqué que nous centrerions notre réflexion sur **les opérateurs d'importance vitale (OIV)**, c'est-à-dire les entreprises dont le fonctionnement ne doit en aucun cas être interrompu, notamment du fait d'une défaillance de leur système d'information numérique.

Ces entreprises sont d'ailleurs soumises à des **directives nationales de sécurité (DNS)** qui leur imposent des obligations extrêmement précises que la loi de programmation militaire de 2013 a renforcées.

Après quelques mois de nos travaux, l'angle d'attaque pour aborder l'étude à partir des opérateurs d'importance vitale s'est révélé avoir été intéressant pour le raisonnement mais nous a conduit bientôt à replacer l'ensemble des activités desdits opérateurs dans **la chaîne de sécurité numérique** qu'ils constituent avec leurs fournisseurs, leurs sous-traitants, leurs clients et leurs personnels.

En outre, pour être tout à fait complet, au moment où le Gouvernement annonçait un ambitieux projet de loi sur le numérique, il n'a cependant pas attendu le dépôt de celui-ci pour prendre, comme déjà indiqué, dans la loi de programmation militaire, en 2013, des initiatives relatives justement aux opérateurs d'importance vitale et, d'autre part, pour élaborer, au cours de l'été 2014, des mesures relatives à la sécurité numérique concernant les administrations.

Ce qui montre que le Gouvernement, comme nous-mêmes, avons été conduits à effectuer en parallèle des analyses rigoureuses sur les différents secteurs pour finalement constater que tout se recoupe et que la sécurité numérique, voire la sécurité tout court, ne peuvent être assurées qu'à partir de mesures reliées entre elles.

Par quelque bout que l'on considère la question, il est impossible de ne pas voir dans les ramifications du numérique **le système nerveux de la société et même des individus** qui la composent d'où l'impossibilité de scinder artificiellement les préoccupations de sécurité en divers segments d'études.

C'est bien ce qu'ont vu, les premiers, les attaquants des systèmes numériques. À l'heure où notre pays se trouve placé sous les dispositions du plan Vigipirate à son plus haut degré – soit l'alerte attentat –, le thème d'étude de l'OPECST ne peut qu'être au cœur des préoccupations de tous les parlementaires.

Pour relever ce défi, depuis quelques années, des dispositifs ingénieux ont été imaginés et des moyens réels en hommes et en moyens ont été accordés. Par exemple, en 2009, l'Agence nationale de sécurité des systèmes d'informations (ANSSI) a été créée.

Mais, dès l'abord, je dois préciser que des dispositifs étaient déjà en place antérieurement et que, maintenant, ce n'est pas en accordant toujours davantage de compétences à l'ANSSI ni en portant, par exemple, ses effectifs de 300 à 1 000 ou à 3 000 – seuils qui ne sont d'ailleurs nullement envisagés –, qu'on résoudrait toutes les questions posées par les failles de la sécurité numérique, ni qu'on parerait à toutes les attaques dont cette sécurité est l'objet.

En effet, cette question transversale suppose l'acquisition par l'ensemble de la société d'une **culture du numérique** et d'une **éducation initiale et continue** à la hauteur des services rendus par cette technique, à la fois en dépit et en raison des fragilités qu'elle recèle.

Depuis le début de mon propos, et surtout à la suite du visionnage de la vidéo que vous venez de regarder, vous vous demandez peut-être si vos rapporteurs n'ont pas cédé à quelque alarmisme. Je vous rassurerai en disant que nous avons d'abord souhaité démontrer dans une analyse, que l'on a voulu extrêmement fouillée, le mécanisme de transmission d'un message au sein du système d'information de l'entreprise et les fragilités, souvent de conception, des matériels, des réseaux, des services et des diverses applications numériques.

Mais avant cela, nous devons lever une ambiguïté. En dépit de l'actualité sur les aspects les plus médiatisés du risque numérique et ses liens avec le terrorisme, **le présent projet de rapport n'a rien d'une fresque générale ou journalistique sur le numérique** où, par exemple, seraient développées des considérations sur la gouvernance mondiale de l'Internet, car il s'agit d'un rapport technique. L'OPECST produit de tels rapports directement liés aux préoccupations des entreprises que, malheureusement, le Sénat a parfois tendance à négliger. C'est pourquoi je rappelle que la commission des affaires économiques, à l'origine de la saisine, s'inquiétait de l'éventuelle fragilité des entreprises liée aux vulnérabilités des réseaux matériels, logiciels, numériques. Cela est particulièrement technique.

En qualité de membre de cette commission, j'insiste sur l'importance de cette dimension du sujet.

La question sous-jacente posée à l'Office était notamment celle du pillage organisé des informations des entreprises. Il serait déraisonnable de continuer à ignorer le fait que l'on puisse puiser dans ces informations comme dans un libre-service. **La situation de l'économie française s'accommode-t-elle de tels pillages ou bien résulte-t-elle en partie de ceux-ci, alors justement qu'ils durent depuis des années ?**

À un moment donné, il nous est apparu que **les imperfections constatées peuvent constituer également des chances** et c'est cet aspect que Mme Anne-Yvonne Le Dain va maintenant développer pour vous montrer que l'analyse de vos rapporteurs comporte aussi une facette réactive, voire optimiste.

Mme Anne-Yvonne Le Dain, députée, rapporteur. – Je ne crois pas que l'indispensable prise de conscience qu'a évoquée Bruno Sido relève d'une approche pessimiste du numérique, mais l'idée que la sécurité numérique puisse devenir un atout de développement économique me tient à cœur, et c'est là un axe majeur de notre analyse. Il s'agit de faire d'une crainte une opportunité.

Au fur et à mesure des auditions, une idée nous a de plus en plus préoccupés : comment tirer parti d'une situation mal engagée, en l'occurrence, en matière d'insécurité numérique, pour **faire de l'économie avec du droit** ? Un développement dans le rapport illustre ce que cette idée sous-tend.

Il se trouve que **la France possède de nombreux atouts** en ce domaine car, sans même parler des fabricants d'antivirus, les connaissances de l'École française de mathématiques alliées à une grande tradition en matière de cryptologie, de cryptographie et de linguistique, les ressources des centres de recherche de la Direction générale de l'armement ou de l'INRIA, pour ne citer qu'eux, devraient permettre de conforter les entreprises œuvrant en matière de sécurité numérique et, surtout, permettre de nouvelles initiatives qui ne seraient pas récupérées aussitôt par nos concurrents principaux, à savoir les États-Unis d'Amérique – qui écrivent l'informatique à l'aide du même alphabet que nous, contrairement aux Russes, aux Indiens ou aux Chinois.

Pour mettre en valeur les atouts français, il faut se débarrasser de préjugés et d'attitudes routinières. Par exemple, les préjugés associés à l'image des *hackers* alors que certains d'entre eux pourraient être employés fort utilement pour élaborer des solutions de prévention et de riposte aux attaques numériques éventuelles – un certain nombre d'entreprises le fait déjà. Les personnes entendues ont cité des exemples de *hackers* peu diplômés que l'administration française n'avait pu recruter à un niveau de salaire décent. En effet, leur diplôme ne donnait accès qu'à un niveau indiciaire de traitement dans la fonction publique peu propre à rémunérer équitablement les hautes compétences dont ils faisaient preuve.

Une autre personne entendue nous a cité les exemples de jeunes entreprises extrêmement innovantes dans le numérique aussitôt rachetées par des financiers d'outre-Atlantique venus faire, en quelque sorte, leur marché en France.

Face à une telle situation, il ne suffit pas de demander aux autres de faire preuve d'initiative, de créativité, de réactivité, si nous-mêmes, parlementaires, ne montrons pas l'exemple d'abord par notre engagement personnel, puis à travers les décisions des assemblées et collectivités territoriales au sein desquelles nous pouvons avoir une influence. Certaines de nos propositions de recommandations vont dans ce sens.

Libre au Gouvernement d'agir de même face aux administrations.

Venons-en maintenant à l'observation de nos comportements face aux exigences de la sécurité numérique souvent négligées dans la vie courante.

Par exemple, qui d'entre nous hésite avant de s'abonner à une messagerie électronique alors que celle-ci est peut-être contrôlée par une firme étrangère ? Qui prend le temps minimal de réflexion avant de choisir la voie la plus sécurisée pour transmettre un message urgent ? Les services des assemblées sont-ils eux-mêmes à la pointe quant à la sécurité informatique ? Les collectivités territoriales ne pourraient-elles s'intéresser davantage à cette question ? Qu'en est-il enfin des entreprises que l'on suppose à la pointe en matière de technologie de sécurité numérique ? Et, quand on parle de sécurité numérique, les ordinateurs ne sont pas les seuls objets à prendre en considération, les téléphones portables sont également sources de risques, ainsi que tous les « objets dits connectés ».

Tout naturellement, à ce stade de l'analyse, chacun pense au rôle de l'éducation nationale. Or, vos rapporteurs proposent, dans la vingtaine de recommandations prioritaires qu'ils vous soumettent, d'**enseigner le codage** de manière ludique dès l'école maternelle et de **créer une véritable filière d'enseignement de l'informatique incluant systématiquement des modules significatifs sur sa sécurité** jusque dans l'enseignement supérieur. Et, ce, sur tout le territoire national.

Cela peut paraître évident mais la situation actuelle n'est pas à la hauteur des exigences, loin s'en faut.

Qu'observe-t-on aujourd'hui ? L'absence de l'informatique dans les programmes ou, quand elle y figure, c'est avec un nombre d'heures extrêmement restreint et malheureusement sans enseignement sur la sécurité du numérique, ou si peu, y compris dans les écoles spécialisées.

En outre, quels sont **les enseignants** censés faire face à cette nouvelle demande ? D'où proviennent-ils aujourd'hui ? D'où proviendront les effectifs accrus nécessaires demain ? Il serait bien imprudent de croire qu'on peut facilement reconvertir un professeur de mathématiques, de sciences physiques ou de technologie en professeur d'informatique. Chacun sait que l'informatique n'est pas vraiment une branche des mathématiques ni une section de l'électronique.

Quand je parle de filière de l'enseignement de l'éducation au numérique, il s'agit aussi de **diplômes** reconnus et d'un **corps d'inspection**. Et où placer cet enseignement dans l'emploi du temps des élèves ?

Mais, me direz-vous, cette construction n'aurait-elle pas bientôt pour effet de figer les connaissances des enseignants alors que ce secteur évolue si vite ?

C'est un risque réel qui doit être d'emblée pris en compte pour anticiper la sclérose éventuelle desdits enseignants dont la réactivité devra demeurer la qualité première.

Mais, sans entrer davantage dans cette partie de nos propositions, je crois que le Premier vice-président souhaiterait vous en détailler un peu davantage la philosophie.

M. Bruno Sido. – Pour bien situer notre propos par rapport aux contextes international, européen et national actuels, je souhaiterais insister sur la totale symbiose existant entre le numérique et la société.

En général, chacun admet ce phénomène fusionnel mais sans accepter d'en tirer vraiment les conséquences. Ainsi, il ne sert à rien d'élever des digues juridiques ou technologiques si, dans le même temps, des accords internationaux ou la réalité d'un rapport de force non encadré viennent ruiner nos efforts.

Autant une partie de notre projet de rapport entre dans le détail des systèmes informatiques, autant il nous a paru indispensable de faire précéder cette analyse par **une vision d'ensemble**.

Tel fut le cas pour expliquer pourquoi la négociation actuelle du Traité de partenariat transatlantique et le rythme d'avancée de l'élaboration de la directive et du projet de règlement européens, ainsi que la maturation du projet de loi sur le numérique en France sont en réalité étroitement liés.

Vous avez pu trouver, dans les deux premiers chapitres du rapport, les raisons pour lesquelles il est très important, à la fois, que **les droits et libertés soient respectés** dans l'univers numérique, tout en veillant à **protéger la souveraineté numérique de la France comme de l'Union européenne**.

Il s'agit là d'objectifs vitaux qui doivent primer sur la libre circulation des marchandises, l'abaissement des droits de douane ou l'instauration d'une concurrence libre et parfaite.

Vos rapporteurs se sont d'ailleurs demandé s'il ne serait pas primordial de concevoir une exception numérique d'après le modèle de l'exception culturelle et pour les mêmes raisons.

En effet, l'exception culturelle a permis de conserver une industrie cinématographique française dynamique alors qu'elle aurait pu être laminée par des principes commerciaux qui prétendaient la dominer. Les cinémas d'autres pays d'Europe en ont été victimes.

De même, dans le numérique, **toutes les chances doivent être mises de notre côté pour que des industries françaises et européennes puissent concevoir, fabriquer, voire seulement contrôler pour les labelliser, les matériels, logiciels, systèmes d'exploitation, cœurs de réseaux qui forment la longue chaîne de la sécurité numérique**.

Cette idée n'a pu être qu'esquissée dans ce rapport mais elle mériterait d'être développée dans d'autres enceintes et, prioritairement, se concrétiser avant qu'il ne soit définitivement trop tard.

Je voudrais aussi attirer votre attention sur les schémas qui sont projetés depuis le début de notre présentation – et qui figurent tous dans le rapport. Beaucoup de ces schémas ont d'ailleurs été **élaborés par l'OPECST**, ce qui n'est pas si fréquent. Ils nous ont semblé utiles pour expliciter **une réalité numérique multiple difficile à appréhender** autrement.

C'est ainsi que, devant la difficulté d'expliquer une réalité technologique plus que complexe, le schéma de l'éléphant vous permet soudain de voir que, par exemple, la perception du numérique n'est que parcellaire, ce qu'a d'ailleurs illustré aussi la **multitude de rapports parlementaires** traitant de ce thème. Beaucoup de ces études n'ont porté que sur un aspect bien particulier du numérique. Et **très peu ont approfondi la question de la sécurité du recours croissant au numérique par les entreprises**.

C'est ainsi qu'un rapport parlementaire analyse l'ouverture des données ou « *open data* », un autre le traitement des données massives ou « *big data* », le troisième la gouvernance mondiale de l'Internet, un autre enfin le modèle proposé par les États-Unis d'Amérique, et ainsi de suite.

Le présent rapport n'a pas pour ambition de constituer une anthologie du numérique mais de montrer que, même si cela ne saute pas aux yeux, toutes ces questions sont interdépendantes.

La sécurité numérique est présente derrière chacune d'entre elles et permet, peut-être, de reconstituer le puzzle des Internet et de tous les aspects du numérique en général, pour en faire ce que vous voyez sur l'écran sous la forme imagée de cet éléphant.

Mme Anne-Yvonne Le Dain. – En ma qualité de scientifique, je souhaiterais vous montrer quelques schémas qui rendent compte de la réelle complexité de ce numérique que nous croyons pouvoir appréhender avec ce que avons sous les yeux. Ce schéma-ci représente le réseau global de l'Internet en Île-de France et vous pouvez noter le nœud dense de ramifications se trouvant sous La Défense. Un spécialiste nous a indiqué que, à cet endroit, une frontière numérique séparait l'Inde de l'Europe du point de vue de la gestion des réseaux numériques, ce qui ne tombe pas sous le sens. La dématérialisation a des conséquences absolument sidérantes.

Cet autre schéma représente les ramifications numériques d'une entreprise avec son centre de gestion, ses activités de production, ses contacts avec l'extérieur, avec ses sous-traitants et leurs propres sous-traitants et, se superposant à tout cela, les multiples connexions, par nature très imprévisibles, réalisées à l'initiative de ses employés.

Il est évident que des liens entre tous ces éléments, de leur continuité, de leur intégrité, dépendent, dans un premier temps, la sécurité numérique, et, bien sûr, ensuite, la protection contre de mauvaises surprises. À cet égard, une des recommandations de vos rapporteurs consiste à **couper totalement les *SCADA* – c'est à dire les systèmes numériques commandant la production – de l'Internet**. Cette préconisation peut, à première vue, sembler très exagérée pour beaucoup d'organisations croyant fonctionner parfaitement.

Cependant, pour vous convaincre en un instant de l'utilité de cette recommandation, j'évoquerai simplement l'anecdote rapportée par une personne entendue, à savoir la pénétration du système des *SCADA* d'un hôpital nord-américain par un adolescent de seize ans qui avait réussi à bloquer la climatisation de cet établissement, et exigeait une rançon pour la rétablir. Cela va au-delà de la simple constatation de l'habileté avérée d'un adolescent face à l'inconscience de l'administration d'un hôpital. La prise en considération du facteur humain est primordiale pour opposer une défense idoine.

Par ailleurs, quand on sait que des **logiciels d'attaques informatiques** sont maintenant disponibles dans le commerce, donc éventuellement à la disposition d'individus particulièrement malfaisants, le rapprochement de ce fait avec le fait précédent peut conduire à réfléchir.

D'autant que, même si notre rapport a souhaité disséquer, pour ainsi dire, la complexité de la sécurité numérique d'une entreprise, un des constats auxquels vos rapporteurs sont parvenus, mentionné dans le préambule du rapport, est le suivant : **au-delà des failles technologiques, les failles humaines entraînent des vulnérabilités plus grandes**.

D'où l'effort d'éducation que nous avons déjà évoqué et, plus généralement, une action de sensibilisation massive à mener dont la petite projection du début de notre réunion a montré la nécessité.

En effet, ce **film réalisé par le CIGREF** à la demande d'une **quarantaine d'entreprises internationales** est **destiné à être diffusé**, accompagné d'un test ludique, **à destination de tous les employés** desdites sociétés avec, évidemment, l'espoir que cette sensibilisation gagne **leurs familles et d'autres entreprises**, ainsi que les administrations, voire les politiques eux-mêmes.

Trop souvent, les dirigeants des entreprises ne prennent pas assez au sérieux les exigences de la sécurité numérique. Ainsi, l'usage systématique d'un téléphone portable sécurisé est difficile à accepter.

Pour illustrer cette prégnance tous azimuts du risque numérique, nous avons inséré en annexe du tome premier du rapport, un petit questionnaire, imaginé par le même CIGREF, recensant certaines situations quotidiennes liées au numérique et proposant plusieurs réactions possibles.

Il a été remis à chacun d'entre vous les quelques pages de ce jeu-questionnaire et, tout en écoutant avec attention notre présentation à deux voix, vous avez peut-être déjà tenté de déterminer ce qu'aurait été votre attitude numériquement responsable dans tel ou tel cas.

Quand on parcourt l'ensemble de ce questionnaire, chacun ne peut que s'étonner des erreurs de réflexe ou des hésitations à opter pour la bonne option qui auraient constitué autant des failles de sécurité dans la vie quotidienne.

Cela illustre qu'il ne faudrait plus **jamais concevoir quelque avancée du numérique que ce soit sans qu'une analyse approfondie ait pu proposer, dans le même temps, des instruments de sécurité**. Cet enjeu pourrait, d'ailleurs, constituer une opportunité pour notre économie.

Cela suppose de faire preuve de davantage de cohérence dans la prise au sérieux du concept même de sécurité numérique. Et cela commence au stade de la conception des **organigrammes des entreprises,** où l'« empêcheur de tourner en rond » que représente souvent le responsable de la sécurité n'est pas situé au bon niveau pour que ses conseils puissent être entendus et acceptés à temps par les dirigeants.

Ces affirmations ne sont pas excessives car des exemples quotidiens montrent que **les entreprises n'ont pas encore tiré les conséquences des impératifs que devraient leur dicter la sécurisation numérique de leurs activités**.

Dans de nombreuses entreprises, les employés utilisent indifféremment leurs matériels numériques personnels ou professionnels, d'autant que les usages sont de plus en plus nomades. Les accès Internet sont multiples, les personnes séjournant temporairement dans l'entreprise pas assez contrôlées, l'usage des clés USB s'est banalisé et les comportements inconséquents vis-à-vis de l'utilisation des objets connectés sont aussi variés qu'innombrables.

Et des exemples récents montrent que des pirates ou attaquants ont bien compris que **les failles du numérique peuvent être d'autant mieux exploités qu'elles sont élargies par les défaillances humaines**.

C'est ce que les spécialistes du numérique appellent l'ingénierie sociale associée aux attaques techniques. Tel a été encore le cas, à la fin de l'année 2014, à propos de l'attaque connue sous le nom d'« arnaque au président » où, après une étude poussée des habitudes numériques et des caractéristiques de chacun des protagonistes, un appel téléphonique du supposé président d'une société est adressé, le vendredi soir, à un comptable de cette entreprise pour lui demander d'adresser d'urgence, de la part du président, une somme importante qui permettra d'assurer *in extremis*, au cours de la fin de semaine, la conclusion d'une négociation déjà bien avancée.

Ce procédé peut vous paraître enfantin voire grossier, mais, à la fin de l'année 2014, **l'entreprise Michelin** s'est fait piégée à hauteur de **1,6 million d'euros** avec cette arnaque.

De nombreux présidents, dirigeants d'opérateurs d'importance vitale ont été sollicités de la même manière et tous n'ont pas eu la chance d'avoir des personnels assez sensibilisés au risque numérique pour ne pas tomber dans de tels traquenards.

Parfois, même si l'attaque n'est pas identifiée immédiatement, il est encore possible d'interrompre les rebonds successifs de pays en pays de l'argent ainsi naïvement remis, mais à condition d'opérer extrêmement rapidement.

M. Bruno Sido. – Je voudrais, avant de terminer notre présentation, et avant d'en venir à vos questions, évoquer les objets connectés dont chacun s'amuse et s'émerveille et qui ont constitué des cadeaux de Noël recherchés : il faut savoir que ces objets sont conçus d'abord pour séduire, **sans que la question de leur sécurité soit incluse** dès l'origine.

Or, d'après certaines personnes auditionnées, le nombre de ces objets par individu pourrait dépasser la cinquantaine dans quelques années et la plupart de ces objets communiqueront entre eux sans intervention ni contrôle humains.

D'où la recommandation de vos rapporteurs de **prévoir des protocoles de conception d'objets connectés incluant obligatoirement à tout coup des préconisations de sécurité** et, à tout le moins, une information sur l'absence de sécurité.

Pour résumer l'esprit des propositions de recommandations essentielles faites par vos rapporteurs en faveur d'une amélioration de la sécurité numérique des entreprises, nous vous les présentons en distinguant les trois temps d'une attaque : avant, pendant et après.

Avant une attaque numérique, il serait infiniment souhaitable pour les entreprises de :

- classer les données et **simuler des pertes d'archives** ;

- chiffrer les données sensibles ;

- chiffrer les réseaux *Wi-Fi* ;

- construire une **sécurité numérique dans la profondeur** ;

- établir un **plan global de sécurité** prévoyant l'homogénéité de celle-ci ;

- installer des **sondes sur le réseau,** dont des **sondes de détection d'attaque** ;

- n'acheter que des **matériels** et ne recourir qu'à des **fournisseurs référencés par l'ANSSI** ;

- déconnecter les *SCADA* de l'Internet ;

- sécuriser les passerelles d'interconnexion avec l'Internet ;

- éviter l'usage d'infrastructures sans fil (*Wi-Fi*) ;

- effectuer des **tests d'intrusion** et des **exercices réguliers de crises informatiques**, des **audits de sécurité** des règles informatiques ;

- former à la sécurité informatique ;

- mettre en place un **centre de sécurité opérationnel** ;

- assurer le risque numérique.

Mme Anne-Yvonne Le Dain. – **Pendant une attaque numérique**, il est urgent :

- d'activer les **cellules de crise** et les **équipes d'intervention** ;

- d'informer sans délai l'ANSSI et la CNIL ;

- de communiquer avec d'autres opérateurs d'importance vitale (OIV) ;

- d'avoir à disposition le nom du développeur du site de l'entreprise, ses clés d'accès, ses mots de passe et la manière d'obtenir les journaux informatiques ;

- de réagir à un virus en moins de vingt-quatre heures ;

- d'analyser l'attaque informatique subie.

M. Bruno Sido. – **Après une attaque numérique**, si une prévention avait été mise en place et utilisée lors de l'attaque, il faudrait **:**

- mettre en œuvre les enseignements des exercices de **restauration des archives** ;

- changer les mots de passe.

Si certaines de ces précautions sont négligées, , malheureusement pour les entreprises concernées, il ne resterait plus à celles-ci qu'à adopter d'urgence toutes les préconisations de vos rapporteurs.

Dans leurs préconisations, vos rapporteurs ont souhaité distinguer deux grandes catégories. D'abord **une vingtaine de recommandations générales**, classées en cinq sous-ensembles, puis, pour ceux qui souhaitent aller plus loin, **une centaine de recommandations placées sous un intitulé « *Vade-mecum pour la sécurité numérique des entreprises* »** où sont détaillées environ la moitié des prescriptions que la centaine d'auditions a inspirée à vos rapporteurs.

Il est donc possible d'avoir deux niveaux de lecture des recommandations du rapport, l'une, traditionnelle, avec les vingt premières recommandations et l'autre, plus technique, et qui se veut opérationnelle, avec le *vade-mecum* destiné aux entreprises.

Faut-il rappeler que toutes les recommandations pouvant émaner de l'OPECST ne se traduisent pas obligatoirement ou uniquement dans un texte législatif mais peuvent prendre des formes plus directes à destination soit du Gouvernement, soit encore des entreprises, soit, enfin, des individus eux-mêmes puisque, vous le verrez à la lecture de ce rapport, chacun d'entre nous peut en tirer des leçons pour son comportement quotidien personnel.

Pour terminer, vos rapporteurs ont constaté qu'il existait peut-être, à ce stade de leurs travaux, comme cela est souvent le cas, une insuffisante adéquation entre l'objet du rapport et son intitulé initial. D'où la proposition de **modifier cet intitulé** pour mieux marquer que, au-delà des risques du numérique, il s'agit de **favoriser les conditions de la confiance** à mettre en lui et de mieux indiquer que ce rapport est très largement **tourné vers les entreprises**.

Le nouvel intitulé pourrait être, par exemple, « *La sécurité numérique des entreprises* » ou « *Les conditions de la confiance pour une sécurité numérique des entreprises* » ou bien d'autres encore que nous évoquerons ensemble lors de la discussion.

Nous vous remercions de votre attention et vous proposons de répondre maintenant à vos questions.

M. Jean-Yves Le Déaut. – Je voudrais tout d'abord vous remercier pour le travail qui a été accompli. La parole est à M. Daniel Raoul.

M. Daniel Raoul. – Je dois vous dire que j'ai eu un peu de difficulté à suivre compte tenu de la vitesse du débit avec lequel les orateurs ont exposé les conclusions de leurs travaux. Je relirai donc cela à tête reposée.

Avez-vous fait une distinction, quant au risque numérique, entre les voies hertziennes et les réseaux fibres ? Cela me paraît relativement important car l'on voit se développer la Wi-Fi avec tout ce qu'on appelle la domotique, mais c'est également vrai dans une entreprise ; or, r n'importe qui, avec un scanner de fréquences, peut attaquer ce système qui est d'une grande fragilité et ne procure aucune sécurité.

Je me souviens avoir préconisé, à l'occasion du versement de la subvention que j'accordais à une école d'ingénieurs, d'éviter le *Wi-Fi* dans les laboratoires et de préférer les réseaux câblés. Cette école d'ingénieurs, qui avait des contrats avec des entreprises privées, s'exposait inutilement.

Ma deuxième observation concerne le fait que, dans les entreprises, il apparaît impossible que des compagnies d'assurance acceptent d'assurer le risque numérique.

En tout cas, dans les entreprises comme chez les particuliers, des précautions simples pourraient être prises comme l'arrêt de tous les appareils en cas de non utilisation, ou du moins en fin de semaine, au lieu d'une simple mise en veille.

Par exemple, en ce moment, n'importe qui peut écouter ce qui se passe ici grâce à nos téléphones alors qu'ils sont en veille.

M. Bruno Sido. – Je serais tenté de répondre qu'effectivement, ce problème existe avec tout ce qui est hertzien, mais la sécurité n'est pas meilleure avec la fibre si les fabricants ont prévu des « portes dérobées » aux bouts de celle-ci,. Pour ceux qui ont des informations vraiment confidentielles à transmettre, cela n'est pas plus sûr.

D'ailleurs l'exemple de l'homme d'affaires qui se rend en Chine avec ses ordinateurs et ses téléphones personnels ou professionnels montre combien on est exposé à l'erreur. Il devrait partir avec des ordinateurs vides et des téléphones simples achetés pour la circonstance et qui ne feraient plus usage ensuite. Dans le cas contraire, il est susceptible de se faire piller les informations disponibles sur ses appareils, et, de ce fait, de ne pas pouvoir conclure des affaires très importantes.

Mme Catherine Procaccia, sénatrice. – Je trouve que vous avez été très ambitieux en pensant qu'un rapport de l'OPECST pouvait apporter des solutions au risque numérique.

En outre, depuis quelques années, il y a, comme vous le citez, l'ANSSI et d'autres organismes qui interviennent sans arrêt, ce qui n'empêche pas tous les risques. Alors les précautions que vous évoquez seraient importantes aussi bien pour les entreprises que pour les hommes politiques qui nous dirigent. Quant à ce que font les assemblées parlementaires, cela est plutôt public.

Je rapproche de ce que vous venez de dire de ce qui a été exposé précédemment à propos des vaccins. Pour le risque numérique, c'est la même chose ; il y a des virus qui nous atteignent et des gens qui essayent d'attaquer les données des entreprises et des gouvernements.

Il pourrait y avoir des sortes de vaccins consistant à crypter les données et à éteindre tous les appareils systématiquement lors de leur non utilisation, même si on ne le fait pas.

Je ne sais pas si le rapport va pouvoir apporter grand-chose mais, en tout cas, je puis vous affirmer que, en matière d'assurance, il est actuellement impossible d'assurer le risque numérique puisque le principe de l'assurance repose sur l'analyse des risques qui se sont produits. Alors, quand vous dites que 73 % des entreprises se sont fait piller des données, comment voulez-vous que des assureurs puissent proposer quoi que ce soit, puisque le coût de l'assurance risquerait d'être supérieur à celui de la sécurisation du système informatique de l'entreprise ?

J'ai la connaissance d'un certain nombre d'entreprises où les salariés se plaignent parce que, tous les mois, si ce n'est pas toutes les semaines, ils ne peuvent plus accéder à leur messagerie parce qu'on leur demande de changer leurs mots de passe.

Il me semble que les entreprises qui exportent ont conscience de l'ampleur du risque numérique mais il reste difficile de trouver les moyens d'une sécurité totale, sans parler des moyens financiers et des moyens intellectuels qui risquent d'être inférieurs à ceux mis en œuvre par les pirates.

M. Daniel Raoul, sénateur. – En ce qui concerne la comparaison avec les virus, cela n'est pas tout à fait équivalent puisque, dans le domaine du numérique, outre les virus, il existe la volonté des pirates qui se livrent à l'attaque sans qu'il y ait forcément de virus injecté.

Mme Anne-Yvonne Le Dain. – Nous avons reçu en audition plus de cent personnes, de l'écrivain à des responsables industriels. En débutant cette étude, nous savions que le sujet était très riche, mais nous n'avions pas imaginé qu'il l'était à ce point. En fait, on entre dans un nouveau monde où l'on ne peut pénétrer avec les réflexes de l'ancien monde, plus rationnel.

Le nouveau monde est complètement multiforme, multi-ouvert, et ne pas se protéger est une bêtise. Par exemple, après l'attaque contre les *Twin Towers*, les Américains ont pris le *Patriot Act* et s'en servent pour tout, y compris à des fins économiques. Ils ont condamné récemment une très belle entreprise française au motif qu'elle avait une sous- filiale dans un endroit célèbre où elle avait payé un contrat en dollars ; j'en suis resté abasourdie.

Donc les Américains se servent de la sécurité numérique comme d'un enjeu doctrinal, économique. Actuellement, les *GAFA (Google, Apple, Facebook et Amazon)* continuent réussi à faire en sorte que la police de l'Internet soit assurée par une entreprise privée située en Californie, l'*ICANN,* grâce à laquelle la *NSA* américaine s'est procurée les adresses Internet du monde entier. Or, aujourd'hui, les entreprises américaines ont bien conscience que l'Europe est un espace pertinent économiquement. Elles sont donc présentes à Bruxelles où se négocie actuellement le traité transatlantique. Autour de la table de négociation sont présents des dizaines et des dizaines d'Américains qui expliquent à quel point ce traité est une évidence, et qu'il faut lui soumettre l'ensemble du numérique.

Comme il y a davantage d'utilisateurs d'Internet en Europe qu'aux États-Unis d'Amérique, l'Europe est leur meilleur client. Il importe donc de se protéger des Américains, par exemple en créant un *Google* européen. Même si les Américains sont des alliés et des amis, économiquement nous sommes leur meilleur marché.

Sur la question de la sécurité numérique, nous disposons de tout ce qui convient en France et en Europe pour enclencher une dynamique sectorielle s'appuyant sur de nouveaux concepts, et permettant d'aller vers un autre monde que celui que l'on a connu jusque-là. Il n'y a plus de barrières économiques ou techniques comme autrefois ; aujourd'hui, tout est réversible. Il faut de la vitesse, de la réactivité, de l'intelligence et de l'initiative locale, car l'échelon national ne fonctionne plus. Il faut multiplier les nouvelles procédures et les nouveaux procédés autour des concepts de multi-acteur et de multi-action, et construire de l'opacité au moyen de nuages de points. Il faut jouer sur le fait que le numérique est nanométrique et nanoseconde.

M. Jean-Yves Le Déaut. – Nous avons maintenant à conclure. Un certain nombre de corrections tardives ont été proposées, notamment sur le préambule et l'introduction. Avec l'accord des deux rapporteurs, j'ai comparé les versions et constaté que beaucoup de modifications souhaitées étaient relativement mineures. Si vous en êtes d'accord, je transmettrai le document annoté par mes soins aux rapporteurs afin qu'ils intègrent mes remarques au document final.

Le président Bruno Sido a indiqué votre intention de ne pas en rester aux aspects d'ordre général du sujet, comme la gouvernance mondiale de l'Internet, mais vous avez tout de même traitée celle-ci, et même bien traitée, et c'est bien l'un des gros problèmes de la sécurité des systèmes informatiques que cette mauvaise gouvernance internationale de l'Internet. Je pense donc que des questions comme la démocratisation de l'*ICANN*, ou l'idée d'un affichage d'icônes renseignant mieux les usagers pourraient figurer dans la conclusion.

Finalement, tant qu'on n'aura pas fait évoluer le système de gouvernance, notamment au niveau des langues, car la domination linguistique de l'anglais conforte la mainmise américaine sur Internet, nous aurons toujours de grandes difficultés à traiter les problèmes de sécurité numérique et de chaîne de sécurité.

A la fin du rapport, le *vade-mecum* à destination des entreprises est très bien. Il faudrait que la partie de la conclusion intitulée « *Faire de l'économie avec du droit* » figure avant les recommandations. Enfin, je suggérerais de développer les intitulés des principales recommandations.

Nous sommes ainsi arrivés, d'après moi, à un très bon rapport. Je voudrais encore vous remercier car il s'agissait là d'une étude compliquée. Je voudrais encore remercier l'expert pour son apport.

Il faut maintenant fixer un titre qui convienne. Les rapporteurs ont carte blanche pour en décider.

Je vous propose d'adopter ce rapport et ses conclusions. Qui vote contre ? Qui s'abstient ? Le rapport est adopté à l'unanimité et je vous en remercie.

À la suite de ce débat, l'Office a autorisé la publication de ce rapport.

– **Présentation des conclusions de Mme Anne-Yvonne Le Dain, députée, relatives à l'audition publique du 3 juillet 2014 sur le thème « *Construire une société nouvelle, améliorer notre compétitivité grâce à la recherche environnementale* » ;**

Mme Anne-Yvonne Le Dain, députée, vice-présidente. – Cette audition constituait une première puisque l'Alliance nationale de la recherche pour l'environnement (AllEnvi) a souhaité présenter une partie des résultats de ses travaux devant l'OPECST. La démarche est apparue particulièrement intéressante car elle met en lumière les retombées positives de la recherche et la nécessité de soutenir celle-ci sur le long terme, afin qu'elle puisse se traduire en progrès sociétaux et économiques.

Le domaine de l'environnement a semblé parfaitement adapté pour cette démonstration car il recouvre des enjeux cruciaux pour l'avenir et se trouve au cœur des politiques publiques et des préoccupations de nos concitoyens. Parmi les différents groupes thématiques que comporte l'alliance, l'audition a mis l'accent, en matière de valorisation, de transfert et d'innovation, sur la place fondamentale du comité de valorisation de l'alliance : CoVallEnvi qui coordonne les différents services de valorisation des membres de l'alliance. La question de la propriété intellectuelle (dépôt de brevets, signature de licences, …) constitue notamment un enjeu important si l'on veut protéger les innovations issues de la recherche publique.

L'audition a présenté un certain nombre de réalisations significatives choisies dans les domaines très diversifiés que recouvre la recherche environnementale qui peuvent aller de la mesure de la qualité de l'air intérieur jusqu'au plantes à traire, en passant par la restauration des populations d'esturgeons, pour ne citer que quelques exemples. Ces exemples concrets de partenariats d'entreprises ou de collectivités publiques avec des organismes de recherche illustrent les différents types d'impacts que la recherche environnementale peut avoir sur la société et sont l'occasion de prendre conscience de l'utilité de celle-ci. La recherche environnementale repose actuellement sur une forte pluridisciplinarité et un travail collectif qui intègre les sciences humaines et les sciences sociales pour mieux appréhender les retombées économiques et sociétales de celle-ci. Elle est appelée à jouer un rôle déterminant en matière de prévention et de débouchés technologiques, en s'appuyant notamment sur les bases de données et la modélisation.

L'audition a souligné les temps de développement longs de la recherche environnementale et des applications industrielles qui peuvent en découler. Il est donc essentiel de développer des moyens de financement adaptés à ces temps de cycles longs. A cet égard, Bpifrance est susceptible de jouer un rôle d'impulsion décisif.

Il apparaît également important d'accélérer les processus d'homologation. L'interface entre la recherche et la réglementation constitue un préalable indispensable : des évolutions réglementaires sont souvent nécessaires pour permettre l'émergence d'un marché. Cela implique une réflexion sur le principe de précaution qui prenne en compte les évolutions technologiques et économiques. Ainsi, il serait souhaitable de revoir la composition des commissions d'évaluation et d'y introduire plus de diversité, en y faisant figurer davantage d'universitaires, à côté des spécialistes de la réglementation. D'une manière générale, l'innovation devrait être mieux prise en compte dans l'évaluation des chercheurs et des laboratoires, dans le domaine des sciences de l'environnement comme dans les autres.

Il est indispensable de constituer des filières qui partent de la recherche fondamentale pour aller jusqu'aux PME, en bénéficiant du soutien de grands groupes industriels français. Les dispositifs financiers d'accompagnement et de soutien, qu'ils soient publics ou privés, sont essentiels aussi bien aux étapes de pilotage et de pré-industrialisation, qu'au moment de la mise sur le marché. C'est ainsi qu'on pourra gagner des parts de marché, y compris à l'international et créer un nombre significatif d'emplois, permettant à la recherche environnementale d'être porteuse d'avenir et facteur de progrès social.

Cette première audition publique appelle une poursuite des contacts entre l'OPECST et l'alliance AllEnvi, notamment à travers des visites sur place qui sont déjà envisagées.

La séance est levée à 18 h 30

Membres présents ou excusés

Office parlementaire d'évaluation des choix scientifiques et technologiques

Réunion du mercredi 28 janvier 2015 à 16 h 30

Députés

Présents. - M. Christian Bataille, Mme Anne-Yvonne Le Dain, M. Jean-Yves Le Déaut, M. Jean-Louis Touraine

Excusés. - M. Alain Claeys, M. Alain Marty, Mme Dominique Orliac

Sénateurs

Présents. - M. Gilbert Barbier, Mme Catherine Procaccia, M. Daniel Raoul, M. Bruno Sido

Excusés. - Mme Delphine Bataille, Mme Marie-Christine Blandin, Mme Brigitte Gonthier-Maurin, M. Jean-Pierre Leleux, M. Gérard Longuet, M. Jean-Pierre Masseret, M. Christian Namy