ASSEMBLÉE NATIONALE

XIVe LÉGISLATURE

Compte rendu

Office parlementaire d'évaluation des choix scientifiques et technologiques

Audition publique, ouverte à la presse, sur le risque numérique (deuxième partie)

Jeudi 21 février 2013
Séance de 14 h 30

Compte rendu n° 21

SESSION ORDINAIRE DE **2012-2013**

Présidence de M. Bruno Sido, sénateur, *Président* et de M. Jean-Yves Le Déaut, député *Premier vice-président*

ASSEMBLÉE NATIONALE

Office parlementaire d'évaluation des choix scientifiques et technologiques

Jeudi 21 février 2013

Présidence de M. Bruno Sido, sénateur, Président,
et de M. Jean-Yves Le Déaut, député, Premier vice-président

La séance est ouverte à 14 h 30

- Audition publique, ouverte à la presse, sur le risque numérique

DEUXIÈME PARTIE :
PRÉMUNIR LA SOCIÉTÉ CONTRE LE RISQUE DE LA DÉPENDANCE NUMÉRIQUE

Première table ronde : la sûreté numérique dans la gestion courante

Présidence de M. Bruno Sido, sénateur, président de l'Opecst

M. le président Bruno Sido. Après avoir parlé ce matin de sécurité numérique et de résistance des systèmes aux attaques, nous abordons cet après-midi un sujet tout aussi important, celui de la sûreté intrinsèque de ces systèmes. Nous examinerons successivement les questions de l'étendue de l'exposition aux risques de défaillance, de la fiabilité des appareils servant au diagnostic en matière de santé et de la capacité à certifier la validité des systèmes numériques.

Comme un certain nombre d'entre nous, j'ai grandi dans une société sans ordinateur. Notre premier contact avec l'informatique se faisait par l'initiation à des langages aux intitulés étranges, comme le cobol ou le fortran, qui permettaient de faire fonctionner un ordinateur dont les calculs se traduisaient par un amoncellement de cartes perforées.

C'est une banalité de pointer l'ampleur des progrès accomplis depuis, mais j'ai la conviction que la numérisation de la société en est au stade où, comme le nénuphar, elle ne remplit que la dixième partie du bassin, avant d'en occuper la moitié demain et la totalité après-demain.

L'aviation civile est un bon exemple de cette progression car elle emploie des logiciels dits critiques, c'est-à-dire qui ne doivent pas connaître de défaillance. Le Concorde a été, en 1969, le premier appareil à être équipé de commandes de vol électronique. Aujourd'hui, les commandes de vol d'un A380 comptent plus d'un million de lignes de codes. Demain, d'ici 2025, la navigation aérienne sera assurée par un système entièrement numérisé dont les codes compteront des millions de lignes. Au stade ultime de cette évolution, les avions de ligne seront devenus des objets numériques pouvant rectifier en permanence leur trajectoire en fonction de leurs perspectives d'atterrissage, de la météo et du trafic aérien. Cet exemple nous permet de mesurer l'ampleur du défi qui nous attend.

Produire des logiciels est une chose, vérifier leur validité en est une autre. Le logiciel de conception des trains d'atterrissage de l'A380 est six fois moins volumineux que ses logiciels de vérification. Les écoles françaises de mathématiques ont développé, à compter du milieu des années soixante-dix, des instruments comme l'analyse statique et la vérification formelle qui s'assurent de la validité de systèmes de plus en plus massifs à moindre coût. En dépit de l'excellence de nos chercheurs dans ce domaine et de l'intérêt de nos industriels pour ces questions, je ne suis pas sûr que les pouvoirs publics français aient conscience de l'importance de ce qui se profile. C'est pourquoi je souhaite que l'Office, dont c'est la vocation, soit saisi de ces questions.

La première table ronde de cet après-midi va nous conduire à nous pencher d'abord sur l'importance prise par les systèmes numériques dans les dispositifs de gestion courante. Cette dépendance fragilise *de facto* toute l'architecture sociale. La crainte cataclysmique du fameux bug de l'an 2000 est une anticipation, certes exagérée, de ce phénomène. La question est de savoir à quelle vitesse la réalité va finir par rattraper ce type d'appréhension. C'est une interrogation que je soumets à M. Gérard Berry.

M. Gérard Berry, professeur au Collège de France, membre de l'Académie des sciences et de l'Académie des technologies. Je suis ravi que vous ayez pris l'exemple de la navigation aérienne, domaine dans laquelle la France était très en avance. Il était devenu impossible de piloter des avions de chasse à la main. En outre, l'informatique a permis une navigation plus économique, plus légère et surtout plus sûre.

Elle est désormais partout et ses applications sont innombrables. Je vais vous parler aujourd'hui de ses dangers, mais ceux-ci ne doivent pas faire oublier ses succès, qui sont plus importants.

Il y a deux grands dangers liés à l'informatique : les bugs et l'inculture informatique.

Il faut savoir qu'un programme informatique est un système qui exécute exactement et obstinément des ordres extraordinairement détaillés, y compris ceux qu'on n'aurait pas dû lui donner, d'où les bugs. Cela ne signifie pas que tous les systèmes engendrent des bugs. En avionique, l'extrême sophistication des méthodes de développement et de certification des équipements informatiques permet de les éviter. En réalité, les bugs sont dus au manque de soin dans la fabrication des applications. C'est le cas pour les téléphones portables, les industriels ayant d'abord le souci de sortir de nouveaux produits le plus rapidement possible pour conquérir des parts de marché. Il est vrai que la qualité des téléphones portables n'est pas un enjeu vital, à la différence de celle d'un avion. Les équipements informatiques posent également beaucoup plus de problèmes dans les voitures que dans les avions, parce que la règle de base des constructeurs automobiles est de réduire les coûts.

Le manque de culture informatique est peut-être plus grave, dans la mesure où il est plus difficile d'y remédier qu'à un simple problème technique. Pendant très longtemps, nos dirigeants ont relégué l'informatique à une place ancillaire. Cela s'explique par le fait qu'ils sont généralement dépourvus de toute formation dans ce domaine, voire du simple bon sens qui leur permettrait de comprendre à peu près comment cela fonctionne. Faute de cette qualité, on a tendance à projeter sur ce sujet les compétences apprises ailleurs. Je me suis ainsi rendu compte que les ingénieurs avec lesquels j'ai été amené à travailler sur le projet de navette Hermès appliquaient à l'informatique des raisonnements de mécanique.

Pour contrer les bugs, les informaticiens, tant les chercheurs que les industriels, développent des techniques de génie logiciel ou de mathématique formelle, domaine où la France excelle. Malheureusement les techniques de génie logiciel ne bénéficient pas de la même considération que les techniques de génie mécanique.

Il faut donc promouvoir les systèmes qui marchent, car ils existent : on n'est pas obligé d'utiliser des programmes qui ne fonctionnent pas ! Si la commande publique en matériel informatique n'était pas obnubilée par le critère du moindre coût, l'État risquerait moins de bugs, dont le coût peut se révéler important : récemment, un bug affectant la fabrication d'un des transistors du dernier Pentium a coûté un milliard de dollars à Intel.

L'autre remède, c'est l'éducation. Aujourd'hui que tout est numérique, il est grand temps que les ingénieurs et les dirigeants soient éduqués à l'informatique. L'éducation à l'informatique fait d'ailleurs l'objet de travaux de l'Académie des sciences. Il faut absolument que les parlementaires se saisissent de ce sujet crucial : nous ne serons pas en mesure de fabriquer des systèmes fiables et exportables tant que la culture informatique ne sera pas généralisée dans notre pays. Comme le disait Jean Vilar, « si vous trouvez que l'éducation coûte cher, essayez l'ignorance. »

M. le président Bruno Sido. Monsieur Marko Erman, comment percevez-vous les progrès de la numérisation globale de la société ? Ne risquent-ils pas de générer à terme un grave risque de système ?

M. Marko Erman, senior vice president, recherche et technologie, chez Thales et membre de l'Académie des technologies. Je voudrais vous sensibiliser à l'importance des données dans la société numérique. Notre société de l'information se caractérise par une production massive de données numériques de toutes sortes et la capacité de les interconnecter et de faire communiquer les personnes, les objets et les différentes organisations. Ces données sont en quelque sorte la matière première de la société de l'information. Elles représentent un enjeu économique, stratégique, voire culturel, majeur. C'est sur cet enjeu et ses risques associés que je voudrais centrer mon intervention.

Ces données viennent de partout et de tout le monde. Chacun de nous crée des données, soit de façon passive, à travers son identité numérique ou la dématérialisation d'actes administratifs, soit de façon active, par exemple en participant à des réseaux sociaux. Les entreprises, les banques, les institutions à travers leurs activités de production, de gestion, d'interaction avec les clients, en produisent beaucoup. De plus en plus de données sont également produites par des systèmes dits embarqués, qui, à travers différents capteurs, interagissent et recueillent des informations liées à leur environnement. En 2012, 2,5 Exabyte de données ont été produites chaque jour, soit dix fois plus qu'il y a à peine cinq ans, et 50 000 fois plus que la somme de toute la littérature de l'humanité. Ces chiffres donnent le vertige, et on pourrait les multiplier à loisir. Nous sommes entrés *de facto* dans l'ère des *big data*, c'est-à-dire des ensembles de données dont la taille va au-delà de la capacité actuelle des logiciels de gestion.

La problématique des données est indissociable de celle des réseaux de communication qui permettent de les échanger, de les stocker et de les consulter.

D'ores et déjà, toutes nos infrastructures – aéroports, gares, stations de métro, lignes ferroviaires, autoroutes, centrales d'énergie, etc. –, leurs systèmes de contrôle et les outils industriels sont interconnectés, voire connectés à Internet, directement ou indirectement, de

manière permanente ou temporaire. Basés sur ces technologies de l'information – capteurs, données, communication –, des systèmes extrêmement complexes deviennent possibles, tels que les villes intelligentes, les *smart cities* ou les réseaux de distribution d'énergie du type *smart grids*.

Les systèmes qui pilotent nos infrastructures produisent beaucoup de données mais, dans la majorité des cas, ne les exploitent pas. Ils réagissent en fonction de celles « du moment » – alertes remontées par des capteurs, contrôle de la validité d'un titre de transport, par exemple – mais ne tirent partie ni du passé, ni de la totalité des données disponibles pour prendre ou proposer une meilleure décision. Ce n'est pas étonnant : jusqu'à récemment, le trop grand volume de celles-ci et les ressources de calcul nécessaires pour les traiter rendaient cette tâche difficile.

Aujourd'hui, les progrès dans le domaine de l'algorithmique – le réseau Internet, le *cloud* – et les capacités accrues de traitement des données sont autant d'atouts supplémentaires pour s'attaquer à ce défi. Des approches mathématiques adaptées doivent permettre d'extraire des informations pertinentes. Il est important de comprendre que ceci peut se faire hors hypothèses *a priori* : on découvre en quelque sorte l'information cachée. C'est bien cela qui donne au couple « données brutes – information extraite » une valeur économique et stratégique forte.

La valeur économique fonde le « *business model* » des grandes entreprises du web, telles Google, Facebook ou Twitter. L'objectif de ces sociétés est de collecter le maximum d'informations sur le plus grand nombre d'usagers possible pour leur offrir un service personnalisé. Des acquisitions récentes ont montré que la valeur de celles-ci est directement liée à la taille de leur base clients.

Lorsque le champ des données inclut des éléments relatifs aux activités industrielles, financières, au transport, à l'énergie, son caractère stratégique devient évident. Les grands pays, et d'abord les États-Unis, l'ont parfaitement compris. Ils en exploitent formidablement le potentiel économique. Mais des initiatives, comme le *Patriot Act*, montrent, s'il en était besoin, que la valeur stratégique des données est au centre des préoccupations liées à la sécurité nationale. Aujourd'hui, et plus encore demain, les grands pays qui connaissent un développement économique rapide, comme l'Inde, la Chine ou le Brésil, emprunteront le même chemin. Il est certain que ces pays voudront exploiter eux-mêmes cette matière première.

La France ne peut rester indifférente à ce qui est un enjeu majeur pour notre pays aussi, et, au-delà, pour l'Europe.

Pour relever ce défi, elle ne manque pas d'atouts, dont en premier lieu l'excellence de notre recherche en mathématiques – je rappelle que cette science est à l'origine des algorithmes nécessaires aussi bien à l'exploitation des données qu'à leur protection. C'est pourquoi elle doit être préservée et renforcée.

Le comité interministériel pour la modernisation de l'action publique du 18 décembre 2012 a présenté la transition numérique comme « un formidable levier de modernisation de l'action publique », porteur de valeurs « d'égalité, de neutralité, de transparence, d'efficacité et d'adaptation ». Cette transition comportera quatre volets : l'amélioration du service à l'usager ; le développement des services numériques ; l'ouverture de l'administration et des données publiques ; la modernisation des systèmes d'information.

La démarche « *Open Data* » et la création de la structure ETALAB s'inscrivent parfaitement dans ce souci d'ouverture des données publiques, permettant de créer de nouveaux services. C'est pourquoi il faut la soutenir. Cependant, si on veut se prémunir contre les risques potentiels, il est important de prendre en compte dès maintenant la problématique de la sécurité, en même temps que celle des formats et du stockage.

Ce qui est vrai pour les données publiques l'est encore plus pour toutes les autres.

Du coup, la question de la fiabilité et de la protection des informations devient cruciale. Elle nous ramène directement à la problématique sur les données dont elles sont extraites. Au-delà des problèmes de cybersécurité, absolument essentiels, il faut établir les conditions qui permettront d'assurer l'intégrité des données et la confiance numérique. Cela nécessite de maîtriser les technologies de stockage de celles-ci, les réseaux de transmission et bien évidemment l'analyse et l'exploitation.

On le sait, l'informatique en nuage offre des solutions économiques et performantes pour le stockage et est capable de fournir des services à la demande. Au travers de la création de sociétés comme CloudWatt et d'autres, la France commence à se doter de solutions de *cloud* sécurisées. C'est absolument nécessaire dans ce contexte.

Le réseau Internet, qu'il soit fixe ou mobile, assure l'indispensable interconnexion entre tous ses points – serveurs, capteurs, usagers, etc. Il est considéré comme intrinsèquement résistant aux chocs puisqu'il s'agit d'une immense toile qui peut supporter la perte d'un ou plusieurs nœuds de connexion. Cependant, si, dans sa description logique, il se compose de plusieurs centaines d'opérateurs, offrant ainsi de la redondance, le réseau physique a, quant à lui, une réalité moins diversifiée. Certaines catastrophes naturelles récentes ont montré la fragilité des réseaux de communication. Il est donc également essentiel d'améliorer leur résilience. Pour ce faire, il est nécessaire que l'analyse des risques prenne en compte les cas exceptionnels, voire aberrants.

J'ai essayé de vous faire partager ma conviction que les données vont jouer un rôle essentiel dans la société et l'économie numérique. Leur valeur économique et stratégique est d'ores et déjà établie, mais les possibilités dépassent l'imagination. Il est indispensable de maîtriser cette évolution en étant lucide sur les risques potentiels. Mme la ministre déléguée Fleur Pellerin a récemment déclaré : « Si la sécurité des systèmes d'information n'est pas assurée, aucune économie moderne ne peut prospérer ». Cela nécessite de garantir la sécurité des données, de mettre en place des opérateurs de confiance et de promouvoir une approche de régulation, de préférence à une approche purement réglementaire.

M. le président Bruno Sido. Le secteur de la santé bénéficie, comme tous les autres secteurs, des progrès de la numérisation. L'audition du président de l'Académie des technologies nous a fait découvrir les perspectives intéressantes de la « domomédecine » pour les soins à domicile. Cependant, une défaillance des systèmes constituerait une menace directe pour la santé des personnes. Comment peut-on garantir, monsieur de la Boulaye, la sécurité des systèmes numériques œuvrant dans ce secteur sensible ?

M. Olivier de la Boulaye, directeur du développement du secteur santé d'Altran. Je vous répondrai à travers une illustration : le projet PICADo, premier système opérationnel de domomédecine. Cela me permettra de vous présenter les solutions que nous pouvons, nous, les industriels, proposer pour sécuriser l'utilisation des données de santé.

Je rappelle que la domomédecine est un terme inventé par François Guinot, Président honoraire de l'Académie des Technologies, après la parution du rapport de cette Académie « Le patient, les technologies et la médecine ambulatoire » et repris à l'occasion de la journée Télésanté organisée Conseil Régional de Champagne-Ardenne le 4 novembre 2009. La domomédecine se définit comme l'ensemble des actes et soins, parfois complexes, dispensés au domicile du patient ou durant ses activités socio-professionnelles, au moins comparables en quantité et qualité à ceux effectués à l'hôpital voire de meilleure qualité, s'appuyant sur des technologies modernes. Elle vise à privilégier le maintien à domicile ou en activité et à stimuler le progrès médical.

C'est le cas par exemple de la chrono chimiothérapie, une des thérapies du projet PICADo. Le patient enverra à son médecin, *via* des capteurs communicants, des éléments tels que sa température ou son niveau d'activité, afin que celui-ci puisse adapter son traitement et proposer en temps réel le meilleur moment d'administration et les meilleurs dosages.

Ce type de dispositif doit évidemment respecter le cadre législatif et réglementaire existant, c'est-à-dire le décret du 19 octobre 2010 relatif à la télémédecine et la loi « informatique et libertés ». Les industriels que nous sommes doivent en outre tenir compte des préconisations du conseil de l'ordre des médecins et de celui des pharmaciens.

Selon l'article 34 de la loi « informatique et libertés », « le responsable du traitement [d'une donnée de santé] est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. ». Le respect de cet article se décline selon cinq grands principes : la finalité des données ; leur pertinence – nous n'utilisons que celles dont nous avons réellement besoin – ; leur conservation pendant un temps limité – c'est le droit à l'oubli ; la sécurité et la confidentialité ; le respect des droits des personnes, qui nous impose, par exemple, de nous assurer que le patient accepte que ces données soient utilisées.

Le projet PICADo concerne quelques centaines de patients et associe à Altran des sociétés plus petites comme Axon, Voluntis, Bluelinea ou FSI, soit des partenaires aux parcours très différents, qui n'ont pas tous la même capacité à respecter les normes imposées par nos tutelles.

Un tel système de santé suppose trois niveaux de mise en place. Au niveau des processus, nous nous interrogeons sur la finalité ou l'usage. C'est la notion d'authentification, *via*, par exemple, la carte de professionnel de santé (CPS) ou la carte Vitale pour le patient. Nous cherchons ensuite comment collecter et utiliser ces informations, qui peuvent être utilisées à des fins, non seulement médicales, mais aussi médico-légales – d'où l'importance de mettre en place des systèmes garantissant une parfaite traçabilité. Deux nouveaux enjeux sont apparus récemment dans l'univers de l'e-santé : l'impact du sans-fil, qui, comme toute innovation, appelle de nouvelles solutions en termes de sécurité, et la problématique de la consommation énergétique.

Après les processus, notre réflexion porte sur les données. Nous bénéficions en la matière d'un cadre normatif assez précis, notamment en ce qui concerne l'hébergement des données de santé, soumis à l'agrément de l'Agence des systèmes d'information partagés de santé (ASIP). Cela suppose le respect d'un cahier des charges très précis en matière de redondance, de sécurisation et de traçabilité des données notamment.

Il faut enfin considérer le niveau applicatif, qui concerne la conception des logiciels, l'ergonomie ou la gestion des habilitations : beaucoup de failles de sécurité sont dues à des problèmes d'habilitation. Quant à la conception des logiciels, elle doit respecter un certain nombre de référentiels internationaux pour les systèmes d'information de santé, tel l'*Integrating the Healthcare Enterprise*, l'IHE. Ils nous permettent de respecter au mieux les très nombreuses normes en vigueur, qui sont en outre extrêmement complexes. Les seules directives européennes imposent à un projet tel que PICADo le respect de la norme ISO 13485, qui précise les exigences des systèmes de management de la qualité pour les dispositifs médicaux, de la norme ISO 62304, qui définit les exigences du cycle de vie des logiciels de dispositifs médicaux, et de la norme ISO 60601, qui fixe les exigences de développement d'un dispositif médical – pour ne parler que des plus importantes.

Je ne peux pas terminer mon propos sans évoquer deux notions. D'abord celle du « *bring your own device* ». Aujourd'hui, un médecin va plutôt utiliser son iPhone ou son iPad que son poste de travail pour transmettre des données, ce qui induit de nouveaux problèmes de sécurité des systèmes d'information de santé. La bonne nouvelle, c'est que nous avons des solutions pour y remédier.

L'autre notion est celle de modèle économique, qui appelle la capacité à proposer une itération et une progression dans la mise en place du niveau cible de conformité aux normes. En tant qu'industriel, nous souhaitons pouvoir à la fois conseiller un fabricant de dispositifs médicaux, qui est souvent une petite entreprise, et un professionnel de santé quant au bon niveau de risque.

M. le président Bruno Sido. Le dernier thème de cette table ronde va nous permettre de mettre en valeur la qualité remarquable de la recherche française dans le domaine du numérique, puisque c'est dans le cadre de l'Institut national de recherche en informatique et en automatique (Inria) qu'ont été mis au point les premiers dispositifs de vérification de la validité intrinsèque des programmes. Pourriez-vous, monsieur Gilles Dowek, nous expliquer de manière pédagogique les tenants et les aboutissants de ce problème scientifique complexe ?

M. Gilles Dowek, directeur scientifique adjoint à l'Institut national de recherche en informatique et en automatique (Inria). Les systèmes informatiques sont partout, pour le mieux en général. Ils permettent par exemple d'améliorer la qualité des soins médicaux, *via* notamment l'imagerie médicale ou la robotique chirurgicale ; ils facilitent l'accès à la connaissance, appelé à connaître une transformation radicale avec la mise en place d'e-universités. Ils ont bouleversé les modes de communications interpersonnelles. On ne peut pas, bien entendu, passer sous silence l'accroissement considérable de la productivité qu'on leur doit. C'est précisément parce que l'informatique nous apporte tous ces bénéfices que leur dysfonctionnement peut provoquer des dommages, tant matériels qu'humains, à la mesure de cette omniprésence.

On appelle domaines critiques ceux dans lesquels le dysfonctionnement d'un système informatique provoque des conséquences graves. On en compte au moins quatre : les transports, la santé, l'énergie – on a évoqué la sûreté des centrales nucléaires –, la banque et plus largement les services.

Définir les menaces pesant sur un système informatique suppose de faire la distinction traditionnelle entre sûreté et sécurité : c'est la différence entre défaillance involontaire et action malveillante. Un crash aérien, par exemple, peut être consécutif à une

panne de son moteur : c'est là un problème de sûreté. Mais s'il est dû au déclenchement d'une bombe placée dans l'avion, il s'agit d'une faille de la sécurité.

Fabriquer des objets qui fonctionnent n'est certes pas un objectif propre à l'informatique. Cependant, les objets informatiques présentent la spécificité d'être les plus complexes de toute l'histoire de l'industrie humaine. Un programme compte plusieurs dizaines de millions de lignes, contre quelques dizaines de milliers dans un roman. C'est encore plus vrai s'agissant des matériels : il y a plusieurs milliards de transistors dans un processeur, contre cinq ou dix dans un poste de radio. Il est humainement impossible de construire un système aussi complexe sans se tromper. De plus, l'interconnexion des systèmes produit des bugs généralisés ou en cascade.

Étant donné le caractère faillible des êtres humains, le développement de logiciels ne peut pas être une activité exclusivement humaine. C'est la raison pour laquelle on utilise des outils informatiques pour concevoir des systèmes sans bugs. Ces outils s'appellent l'analyse statique, la vérification dans un modèle, la preuve, *etc*. Ils sont le fruit de recherches fondamentales en théorie de la démonstration, en théorie des langages de programmation et en combinatoire, ainsi que dans d'autres domaines à la frontière de l'informatique et des mathématiques. Ils ne sont pas plus interchangeables que ne le sont un marteau, un tournevis et une clé à molette : ils traitent des problèmes différents et doivent souvent être combinés. Ensemble, ils constituent une boite à outils qu'on appelle les méthodes formelles.

Ainsi, les algorithmes et les programmes de contrôle aérien peuvent être très complexes, mais la tâche qu'ils doivent réaliser est très simple : maintenir une distance de séparation minimale entre les avions à tout instant.

Lorsqu'on a cette spécification et ce programme, il est possible, en utilisant des outils appropriés, de démontrer, au sens mathématique du terme, que tel programme vérifie telle spécification.

La preuve de programme a été appliquée à de nombreux cas, notamment aux trains de la ligne 14 du métro parisien ou à certains compilateurs utilisés par Airbus.

En conclusion, la France fait partie des pays leaders en matière de recherche dans les méthodes formelles. Il y a, dans notre pays, un véritable potentiel de développement pour une industrie dans ce domaine.

Une manière de soutenir ce développement et d'améliorer la sûreté et la sécurité des logiciels que nous utilisons tous les jours est d'imposer, lors de la commande publique de systèmes critiques, l'utilisation de méthodes formelles, par exemple en utilisant le vocabulaire des critères communs, qui mesure la qualité d'un projet sur une échelle allant de EAL-1 à EAL-7. C'est déjà le cas, mais ce pourrait être systématique.

M. le président Bruno Sido. M. Bolignano va maintenant nous expliquer comment on peut tenter de développer, au niveau commercial, une activité de vérification de la sûreté intrinsèque des logiciels.

M. Dominique Bolignano, président directeur général de Prove&Run. Je vais vous parler de l'état actuel de l'utilisation des méthodes formelles dans l'industrie et du potentiel de celles-ci.

Pour ce faire, je répartirai les trois catégories de méthodes formelles dont a parlé Gilles Dowek en deux groupes.

Celles du premier groupe – analyse statique et vérification dans un modèle – sont les plus simples d'utilisation. Elles permettent de répondre à des questions précises, mais plus limitées, et d'éviter certains types d'erreurs informatiques ou sur certaines catégories de logiciels. Gérard Berry a donné plusieurs exemples de leur application dans les transports, notamment dans l'aéronautique. Ce sont, de loin, les plus utilisées dans l'industrie.

Une dizaine de sociétés – françaises ou contrôlées par de grands groupes français – commercialisent ces technologies. Malgré un grand potentiel de croissance, ces sociétés restent de taille modeste – entre 10 et 200 personnes. Elles n'en ont pas moins une grande importance pour la sûreté et la sécurité numériques.

Le deuxième groupe de méthodes formelles concerne la preuve de programme : il faut l'appliquer là où les techniques du premier groupe ne réussissent pas, car elle est beaucoup plus coûteuse et demande plus de temps. En revanche, son domaine d'application est beaucoup plus vaste. Elle couvre à peu près tous les secteurs qu'on a cités et permet de répondre à un nombre de questions beaucoup plus important.

Il en est ainsi pour la téléphonie mobile. La plupart des informations importantes, autant pour les entreprises que pour les particuliers, passent par les téléphones, et celles qui n'y passent pas sont accessibles à distance grâce à eux. C'est donc un point de vulnérabilité très important.

Actuellement, à chaque nouvelle version, quelques semaines suffisent pour que les téléphones de dernière génération – comme ceux d'Apple ou d'Android – soient crackés, c'est-à-dire attaqués et cassés dans leur sécurité. Les pirates ou les attaquants exploitent des vulnérabilités, qui sont des erreurs logicielles. Ce sont les bogues – ou bugs dont parlait Gérard Berry. Les bogues en matière de sûreté ont moins de répercussions, mais en matière de sécurité, quelques-uns suffisent pour mener une attaque de grande envergure. Voilà pourquoi on essaie de s'approcher le plus possible du « zéro faute ».

Ces erreurs sont exploitées pour des besoins relativement modestes, mais elles pourraient l'être pour lancer des attaques beaucoup plus graves. Cela nous renvoie aux propos qu'a tenus ce matin le représentant du ministère de la défense.

Je citerai deux exemples liés à la téléphonie mobile.

Le premier concerne les entreprises. La plupart des cadres utilisent leur téléphone à des fins aussi bien professionnelles que personnelles : ils consultent des mails et peuvent charger des applications à la fiabilité douteuse. Or les erreurs logicielles peuvent être utilisées pour corrompre et faire du cyberespionnage à relativement grande échelle, ce qui peut avoir des répercussions dramatiques sur l'entreprise.

Ces erreurs pourraient être évitées par une bonne application des méthodes formelles, en particulier de la preuve de programme. Certes, cela coûte cher et est difficile à faire, mais c'est faisable.

Deuxième axe : le paiement par téléphone. S'il y a eu beaucoup d'avancées grâce à la carte à puce, le téléphone reste un élément vulnérable dans la mesure où l'on a remplacé des terminaux de paiement relativement sécurisés par des objets qui le sont beaucoup moins.

Quant à la banque à domicile, qui n'est pas considérée comme un moyen de paiement mais permet de faire des virements, elle est encore plus vulnérable.

Il ne s'agit pas d'appliquer ces techniques sur tout le logiciel. En effet, les téléphones peuvent comporter jusqu'à plusieurs dizaines de millions de lignes de codes. Les architectures modernes permettent de se focaliser sur une « base de confiance », qui ne fait que quelques dizaines de milliers de lignes de codes : en s'attaquant à celles-ci, on peut vraiment s'approcher du « zéro défaut » s'agissant des parties critiques et éviter ces erreurs.

On a dit ce matin que cette problématique connaissait une croissance exponentielle. Je le confirme : nous n'en sommes qu'au début.

L'utilisation des méthodes formelles reste très modeste, essentiellement pour des problèmes liés à leur mise en œuvre et au manque de disponibilité d'experts dans ces domaines. Cela étant, la nouvelle société que j'ai créée a pour objet de les appliquer à grande échelle : des raisons objectives m'amènent à penser que c'est possible.

Nous nous trouvons aujourd'hui dans une situation très proche de celle d'il y a trente ans, au moment de la conception en 3D. Des sociétés comme Dassault Systèmes, qui est devenu le numéro un mondial dans son domaine, ont transformé la manière dont le développement était fait. Aujourd'hui, l'enjeu est encore plus grand, car le potentiel est probablement beaucoup plus important.

Pour terminer, je rejoindrai Gilles Dowek en disant que c'est le moment de se lancer. Je le montre moi-même en investissant beaucoup. Les pouvoirs publics pourraient de leur côté favoriser l'utilisation de ces méthodes formelles, afin d'enclencher un cercle vertueux.

M. le président Bruno Sido. Je vous remercie. Le débat est ouvert.

M. Michel Cosnard, président directeur général de l'Inria. Ma question s'adresse à Dominique Bolignano : quel serait le bon modèle économique, susceptible de favoriser l'usage de méthodes de développement garantissant une meilleure qualité et une meilleure fiabilité des logiciels critiques ?

M. Dominique Bolignano. C'est un modèle que j'ai déjà testé dans de précédentes entreprises et que je compte appliquer à plus grande échelle. Il consiste à développer des composants réutilisables clés avec les méthodes formelles et à les licencier pour que, dans un deuxième temps, les clients utilisateurs demandent à se les approprier, licencient les outils et adoptent la technologie. Il faut entrer dans un cercle vertueux en démontrant que c'est faisable et utile, afin que les entreprises soient prêtes à investir.

M. Michel Cosnard. Y a-t-il un secteur d'activité privilégié ?

M. Dominique Bolignano. Oui. Nous allons commencer par le domaine de la téléphonie mobile, où il y a énormément à faire. Mais il y a aussi beaucoup à faire dans l'aéronautique, l'automobile et probablement aussi dans le domaine médical.

M. le président Bruno Sido. Monsieur le professeur, on nous a dit qu'il était humainement impossible, dans un programme de plusieurs milliers de lignes de code, de ne pas introduire quelque part une erreur, un bug. Mais ce bug, introduit involontairement par l'homme, se déclenchera-t-il de façon aléatoire ou systématique ?

M. Gérard Berry. Il est très difficile de vous répondre. Sur du *hardware*, sur un circuit, il y a des probabilités de panne qui sont chiffrées, raisonnables et mesurées. Sur un logiciel, la question n'a pas vraiment de sens. En effet, on peut ne jamais voir le bug qui existe. En général, il ne se produira pas, sauf si des hackers la cherchent. Car avec des bons hackers, la probabilité devient 1.

Ainsi, une faculté américaine a montré qu'on pouvait prendre le pouvoir sur 50 % des pacemakers livrés aux États-Unis : on peut les arrêter, envoyer 800 volts, faire absolument ce que l'on veut. Ce bug ne se produira jamais sur un humain normal, mais on peut le fabriquer exprès.

Il n'est donc pas ridicule de viser le « zéro défaut ». Cela demande de modifier le design. Il n'y a pas que la vérification, mais aussi la façon de concevoir les applications. Nous avons ainsi fabriqué des langages, dont la définition est mathématique et dont le mode d'emploi mélange formules mathématiques et commentaires en anglais.

Pour les bugs modernes, le danger réside donc essentiellement dans les hackers.

Mme Sylviane Toporkoff de l'Inria. Il existe maintenant des sociétés de hackers, qui sont très compétents. Fait-on systématiquement appel à elles lorsqu'on réalise un programme ?

M. Gérard Berry. Oui, cela arrive. D'assez nombreux hackers se sont fait embaucher, notamment par AT&T dans les télécoms.

Dans les sciences aussi, on fait de même. Après le bug d'Ariane, un grand informaticien, qui n'est pas du tout un hacker, a ainsi été employé pour analyser des programmes parce qu'il a une aptitude à découvrir des bugs là où les autres n'en trouvent pas.

Le problème est que ce n'est pas en se faisant embaucher par l'État français que les hackers gagnent le plus d'argent. Et donc, on n'a pas forcément les meilleurs …

M. Olivier de la Boulaye. Aujourd'hui, c'est le client qui définit le prix. Nous aimerions avoir recours à l'ensemble des méthodologies qui pourraient améliorer la sûreté des logiciels. Mais les clients ne sont pas forcément disposés à faire appel à une société comme celle de M. Bolignano.

Il faudrait proposer une démarche itérative. L'important est de se donner une certaine durée pour avoir un cap et anticiper ce cap. Les méthodes qui sont proposées le permettent.

Nous nous intéressons aussi beaucoup à la « base de confiance », qui permet de travailler sur un socle que l'on peut ensuite étendre progressivement, et d'apporter une première réponse aux contraintes économiques que l'on rencontre dans ce genre de projets.

M. Jean-Yves Le Déaut. On nous a indiqué ce matin que l'informatique était une suite de couches successives de travaux qui continuaient à être utilisés et qu'il était impossible d'aller explorer la totalité des réalisations anciennes.

On nous a dit aussi qu'aujourd'hui, elle était faite de systèmes intégrés, de briques associées les unes aux autres. Êtes-vous capables de vérifier qu'il n'y a pas de problème entre les briques et d'empêcher des personnes malveillantes de s'introduire dans le système d'intégration ?

M. Dominique Bolignano. Il est en effet possible de passer entre les couches et d'aller en dessous des logiciels. Ces deux problèmes peuvent être évités en choisissant les bonnes architectures. Il ne suffit donc pas d'appliquer les méthodes formelles.

En matière de téléphonie mobile, nous avons ainsi réussi à convaincre les principaux fabricants de téléphones de modifier leur architecture, précisément pour aller mettre, sous les couches de logiciels, les parties que l'on pouvait véritablement sécuriser.

M. Gérard Berry. Attention : toute l'informatique n'est pas vieille ! Elle est même principalement récente. Il s'écrit beaucoup plus de programmes maintenant qu'il ne s'en est jamais écrit. Mais les problèmes liés à la vie des appareils se posent effectivement parce qu'à l'époque, on ne se préoccupait pas de cela.

Il faut absolument fabriquer des composants de très haute qualité. D'où l'importance des procédures et des contraintes de certification. En avionique, il y a ainsi des procédures de certification internationales obligatoires et des réciprocités entre les pays. En revanche, dans le nucléaire, il n'y a que des procédures de certification nationales, nettement plus indicatives et variables selon les pays. Au Japon, par exemple, certaines normes valables dans les années cinquante sont restées les mêmes.

La qualité des règles imposées par les États est absolument essentielle. Or en matière de santé, notamment, les normes ne sont pas tout à fait définies.

M. Olivier de la Boulaye. On voit bien à cet égard que les niveaux d'exigence ne sont pas les mêmes pour un dépistage et la prise en charge d'un acte médical.

M. Gilles Dowek. Il est beaucoup plus facile de développer des produits de qualité en utilisant des méthodes formelles au moment où on les développe, que de revenir sur des vieux codes d'il y a dix ou vingt ans, ou même de vieux algorithmes. En contrôle aérien, on m'avait demandé de démontrer la correction d'un algorithme ; je n'ai pas réussi et j'ai proposé mon propre algorithme. C'est de cette manière que l'on peut faire avancer les choses : davantage par une « co-conception » – conception de l'objet et de sa preuve en même temps – que par un retour sur le passé.

Ensuite, il ne suffit pas que les composants qui sont assemblés soient sûrs pour que l'ensemble le soit aussi. Mais les méthodes formelles peuvent s'appliquer aussi bien pour démontrer la sûreté de composants que celle de l'assemblage. Si cette dernière constitue un problème plus difficile, l'objectif est bien la sûreté globale, qui n'est jamais que celle du maillon le plus faible.

M. Michel Cosnard. Gilles Dowek a évoqué les critères EAL de 1 à 7. J'aimerais qu'il les précise et nous donne quelques exemples et, éventuellement, des recommandations sur leur utilisation. Y a-t-il des cas où un niveau minimum d'exigence serait souhaitable ? Si oui, comment le traduire en obligation réglementaire ?

M. Gilles Dowek. Je reviens sur une autre question que vous avez posée tout à l'heure, relative à la probabilité qu'un bug se produise.

Prenons l'exemple du bug du Pentium, évoqué par Gérard Berry. Nous sommes face à un circuit qui fait des multiplications. Si on essaie de multiplier 3 par 4, cela fait 12 ; en revanche, si on multiplie 0 par 0 – et c'est là qu'il y a un bug – cela fait 256. S'interroger sur

la probabilité que ce bug se produise revient à s'interroger sur celle que l'utilisateur de la calculette décide de faire cette multiplication de 0 par 0.

Cela nous amène à la première méthode, que personne n'a mentionnée, consistant, pour vérifier que des programmes sont corrects, à les tester, et donc à les utiliser. On fait une, puis trois, puis dix multiplications. Si le résultat est exact pour dix opérations, on se dit que le programme ou le circuit semble correct, et l'on s'arrête là. Cela définit les niveaux EAL les plus bas, soit 1 ou 2.

Il y a ensuite, au milieu de la gamme, d'autres critères. On demande au développeur d'exprimer formellement, sans établir de preuve, mais de manière très précise et mathématique, la spécification du programme.

Ce n'est qu'aux niveaux 6 et 7, les plus élevés, que l'on demande au développeur, non seulement d'exprimer ainsi ce que doit faire le programme, mais aussi de démontrer qu'il fait bien ce que l'on attend de lui.

Ces critères correspondent à des niveaux d'exigence et de coût variables. Pour certaines applications, le bug n'est pas très grave : c'est le cas par exemple pour un DVD, au contraire d'un avion de ligne. Mais parfois il se mesure en milliards de dollars. Or pour anticiper un bug d'un milliard de dollars, on peut s'offrir beaucoup de méthodes formelles …

M. Jean-Yves Marion, responsable du Laboratoire de haute sécurité en informatique de Nancy. La sûreté informatique, le fait que les programmes n'aient pas de bugs, est importante. Mais la sécurité ne se réduit pas à cela. On peut attaquer un programme quasiment sans bug en utilisant l'ingénierie sociale, c'est-à-dire en contournant les problèmes d'usage au niveau des utilisateurs. D'où l'intérêt des systèmes de protection tels que les pare-feu, les antivirus ou les systèmes de virtualisation.

M. Marko Erman. Je suis d'accord avec vous. La sécurité n'est pas une caractéristique purement technique. Elle se conçoit au niveau d'un système.

Nous faisons des audits de cybersécurité, soit en anticipation à la demande des entreprises, soit en *post attack*. Comme dans les accidents d'avion, le facteur humain est souvent celui qui fait casser le système. Dans un système informatique totalement fermé, un immeuble blindé, si les personnels introduisent des clés USB non contrôlées, cela peut être catastrophique.

Au-delà de la sécurité technique, il faut s'intéresser à la sécurité physique, aux protocoles, aux process, à l'organisation et à la formation – *via* une sorte de labellisation ou de certification des personnes. De fait, lorsque la technologie est tellement diffusée, que toute personne est dans le système, la situation devient très difficile.

On progressera dans la sécurité quand le plus grand nombre des citoyens sera conscient des risques. Il ne s'agit pas de devenir paranoïaque, mais c'est en connaissant les risques que l'on peut se comporter correctement et s'en protéger.

M. Jean-Yves Le Déaut. Lorsque je demande à mes étudiants de Sciences Po de situer le bug informatique sur une échelle des risques, ils le classent en dernier ! Je pense que le citoyen n'a pas pris conscience de l'existence du risque informatique.

Les bienfaits de l'informatique sont avérés, mais nous devons nous prémunir contre les risques qu'elle entraîne et les attaques. L'objectif de cette table ronde est aussi de savoir s'il faut faire évoluer la législation ou mettre en place une régulation dans ce domaine.

M. Gilles Dowek. C'est précisément parce que les bienfaits de l'informatique sont nombreux que les risques existent.

M. Gérard Berry. À l'heure actuelle, les gens peuvent passer de l'absence totale d'inquiétude à l'angoisse. Ces deux attitudes absurdes prouvent qu'ils ignorent totalement ce qu'est l'informatique. Or la seule façon de maîtriser un risque, ou un bienfait, c'est d'en comprendre la nature. Il est sûr qu'un travail de fond s'impose dans ce domaine. L'éducation a un rôle essentiel à jouer à cet égard.

M. le président Bruno Sido. Vous avez parfaitement raison. Cela étant, les gens supportent de moins en moins les contrariétés – que les trains arrivent ou partent en retard, ou que les téléphones ne fonctionnent plus. Après tout, la panne d'Orange n'était pas particulièrement gênante, même si on n'a pas pu téléphoner pendant plusieurs heures.

M. Jean-Yves Le Déaut. Monsieur Berry, je vous rejoins sur le fait que les gens passent de la négation du risque à sa surestimation et sur l'ignorance en informatique. Si les sujets que l'Office étudie en amont de la législation sont ceux qui font débat dans la société – OGM, ondes électromagnétiques, réchauffement climatique, vaccins, nucléaire… –, il arrive que certains ne donnent pas lieu à débat. C'est ce qui est arrivé avec les OGM : en 1991, la transposition d'une directive européenne était passée dans l'indifférence générale. Il a fallu attendre cinq ans, soit les exportations de soja américain, pour que les OGM deviennent un problème politique. Avec les nanotechnologies, nous avons connu à peu près le même phénomène.

Si l'on aborde un sujet très tôt, cela n'intéresse absolument personne, et si on le fait trop tard, on nous prête l'intention de vouloir justifier certaines positions. Ces sujets sont très compliqués : il est difficile de se prononcer en amont des évolutions techniques et de comprendre l'incidence qu'elles auront sur la société.

M. Claude Kirchner. Je voudrais revenir sur la panne de France Télécom. Certes, il était très inconfortable de ne pas pouvoir téléphoner pendant onze heures. Mais cette panne a eu des conséquences plus larges qu'on n'avait pas envisagées : des sociétés importantes, qui faisaient passer leur cellule de gestion de crise par la téléphonie mobile, ont arrêté complètement leur activité lorsqu'elles se sont rendu compte qu'elles n'étaient plus capables de gérer une éventuelle crise.

Il ne faut pas oublier le rôle essentiel que joue la maintenance. Un logiciel a une vie et peut connaître, au cours de cette vie, des phases critiques – je pense plus particulièrement aux mises à jour. Comment ce problème est-il géré ? L'est-il de façon sûre ?

M. Gérard Berry. Ce problème a beaucoup évolué ces derniers temps. Par exemple, ceux qui possèdent un ordinateur reçoivent des nouvelles versions de logiciel – notamment du logiciel Java, qui, en ce moment, fait l'objet de nombreuses attaques. Avant, ce n'était pas le cas.

Mais ce qui vaut pour les ordinateurs est beaucoup plus compliqué pour les voitures. Je connais quelqu'un qui a acheté une voiture très moderne. Sous le capot de celle-ci, il y a

des emplacements pour l'eau, l'huile, le lave-glace … et pour télécharger des logiciels. Or les garagistes sont très démunis devant les pannes logicielles. Dans cet exemple, le malheureux automobiliste est resté bloqué dans sa voiture ! Il faut combattre l'excès de maintenance. S'il s'agit de rajouter des fonctionnalités, pourquoi pas ? Mais si cela doit conduire à rajouter des bugs, c'est très dangereux.

M. Gilles Dowek. Une panne de téléphone risque de ne pas être bénigne. Le téléphone peut servir à appeler les pompiers. Au moment de la panne d'Orange, un seul réseau était affecté et on imagine qu'il aurait été possible, en cas d'incendie, de passer par un autre opérateur. Mais prenez le cas d'une personne attachée à la sûreté d'une centrale nucléaire qui utilise son téléphone lorsqu'elle est d'astreinte. Si un incident nucléaire intervient au même moment, il peut se produire des bugs en cascade, avec des conséquences tout à fait dramatiques.

M. Marko Erman. La société a évolué. Les réseaux de données nous offrent aujourd'hui des possibilités que nous n'avions pas par le passé, comme l'approvisionnement des grandes cités. La société devient donc extrêmement dépendante de leur bon fonctionnement.

Je suis d'accord pour dire que la panne d'un réseau de téléphonie ne peut être résumée à l'impossibilité de quelques personnes de communiquer. Elle peut aussi provoquer un « arrêt » de la société.

M. le président Bruno Sido. Cela relève d'une autre table ronde. Lorsqu'on a vraiment besoin de quelque chose, on doit avoir des systèmes redondants. Surveiller une centrale nucléaire avec un téléphone portable, ce n'est pas raisonnable ! Reste que le sujet est grave. C'est bien pourquoi, ce matin, j'ai parlé de « fragilisation ».

M. Gilles Dowek. Il n'y a qu'un seul réseau Internet. Celui-ci ne peut donc faire l'objet d'un système redondant.

Mme Nathalie Le Bars, du CEA. J'ai toujours un pincement au cœur quand on laisse croire que la sécurité nucléaire pourrait passer par un portable !

Mme Hélène Legras, correspondant « informatique et libertés » à la direction juridique d'Areva. En tant que salariée d'Areva, je confirme qu'on ne peut prendre un tel risque !

Deuxième table ronde : L'installation insidieuse d'une vulnérabilité numérique tous azimuts.

Présidence de M. Jean-Yves Le Déaut, premier vice-président de l'Office.

M. Jean-Yves Le Déaut, premier vice-président de l'Office. La première table ronde de l'après-midi était centrée sur le risque de système induit par la pénétration des outils informatiques dans tous les dispositifs de gestion et de pilotage. Ce risque de système a une dimension stratégique, car une paralysie globale de la société peut être la phase préliminaire d'une attaque militaire massive.

En 1943, René Barjavel avait imaginé le retour brutal au néolithique provoqué en quelques heures par une disparition soudaine de l'électricité. L'action de ce roman était censée se dérouler en 2052, mais notre dépendance à l'égard des systèmes numériques est déjà

considérable. Notre deuxième table ronde a pour objet de montrer que la dépendance de système au niveau des outils de gestion se double d'un appétit collectif de consommation individuelle de services de communication numérique qui démultiplie les bienfaits mais aussi les risques. Il accroît en effet la fragilité intrinsèque de l'architecture sociale en cas de panne par un risque accru d'exposition à des attaques.

Les connexions individuelles à des fins personnelles, dans un contexte de proximité immédiate, ou même d'intégration, avec des outils informatiques de gestion, sont sources de failles potentielles dans les dispositifs de sécurité. Voilà qui explique l'idée directrice de cette table ronde, qui suggère l'installation insidieuse d'une vulnérabilité tous azimuts, à partir du constat du développement fulgurant des réseaux sociaux et des différentes formes du Web 2.0, qui fonctionne sur le principe d'une accumulation des données en ligne pour assurer des réponses plus rapides et précises.

Nous traiterons pour commencer de l'addiction aux systèmes numériques. Ce que certains considèrent comme un nouveau fléau crée des fragilités en raison du volume d'informations mis en ligne par les personnes concernées ; ces informations, qui concernent des individus et indirectement des organismes ou des entreprises, fournissent des points d'appui, au mieux à des ciblages aux fins de marketing, au pire à des attaques.

Nous aborderons ensuite les nouvelles formes de risques induits par le développement des réseaux sociaux. Là encore, le simple fait d'exposer sa vie publiquement, même de manière non pathologique, peut créer une faille de sécurité au profit de quiconque se donne les moyens d'analyser les informations. On peut d'ailleurs se demander si Facebook, Twitter – qui a fait son apparition à l'Assemblée nationale – ou même Google ne sont pas des formes insidieuses de l'ancien réseau Echelon, si fortement critiqué en son temps.

Nous parlerons enfin des risques pour la vie privée de la dissémination des données numériques par les services en ligne, par les systèmes de télésurveillance ou de géolocalisation et par les objets intelligents. En 2009 déjà, la revue *Le Tigre* avait montré que l'on pouvait reconstituer tous les éléments de la vie d'un internaute pris au hasard. Les protections juridiques sont de moins en moins assurées en raison du nombre toujours croissant de données disséminées, majoritairement stockées sur des serveurs situés au-delà de nos frontières. Il paraît évident que la meilleure protection personnelle consiste en une hygiène individuelle d'utilisation des outils numériques, mais cela demande un grand effort pédagogique.

Nous entendrons d'abord le témoignage de M. Olivier Oullier, qui a enregistré son intervention, sur les axes de la recherche en matière d'addiction aux outils numériques.

M. Olivier Oullier, professeur à l'Université d'Aix-Marseille. Je vous remercie de me donner une nouvelle occasion de participer aux travaux de l'OPECST. Je souhaite préciser la notion d'« addiction ». Nous avons tendance à qualifier ainsi toute pratique excessive, toute consommation massive qui outrepasserait notre contrôle. Mais une utilisation extensive, même si ses effets sont délétères, n'est pas, du point de vue médical, forcément une addiction. Je ferai référence au *Manuel diagnostique et statistique des troubles mentaux* (DSM), publié par la Société américaine de psychiatrie et dont la cinquième version sortira en mai 2013. Lors des travaux préparatoires, qui ont duré plusieurs années, les auteurs du futur DSM-V n'ont pas éludé la question de l'addiction potentielle et des troubles liés à une pratique intensive de l'Internet, mais ils considèrent pour l'instant que les données disponibles ne sont assez probantes pour permettre de qualifier cette addiction de trouble psychiatrique. Les

questions liées à cette pratique sont répertoriées en annexe du DSM mais pas, à ce jour, dans la partie principale, celle du diagnostic des troubles mentaux.

Dans l'étude *Cyberpsychology & Behavior*, publiée en 2008 et fondée sur des données recueillies entre 1996 et 2006, il y est dit en substance que certaines pratiques posent question mais qu'à ce jour la collecte des données souffre de biais dans le recrutement des sujets étudiés et que la définition même de l'addiction est problématique. Il faut donc poursuivre les études.

M. Allen Frances, professeur émérite à l'Université Duke, qui fut le président du groupe de rédaction du DSM-IV, a expliqué dans une tribune publiée en 2012, dans la version américaine du *Huffington Post*, pourquoi l'« addiction à l'Internet » était en train de devenir le nouveau concept à la mode, pointant la multiplication d'articles alarmants et de blogs arrachant des larmes, et l'apparition de protocoles de traitement à l'efficacité non démontrée – le marché explose car il y a des millions de patients potentiels. M. Frances faisait observer que, sans aucun doute, nous sommes pour la plupart devenus « accrocs » à nos appareils électroniques et que certaines personnes s'en trouvent très mal, ayant un attachement malsain et incontrôlable à ces objets. L'important, poursuivait-il, est de « définir ce qui se passe pour pouvoir le traiter : que signifie le terme « addiction », et quand est-ce une manière utile de décrire nos passions et nos besoins ? Nous ne nous considérons pas « accrocs » à nos voitures, à nos télévisions, à nos réfrigérateurs… L'attachement à l'Internet est-il fondamentalement différent ? ». M. Frances observait encore que la définition donnée à l'« addiction » à l'Internet est très proche de celle que l'on applique à la toxicomanie, qui se caractérise par trois éléments : le besoin d'une consommation croissante ; le fait de se sentir excessivement mal quand on essaye de mettre un terme à celle-ci ; la consommation compulsive, presque sans plaisir et même si les conséquences en sont désastreuses sur les plans sanitaire, sanitaire, professionnel, personnel, financier et légal.

Sommes-nous esclaves de l'Internet ? Il faut distinguer le langage que nous utilisons tous les jours et la définition médicale.

Le DSM évoque les addictions comportementales, traite des jeux d'argent, des paris, et l'Internet est un candidat à la réflexion. Mais, avec les données recueillies à ce jour, les spécialistes ont été plutôt prudents et ils attendent de voir l'évolution et d'avoir plus de données.

Nos intérêts passionnés sont à risque pour certains : ils modifient nos comportements et peuvent nous isoler. Nous avons énormément d'exemples aujourd'hui, qu'il s'agisse de l'Internet et des réseaux sociaux ou de pratiques qui n'ont rien à voir avec cela. Il faut néanmoins rester très prudent et s'interroger sur les conséquences de ces comportements et, pour commencer, se poser la question de la pertinence qu'il y a à continuer de séparer comportements « réels » et comportements « virtuels », qui ne le sont plus du tout dès lors que les machines font partie de notre quotidien et induisent la mobilité et l'hyper-connectivité. Les chiffres sont ahurissants : plus de 340 millions de tweets sont échangés chaque jour ; il existe plus d'un milliard de comptes Facebook et 6 millions de vues par minute ; YouTube, présent sur plus de 350 millions de machines, propose 4 milliards d'heures de vidéo vues chaque mois pour un total d'un trillion d'heures visionnées en 2011. C'est un doux euphémisme de dire que nous avons une forte tendance à partager des informations… Pour beaucoup d'entre nous, c'est une pratique quotidienne.

La question est alors de savoir ce qui nous motive. Le plaisir, si l'on en croit une étude de Diana Tamir et Jason Mitchell, de l'Université de Harvard, publiée dans les Actes de l'Académie des sciences des États-Unis en mai 2012. L'étude a utilisé l'imagerie par résonance fonctionnelle magnétique, technique qui permet d'observer l'activité du cerveau et de voir si elle augmente de manière significative pendant certaines pratiques. Il est apparu que lorsque les individus étudiés échangent des informations personnelles, l'activité du système dopaminergique mésolimbique – l'aire tegmentale ventrale et le noyau accumbens, autrement dit « le circuit de la récompense » – augmente de manière significative.

La série de cinq expériences réalisées montre que des gens préfèrent renoncer à une récompense sonnante et trébuchante pour pouvoir continuer à partager ces informations. C'est donc quelque chose d'extrêmement fort, qui s'accompagne de certains biais comportementaux, notamment une illusion de contrôle, d'immunité et d'impunité. Le fait que l'on ne se rende pas compte qu'en partageant des informations avec ce que l'on croit être quelques amis, on y donne en réalité accès au monde entier, qu'il s'agisse de nos « amis » ou de marques, d'institutions… à qui par le simple fait d'« aimer » et de partager, nous donnons un droit légal, très souvent, à l'utilisation de ces informations. Dès lors, des informations sensibles peuvent être partagées sans que les gens en soient conscients. On parle beaucoup de *big data* sans savoir réellement ce que cela implique, car il est très difficile d'évaluer les conséquences de ces nouvelles pratiques et de ces nouvelles collectes de données. Très peu d'études ont été rigoureusement menées à très grande échelle donnant des indications sur l'influence de ces réseaux.

Cependant, la revue *Nature* a publié en 2012 une étude réalisée par des scientifiques travaillant pour Facebook et portant sur 61 millions de personnes. L'étude a été menée pendant les élections au Congrès américain en 2010. À partir des envois sur le « fil d'information » de Facebook des incitations à aller voter, elle a montré l'influence qu'ont les personnes les unes sur les autres *via* les réseaux sociaux. On peut à cet égard s'interroger sur d'autres utilisations qui peuvent être faites de ce que l'on appelle l'influence des pairs, les nouvelles normes sociales transmises et diffusées par les réseaux sociaux.

Enfin, de nouveaux comportements bien réels émergent, qui sont rendus possibles par l'hyper-connectivité, la vitesse de transformation de l'information. On l'a vu avec les « printemps arabes », le mouvement des Indignés ou encore *Occupy* : se sont développées des révolutions sans chefs, une agrégation d'individus qui partagent des informations, l'émergence des « consciences virtuelles collectives » qui permettent à certains messages d'être portés. Mais comment ces mouvements se perpétueront-ils ? Un an ou dix-huit mois plus tard, on voit toutes leurs limites : certaines des idées ne sont plus coordonnées et l'on se rend compte de la limite de ces nouveaux comportements que, pour l'instant, on n'étudie pas encore assez.

On notera que, dans son *Global Risk Report* pour 2013, le Forum économique mondial a classé les « cyber-incendies sauvages » comme un risque majeur, qui peut avoir un impact sur la vie économique et sociale. On donnera pour exemple les rumeurs relatives à une banque française qui, s'étant propagées sur Twitter et d'autres réseaux sociaux, ont fait plonger l'action pendant plusieurs heures.

Il faut prendre en compte l'ensemble des risques mais aussi des bénéfices – le fait que certains consommateurs ne soient plus isolés et que l'on crée des tactiques grossières de marketing. J'observe que ce sont souvent les spécialistes du numérique qui sont interrogés sur ces questions. Il est nécessaire – et je remercie l'Office d'envoyer ce message fort

aujourd'hui – d'inclure dans vos travaux des spécialistes du comportement humain et des médecins. Il y a notamment énormément à apprendre de ce que l'on sait du fonctionnement du cerveau pour comprendre pourquoi les gens partagent des informations et pourquoi ils ont ce sentiment d'impunité et d'immunité. Les « comportements numériques » doivent être étudiés et enseignés dans les cursus des spécialistes du comportement humain et de la médecine, en coordination avec les spécialistes de la sécurité et des nouvelles technologies.

Je renouvelle mes remerciements à l'OPECST pour l'invitation qui m'a été faite et pour la considération ainsi témoignée à l'aspect comportemental, psychologique et neuroscientifique, très important dans ce qui est aujourd'hui une des questions primordiales du fonctionnement quotidien de notre société.

M. Jean-Yves Le Déaut, premier vice-président de l'Office. La parole est maintenant au Dr Marc Valleur, qui nous dira de quels éléments il dispose sur l'importance quantitative de cette forme d'addiction.

M. Marc Valleur, médecin-chef à l'hôpital Marmottan. Le scientifique qu'est Olivier Oullier et le clinicien que je suis envisageons le phénomène avec un regard différent, mais nous sommes d'accord sur l'essentiel. Si c'est de l'addiction aux jeux en réseaux sur l'Internet que l'on parle – une des formes d'addiction dont nous avons à connaître au centre Marmottan –, la prévalence de cette pathologie est infime. Parce que le consensus ne se faisait pas sur la définition de ce que serait une « cyberaddiction », nous avons constitué un réseau pour partager des cas cliniques avec des confrères suisses, belges et québécois ; sur une période de deux ou trois ans, nous sommes arrivés, ensemble, à identifier quelques centaines de cas. On voudra bien convenir que, rapporté aux millions de joueurs en réseau sur l'Internet, on est loin d'un raz-de-marée. Mais ce constat appelle d'autres questions : pourquoi un phénomène aussi mineur en nombre a-t-il une telle résonance médiatique mondiale ? Pourquoi est-ce sous l'angle de l'addiction que, très souvent, la question des jeux en réseau et d'Internet est abordée ?

Je tiens à souligner, plus nettement encore que ne l'a fait Olivier Oullier, que dépendance n'est pas addiction. Nous sommes tous dépendants de l'Internet comme nous l'avons été et le sommes de l'électricité, et comme l'humanité l'a été d'autres techniques auparavant. La dépendance peut être un phénomène tout à fait normal.

D'autre part, de faux consensus se forment autour du mot « addiction » car il a plusieurs significations. L'addiction clinique, celle dont on s'occupe quand, comme moi, on travaille depuis quarante ans avec des toxicomanes, des héroïnomanes, des cocaïnomanes, des joueurs d'argent, c'est le fait pour une personne de vouloir réduire ou cesser une conduite sans y parvenir, la perte de la liberté de s'abstenir.

En santé publique, l'addiction a un autre sens : c'est l'ensemble des dommages causés à la société par une conduite ou une consommation. Ainsi, l'immense majorité des quelque 40 000 morts dus chaque année à l'alcool en France n'a pas pour cause l'alcoolisme mais des accidents de la route, des violences ou des bagarres dont les auteurs ne sont pas alcoolo-dépendants.

La troisième acception du terme, c'est l'addiction au sens d'objet de l'addictologie. Pierre Fouquet, fondateur de l'alcoologie en France, définissait l'alcoolisme comme « la perte de la liberté de s'abstenir d'alcool » mais l'alcoologie comme l'étude de l'ensemble des

relations entre les êtres humains et l'alcool, leurs aspects positifs pour l'individu et pour la société compris.

Autant dire que, contrairement à ce que l'on pense, on ne parle pas toujours de la même chose quand on parle d'addiction.

Quelle est la réalité clinique ? Les personnes que nous recevons à l'hôpital Marmottan viennent volontairement demander de l'aide pour cesser une conduite. Certains joueurs en réseau sur l'Internet se sont dirigés vers notre service après avoir appris qu'y était organisée une consultation « jeux », ignorant que par « jeux » il fallait entendre jeux d'argent ou de hasard, la consultation étant destinée à aider des gens qui se ruinent aux machines à sous par exemple. Si nous accueillons moins d'une cinquantaine de jeunes joueurs en réseau par an, nous recevons tous les jours des appels téléphoniques de parents affolés. Une inquiétude parentale considérable s'exprime donc pour une réalité clinique qui existe, certes, mais qui est, numériquement, extrêmement faible.

Ce que nous voyons se développer depuis deux ou trois ans et que nous essayons de freiner car nous n'avons pas le personnel nécessaire pour y répondre, c'est le problème des personnes qui demandent de l'aide pour arrêter de fréquenter des sites pornographiques ou de rencontres rapides. L'addiction sexuelle se répand dans la société par le biais des sites électroniques : ce qui avait commencé par être, en Amérique du Nord, une « maladie » de quelques stars ou personnalités célèbres se démocratise car l'Internet facilite l'accès à une sexualité mercantilisée. Ce qui est particulier dans notre consultation, c'est que, dans leur immense majorité, les personnes que nous recevons se masturbent devant les sites pornographiques mais ne passent pas à l'acte par le biais des sites de rencontres.

Ce ne sont évidemment pas les technologies de l'information et de la communication modernes qui ont inventé la masturbation, que Freud disait être « l'addiction primitive ». Mais ce qui caractérise cette addiction masturbatoire assistée par ordinateur, c'est que comme pour beaucoup de pratiques actuelles, il y a un court-circuit direct entre la pulsion et le passage à l'acte : c'est une masturbation sans fantasmisation. Dans l'ancien temps, la masturbation était considérée comme un péché mortel, mais les théologiens avaient établi une gradation des fautes : le péché était mortel, soit, mais néanmoins relativement véniel si l'objet du désir était le conjoint légitime ; résolument mortel si le pécheur convoitait la femme de son voisin car il commettait alors, en plus, le péché d'adultère ; affreusement mortel car sacrilège si le fantasme portait sur l'image du Christ ou de la Vierge… Mais, dans le cas de masturbation assistée par ordinateur, on ne pense plus à rien : on regarde et on agit.

Ce court-circuit direct de la pulsion au plaisir explique peut-être pourquoi l'addiction est en passe de devenir le prisme au travers duquel nous sommes tentés de regarder tous les nouveautés qui arrivent dans la société – car ce mécanisme ne concerne pas que les sites pornographiques ou de jeux en réseau mais quantité de formes de consommation.

Ainsi, les problèmes d'addiction et de surendettement liés aux jeux d'argent ont commencé en 1987 avec l'introduction des machines à sous dans les casinos. On est alors passé de la loterie nationale, jeu de rêve où l'on imaginait ce que l'on ferait quand on serait millionnaire, à des jeux de sensation pure où l'on est hypnotisé par un écran. Cette recherche de sensation brute devient le mode dominant de consommation.

Les adolescents, dont on pense – peut-être à tort, comme le souligne le rapport de l'Académie des sciences – qu'ils sont des experts ès Internet, sont en réalité traités comme des

cibles par les marchands, et ils ne s'en rendent pas compte. Il faut appuyer l'idée d'une éducation aux nouveaux médias, au décryptage des images par les adolescents. Quand on leur fait observer que Facebook et Google sont au nombre des sociétés les plus riches de la planète alors qu'elles ne leur proposent que des services gratuits mais dont ils ne peuvent plus se passer, et quand on leur demande ce que peuvent bien vendre ces entreprises pour accumuler de si grandes richesses, ils se rendent compte que l'objet vendu est leur profil, et que leurs données personnelles serviront à cibler les publicités de la manière la plus précise possible ; alors, ils commencent à réfléchir. D'énormes progrès doivent être faits dans les familles et au sein de l'Éducation nationale pour enseigner aux jeunes gens les dangers, les risques et la bonne utilisation de l'Internet. Car un même objet, le jeu en réseau, peut être utilisé soit de manière enrichissante, soit de manière abrutissante, pour faire le vide et rendre son cerveau « disponible pour la publicité »…

La meilleure prévention de l'addiction au jeu en réseau, c'est le développement de la qualité des jeux. Plus ils seront intéressants et complexes, plus il faudra, pour jouer, utiliser son imagination et sa pensée, moins ils seront addictifs, car on devient en général « addict » à des conduites répétitives. Mais ce qui est facile à dire est difficile à mettre en œuvre, et il faudrait rappeler les sociétés de production à leurs responsabilités. Certaines en sont conscientes : ainsi, le syndicat des éditeurs de logiciels de loisirs a mis en œuvre le système signalétique européen PEGI, mais ni les distributeurs ni les parents ne sont au courant ; il faudrait améliorer l'information. Vivendi, qui fabrique le jeu le plus addictif qui soit, travaille aussi sur ces questions. Il reste à interpeller Facebook et Google sur leur responsabilité sociétale.

M. Jean-Yves Le Déaut, premier vice-président de l'Office. Le deuxième thème de cette table ronde pourrait avoir pour intitulé « Les réseaux sociaux sont-ils un cheval de Troie exposant les points névralgiques de la société ? ». Il s'agit, plus positivement, d'examiner comment l'on pourrait mieux faire prendre conscience aux internautes séduits par la convivialité en ligne de leur part de responsabilité potentielle face aux risques numériques.

M. Stéphane Grumbach va nous faire prendre la mesure des progrès fulgurants de la pénétration des nouvelles formes de l'Internet dans nos vies.

M. Stéphane Grumbach, directeur de recherche à l'Inria. La révolution numérique a engagé nos sociétés dans des transformations durables, géniales, mais dont nous sommes incapables, à l'aube de cette nouvelle ère, de mesurer l'impact. Il suffit de retourner seulement dix ans en arrière – Facebook n'existait pas – pour comprendre à quel point le changement est rapide, diffus et peu anticipé. Il est difficile de prévoir tous les services qui apparaîtront dans la prochaine décennie, mais il est déjà clair que certains de ces systèmes balayeront progressivement nos anciennes organisations.

Avant toute chose, je voudrais préciser deux points concernant l'orientation des thématiques abordées aujourd'hui. Cette journée est consacrée aux risques du numérique, non à ses opportunités. C'est une particularité européenne de voir dans la société de l'information avant tout une menace. Il en va vraiment différemment aux États-Unis ou en Asie, même si, bien sûr, le risque est un sujet pris très au sérieux et abondamment abordé aux États-Unis, en particulier ces derniers jours.

Ensuite, le sujet traité cet après-midi est intitulé : « Prémunir la société contre le risque de la dépendance numérique ». J'ai eu certaines difficultés à préparer mon intervention pour y répondre, car la question, dans le domaine de la toile et des réseaux sociaux, ne me

semble plus être de prémunir la société contre ce risque : nous sommes déjà dépendants ! Elle est de savoir si cette dépendance est problématique, si l'on peut en sortir, ou comment on peut l'aménager.

Il y a, fondamentalement, deux types de risques : le premier est lié à la société de l'information en elle-même ; le second, à la dépendance à une industrie étrangère dont nous n'avons pas la maîtrise puisque nous sommes incapables de la développer chez nous.

Le premier type me semble devoir être considéré comme les risques associés aux « *utilities* » de nos sociétés – l'énergie et les systèmes de transports par exemple –, c'est-à-dire en association avec les bénéfices de ces *utilities*, que personne n'envisagerait de supprimer, malgré les inconvénients qu'ils présentent.

Un risque spécifique retient particulièrement l'attention des Européens : celui de la protection de la vie privée. Plusieurs choses méritent d'être dites à ce sujet. D'abord, l'attention portée à ce risque est beaucoup plus forte en Europe qu'ailleurs. Or les outils de la société de l'information sont surtout conçus hors d'Europe. Ils sont donc *a priori* moins respectueux de la sensibilité européenne.

À ce jour, on peut s'interroger sur l'impact des normes européennes de protection de la vie privée sur notre capacité à construire une industrie. On pourrait souhaiter que ces normes assez exigeantes aient le même rôle que les normes environnementales sur l'industrie automobile par exemple, et contribuent à définir une nouvelle génération de systèmes de la société de l'information qui s'impose au monde. Mais on n'en est pas là.

De plus, il est difficile, je l'ai dit, d'imaginer, à dix ans seulement, l'évolution de la société de l'information et de ses services. Il est possible que les normes de protection de la vie privée se renforcent beaucoup. Il est également possible qu'il en aille autrement, et que la mise en ligne, de manière assez facilement accessible, d'informations considérées aujourd'hui comme privées et sensibles – les informations médicales par exemple –, ne pose pas vraiment de problèmes aux générations futures. Quoi qu'il en soit, ces informations sont déjà accessibles par effraction, et il faut faire avec.

J'en viens à l'anonymisation des données. Anonymiser les données, c'est perdre de l'information et donc une capacité d'extraction de connaissances et de services. Ce matin, Jean-Luc Moliner a montré l'impossibilité légale pour Orange de prévenir ses clients des attaques que subissent leurs machines. Il y a un subtil équilibre entre la sensibilité de l'opinion et l'intérêt économique et sociétal dans cette perte d'informations. Les réseaux sociaux ont vocation à enregistrer leurs utilisateurs sous leur identité véritable. Cela a suscité, tout récemment, un fort débat en Allemagne. De toute façon, Facebook et Google sont capables de calculer la véritable identité de leurs utilisateurs, en particulier par des techniques de *crowdsourcing*, en faisant travailler certains utilisateurs pour valider les informations des autres utilisateurs. On ne peut donc négliger aucune hypothèse sur le rapport que l'on aura, dans le futur, à la vie privée numérique.

S'agissant du deuxième type de risques – la dépendance à l'égard d'une industrie étrangère –, il me paraît assez sérieux. D'abord, parce que la croissance de ce secteur nous touchera beaucoup moins que les régions qui sont au coeur de ces industries. Ensuite, parce que notre influence sur la définition de la société de l'information de demain risque de rester assez marginale. Enfin, parce que cette dépendance risque de s'étendre aux nombreux services

que l'on n'imagine pas aujourd'hui et qui ne manqueront pas de devenir, eux aussi, indispensables à brève échéance.

Quant aux réseaux sociaux, ils sont en pleine évolution et leur appellation même porte à confusion. Comme je l'ai dit ce matin, Facebook, pour citer le plus connu d'entre eux, est bien plus qu'un réseau social. C'est un outil qui devient incontournable parce qu'il est utilisé pour l'authentification en ligne pour l'accès à de très nombreux services. Plus généralement, Facebook permet à un acteur économique tiers d'héberger des pages sur les infrastructures de cette société et d'accéder aux informations de ses utilisateurs avec leur consentement. Depuis sa création, il a évolué : d'outil de stockage et de diffusion de données personnelles – le réseau social à proprement parler –, il est devenu un système d'exploitation complet de ces mêmes données. Facebook, d'une certaine manière, est l'ordinateur de demain.

Une des caractéristiques essentielles de l'évolution de la société de l'information est le rôle imprévisible des données associées à certains services, qui peuvent être utilisées par d'autres services qu'on ne soupçonne pas à l'avance. Le traitement des masses considérables de données produites aujourd'hui suscite à la fois l'engouement de l'industrie du numérique et l'intérêt des scientifiques, auxquels il pose de nombreux défis. Le potentiel d'extraction automatique de connaissances à partir de données fait l'objet de nombreux débats. Jusqu'où sera-t-on capable d'aller ? Certains pensent que des découvertes scientifiques pourront être faites automatiquement à partir des masses d'informations disponibles. Nous ne sommes en tout cas qu'au tout début des potentialités ouvertes par les données numériques.

L'exemple du moteur de recherche, qui est l'un des premiers gros systèmes de la toile, illustre bien ce rôle des données. L'ensemble des requêtes faites sur le moteur permet de dresser le profil de chaque utilisateur. Mais, au-delà des utilisateurs, les requêtes permettent de générer des connaissances très riches sur des populations. Google a démontré ce potentiel en 2003, l'année de la crise du syndrome respiratoire aigu sévère (SRAS) : le système *Google Flu* sélectionne les requêtes relatives à la grippe sur l'ensemble de la planète, dans toutes les langues, et permet d'établir une cartographie exacte de la grippe en avance sur le Centre de prévention et de contrôle des maladies (CDC) des Etats-Unis.

Tout moteur de recherche, comme d'ailleurs de nombreux autres systèmes de la toile, dès lors qu'ils jouissent d'une couverture raisonnable, ont ainsi le potentiel d'analyser des populations sous d'innombrables critères. Le spectre des applications est large, du commercial au politique, en passant par la santé publique, le moral de la population… Si l'opinion publique s'est principalement focalisée sur le profilage individuel, il me parait évident qu'il y a beaucoup plus de potentiel dans le profilage des communautés, des habitants d'un pays ou d'une région et, plus généralement, de toute population satisfaisant un quelconque critère. Par ailleurs, si la publicité représente aujourd'hui plus de 90 % des revenus de ces industries, il est probable que sa proportion diminuera au profit d'autres activités, pour peut-être tomber finalement à la proportion qu'a la publicité dans l'économie globale.

Un autre type de système a fait son entrée sur la toile récemment : les cours en ligne. C'est un exemple particulièrement intéressant de l'analyse des données que l'on peut faire de manière indirecte. Accessibles à tous, ces systèmes offrent des cours de très grande qualité, associés à un matériel pédagogique. Il est évident qu'ils auront un impact sur l'enseignement traditionnel et démocratiseront l'accès aux cours des plus grands maîtres. Pour suivre ces cours, il faut s'inscrire en ligne, sous sa véritable identité ; diverses incitations rendront le contournement de cette exigence peu intéressant. Le modèle économique de ces systèmes est

simple : l'extraordinaire banque de ressources humaines, très précisément ciblées, au moment où les pays développés feront face à un manque d'ingénieurs et de scientifiques. Comme pour le moteur de recherche, la valeur ajoutée pour l'entreprise est éloignée du service offert.

Bien sûr, l'impact sur de très nombreuses institutions traditionnelles sera très important. Les négociations récentes entre Google et les organisations de presse de différents pays européens seraient d'une autre nature si l'Europe disposait elle-même d'un moteur de recherche. On peut craindre que des négociations du même type suivront dans d'autres secteurs d'activités qui, comme la presse, subissent la société de l'information et ses nouveaux outils ou services au lieu de prendre pleinement part à leur construction et à leur maîtrise.

Les données sont stratégiques pour un pays. Elles permettent l'analyse statistique d'un nombre illimité d'aspects qui, pour une part, correspondent à ceux que suivent les agences de statistique comme l'Insee. Certes, les méthodes d'analyse sont très différentes. Mais les agences de statistiques devront les intégrer au risque d'être complètement déclassées car, d'une part, les technologies d'analyse des données se raffineront progressivement, d'autre part, les analyses de flux produisent des résultats en temps réel, et non, comme pour ces agences, avec un décalage important.

Un autre aspect me paraît essentiel : celui de l'authentification de l'identité numérique. Le Royaume-Uni envisage d'utiliser le service d'authentification de Facebook pour l'accès aux services publics en ligne. On peut imaginer qu'à brève échéance la France n'aura d'autre choix que de faire de même. Le risque existe que certains services régaliens liés à l'identité des personnes doivent être confiés à de telles sociétés si l'État ne dispose pas d'outils efficaces pour l'identité en ligne ; on pourrait imaginer que, demain, la carte nationale d'identité française soit délivrée par Facebook.

M. Jean-Yves Le Déaut, premier vice-président de l'Office. La parole est à M. Serge Abiteboul. Il évoquera les pistes qui s'offrent à nous pour essayer de concilier les avantages incontestables de l'interpénétration des réseaux et de la vie réelle et les risques collectifs qu'elle suscite.

M. Serge Abiteboul, membre de l'Académie des sciences. Je commencerai par insister sur les bienfaits du développement des réseaux sociaux, dont le premier, comme l'a dit M. Oullier, est le plaisir. Les jeunes gens prennent un plaisir considérable à communiquer entre eux sur ces réseaux, et les personnes âgées, maintenant qu'elles ont à leur disposition des outils d'utilisation plus facile, se réjouissent de sortir par ce biais de leur isolement. Il faut souligner cet apport, sans se limiter à une approche par trop négative qui consisterait à ne décrire que les risques des nouvelles technologies. Il serait bon de garder à l'esprit que si l'économie californienne s'est développée à ce point autour du numérique, c'est parce que l'on en souligne, là-bas, les avantages, et que l'on essaye d'inventer de nouvelles fonctionnalités.

Mais nous sommes réunis aujourd'hui pour traiter des risques, et je dois avouer que la masturbation assistée par ordinateur ne figurait pas dans la longue liste de ceux que j'avais à l'esprit. J'évoquerai pour ma part l'atteinte à la vie privée, qui me paraît être l'un des plus graves.

Les réseaux sociaux récupèrent une masse de données pour mieux vous servir. Pour vous recommander un restaurant, mieux vaut connaître vos goûts, vos interdits alimentaires, vos problèmes de santé, le temps dont vous disposez, etc. Il se trouve que ces informations

valent beaucoup d'argent et, en un sens, c'est tant mieux, car les opérateurs peuvent offrir leurs services gratuitement.

Plus insidieusement, les données collectées permettent de mieux vous cerner. Si quelqu'un est un tant soit peu visible sur Internet, la quantité d'informations explicites est considérable, et suffit pour reconstruire sa vie. Si on creuse un peu, on peut, au moyen du traitement des *big data*, récupérer encore davantage d'informations. L'« anonymisation » des données est très relative dès lors que l'on dispose de temps de calcul.

Le web est devenu un village global, il faut s'y résoudre. L'anonymat et la protection de la vie privée sont en retrait par rapport à ce qu'ils ont été, et la situation est pire que dans vos pires cauchemars. Les données sont recoupées par des systèmes connectés entre eux. Et, avec les objets communicants, il y aura de plus en plus d'informations disponibles : on saura quand et où vous allez, ou ce que vous achetez.

Alors, que faire ? On peut agir dans quatre directions.

Premièrement, la loi. En France, on est un peu mieux protégé que dans d'autres pays grâce à la loi « informatique et libertés », même si elle n'est pas suffisante. Il est ainsi très difficile de faire respecter un droit fondamental comme le droit à l'oubli, par exemple, à cause des contrats qu'on est obligé de signer pour accéder aux réseaux sociaux et que personne ne lit parce qu'ils sont illisibles. Ce faisant, on renonce à tout droit de regard sur ses données, qui deviennent propriété de Facebook ou d'autres. Ce genre de pratique n'est pas acceptable et le législateur a du pain sur la planche. La tâche est complexe, c'est vrai. De quel droit et de quelle juridiction relève un Français en voyage au Maroc qui, pour « twitter », utilise un système américain dont les serveurs sont probablement implantés en Irlande ? En tout cas, il y a quelque chose à faire.

Deuxièmement, le travail des associations de consommateurs, qui est plus facile à mener. Un réseau social ne vaut que s'il inspire confiance car la valeur réside seulement dans les données collectées. Dès lors, le consommateur dispose de l'arme absolue : le boycott. Ainsi, quand Instagram, filiale de Facebook, a voulu s'approprier, pour les vendre, les photos qu'elle mettait en ligne, il y a eu une levée de boucliers et l'entreprise a reculé. Les associations de consommateurs ont donc un pouvoir bien réel et les pouvoirs publics devraient les aider.

Troisièmement, l'éducation. Il faut apprendre aux usagers, jeunes ou moins jeunes, à se protéger, en enseignant l'informatique. Comment, sinon, faire comprendre les risques qu'il court à quelqu'un qui ne sait pas ce qu'est une base de données, une ligne de code, une application ou un serveur ? Les citoyens internautes ne doivent pas être des analphabètes.

Quatrièmement, la recherche. Il y a beaucoup à faire pour développer des outils de protection conviviaux, à la portée de personnes qui n'ont qu'une connaissance rudimentaire, voire nulle, de l'informatique, de façon à leur permettre de spécifier le niveau et l'étendue de la protection des données qu'ils souhaitent.

Je termine par un exemple inquiétant qui vient des États-Unis, où des employeurs ont demandé à des candidats à des postes chez eux de leur communiquer leur mot de passe Facebook. L'accès à des informations privées devrait être purement et simplement interdit. De tels comportements illustrent la nécessité de s'en tenir à un principe simple : les informations

recueillies par un réseau social sont propriété de l'individu qu'elles concernent et personne ne devrait avoir le droit de les accaparer.

M. Jean-Yves Le Déaut, premier vice-président de l'Office. Depuis sa création en 1978, la Commission nationale de l'informatique et des libertés (CNIL) est au cœur de notre dispositif de protection de la vie privée. Mme Sophie Nerbonne va nous expliquer comment la CNIL continue à exercer son contrôle malgré la profusion des dispositifs de stockage des données.

Mme Sophie Nerbonne, directrice adjointe des affaires juridiques, internationales et de l'expertise de la Commission nationale de l'informatique et des libertés (CNIL). Je reprendrai à mon compte la conclusion de M. Abiteboul : les données figurant sur les réseaux sociaux sont personnelles, privées ; elles appartiennent à l'utilisateur et ne devraient pas pouvoir être réutilisées. Or on en est loin puisque le modèle économique sur lequel reposent les réseaux sociaux consiste à les monnayer.

S'agissant de la protection juridique des droits des personnes, le constat est simple : le bateau coule. Les internautes sont moins bien protégés que dans la vie réelle. Les traces qu'ils disséminent partout sur des serveurs délocalisés sont réutilisées et il est de plus en plus difficile d'avoir juridiquement prise sur des intervenants mondialisés.

Le cadre national fixé par la loi « informatique et libertés », modifiée en 2004, est insuffisant. À cet égard, le projet de règlement européen sur la protection des données personnelles comporte deux avantages considérables. D'une part, il vise à renforcer le droit des personnes. Cette approche, spécifiquement européenne, reste très minoritaire. Cela étant, une société numérique est tributaire de la confiance qu'elle inspire, si bien que les États-Unis, même en l'absence de loi générale de protection des données, y sont très attentifs. D'autre part, le règlement européen créera les moyens juridiques de peser sur les grands acteurs du numérique que sont Google, Amazone, Facebook et Apple – regroupés sous le sigle GAFA.

Le projet en cours de discussion devant le Parlement européen donne lieu à des débats virulents dans la mesure où, la législation interférant avec le modèle économique, les pressions sont très fortes, et les outils juridiques dont nous disposons menacés.

Ainsi, il faut tenir bon sur les principes et les notions de base, c'est-à-dire la définition des termes « données à caractère personnel ». Certains considèrent, contrairement à l'ensemble des autorités de protection des données, à la Cour de justice des communautés européennes et au Conseil d'État, que des identifiants numériques qui ne reprennent pas les coordonnées matérielles telles que le nom et l'adresse n'ont pas à être protégés, en particulier l'adresse IP. Comme l'ensemble du système de protection des droits d'auteur repose sur ce critère, il doit évidemment faire partie des données personnelles.

Préserver le champ d'application de la loi, renforcer les droits mis à mal par la façon dont est recueilli le consentement à l'exploitation des données – il est difficile de l'exprimer ou de le refuser quand on exige de vous de lire un contrat long et quasiment illisible –, tel est le sens de l'action de la CNIL vis-à-vis de Google. Elle mène, pour le compte de tous ses homologues européens, un travail d'investigation sur sa nouvelle politique de vie privée. Celle-ci consiste à agréger l'ensemble des politiques suivies pour la quarantaine de produits et de services offerts par Google, dans le souci d'offrir une meilleure visibilité, mais aussi de combiner tous azimuts l'ensemble des données collectées. Nous estimons que ces procédés ne correspondent pas à ce que la directive actuelle prévoit en matière de respect de l'information

et de contrôle par l'utilisateur des données le concernant. Le bras de fer est engagé avec cette société au niveau européen, le seul pertinent.

Pour protéger la vie privée, il faut évidemment une autorité de régulation suffisamment forte, disposant d'outils modernes de régulation, et qui puisse s'appuyer sur des principes solides. Contrairement à l'optique américaine qui se fonde sur la *self regulation*, des codes de conduite sur lesquels les acteurs se sont mis d'accord, nous prônons un socle législatif qui serve de base à des codes de déontologie et à la concertation sur des points pratiques. Ainsi, nous négocions les conditions de recueil du consentement des internautes concernant les *cookies* de profilage rencontrés au cours de la navigation.

Le label peut aussi contribuer efficacement à la protection. Nous n'avons développé cet outil que dans certains domaines, en matière de formation ou d'audit de traitement. Mais il pourrait parfaitement être utilisé pour des services de *cloud*, d'externalisation des données. D'ailleurs, certains prestataires, dans leur offre, garantissent que les données ne sortiront pas de l'espace européen. La protection de celles-ci peut être une source d'innovation pour les entreprises et les inciter à développer des produits labellisés conformes aux règles européennes. Cette approche susceptible d'inspirer la confiance peut attirer des clients.

Toutefois, on ne peut pas se contenter de protection juridique : la CNIL en est consciente. C'est la raison pour laquelle toutes les garanties d'ordre technique ne doivent pas être négligées. S'agissant du droit à l'oubli, les *tags*, qui indiquent à l'internaute la durée de conservation en même temps qu'il dépose la donnée sur Internet, nous paraissent une piste intéressante.

L'éducation représente enfin pour la CNIL un axe stratégique, car elle entend accompagner les jeunes générations dans leur découverte des nouveaux outils.

M. Jean-Yves Le Déaut, premier vice-président de l'Office. Je laisse la parole à Mme Chloé Torrès, qui va nous exposer les avancées et les imperfections de la couverture des données privées à l'échelle internationale.

Mme Chloé Torrès, directrice de l'activité « informatique et libertés » au cabinet Alain Bensoussan. Les données à caractère personnel, on l'a déjà dit, sont dispersées partout. Lorsqu'on ouvre un compte Facebook aujourd'hui, elles sont hébergées aux États-Unis. Ensuite, elles voyagent partout dans le monde au gré des prestations de *cloud computing* : un jour, elles seront hébergées sur des serveurs situés en Grande-Bretagne, le lendemain, elles se retrouveront en Inde.

Cela dit, il existe aujourd'hui un socle juridique substantiel qui permet de protéger les données à caractère personnel. Outre la loi « informatique et libertés », il y a la directive 95/46/CE sur la protection des données, et demain le règlement européen qui harmonisera le droit à la protection des données au plan européen. Il ne faut pas non plus oublier l'article 9 du code civil qui consacre le droit à la vie privée. Au-delà des frontières européennes, certains pays ont adopté des lois dans ce domaine : Singapour vient de le faire, la Nouvelle-Zélande aussi, à qui la Commission européenne a reconnu un niveau de protection équivalent au sien, et le texte en vigueur au Maroc est pratiquement le même que la loi française. On peut dire que le cadre « informatique et libertés » est devenu un standard mondial. Notre modèle s'impose progressivement au niveau international.

La protection des données se traduit par un droit, pour les personnes en cause, à la transparence, à l'information sur la façon dont sont utilisées les données. Et elles peuvent agir sur elles par le biais d'un droit d'accès et de suppression, bien qu'en pratique, ces droits soient souvent difficiles à mettre en œuvre.

Le vrai vide juridique, qu'il faut impérativement combler, c'est l'absence de droit de propriété. Beaucoup de plates-formes aujourd'hui revendiquent la propriété pure et simple des données à caractère personnel postées par les internautes. Dans ce domaine, l'intervention du législateur est indispensable pour créer un droit de propriété qui soit personnel, incessible et inaliénable. Il s'agit d'un enjeu majeur.

Par ailleurs, les moyens à disposition se développent. Des entreprises s'efforcent de mieux appliquer le socle juridique existant et de protéger plus efficacement les données de leurs salariés. On voit se dessiner une tendance, parmi les groupes internationaux notamment, à adopter une approche *privacy based design*. La dimension de protection des données et de la vie privée est intégrée dès la conception d'un projet. Les promoteurs veillent à la conformité de la nouvelle base de données avec la loi en s'assurant que l'information des personnes est garantie et que la protection des données est effective, en amont et tout au long de la vie du projet. Cette démarche, qui est au cœur du futur règlement européen, sera obligatoire dès qu'il aura été adopté.

M. Jean-Yves Le Déaut, premier vice-président de l'Office. C'est au tour de Mme Hélène Legras, d'Areva, de nous expliquer comment elle sensibilise les salariés à leur comportement sur les réseaux de façon à réduire les risques pour l'entreprise.

Mme Hélène Legras, correspondant « informatique et libertés » à la direction juridique d'Areva. Je vous remercie de m'accueillir pour parler d'un sujet passionnant et d'un enjeu important, y compris au sein de l'entreprise. Le statut de salarié ne donne pas à l'employeur le droit de faire n'importe quoi avec les données personnelles de ses employés. M. Alex Türk, au moment de la révision de la loi « informatique et libertés », a eu l'idée de créer les CIL, les correspondants « informatique et libertés », qui représentent en quelque sorte la CNIL au sein des entreprises. Ils sont chargés de veiller à ce qu'elles soient en conformité avec la législation. La loi « informatique et libertés » m'apparaît comme le prolongement de la Déclaration des droits de l'homme et du citoyen.

Être le correspondant unique dans un groupe comme Areva, qui compte, dans le monde entier, 280 sociétés et 48 000 salariés, fait de moi une sorte d'entonnoir par lequel passent toutes les demandes. Si un opérationnel décide de constituer une base automatisée, il viendra me demander si les données qu'il collecte sont personnelles ou non ; si leur traitement est automatisé, la loi « informatique et libertés » s'appliquera et la base devra faire l'objet d'une déclaration dans mon registre CIL.

Les instances représentatives du personnel (IRP) et les syndicats aussi se posent des questions. Eh bien, ils s'adressent à moi parce que le groupe a organisé une communication autour de ma nomination ainsi que sur mes missions. Juriste ou informaticien, le CIL doit connaître son entreprise et se faire connaître d'elle. Protéger les données personnelles constitue un sacerdoce.

J'ai beaucoup aimé, monsieur Le Déaut, que vous parliez d'« hygiène » à propos de l'utilisation des réseaux – plutôt que de « gouvernance » ou de « conformité » –, dans la mesure où il s'agit de ne pas faire n'importe quoi avec les données personnelles des salariés.

Au sein du groupe Areva, lors des formations que je fais, je recommande aux opérationnels de ne pas collecter de données sensibles – ethniques, raciales, voire philosophiques. Un service de ressources humaines peut être enclin de consigner le motif pour lequel telle ou telle personne n'a pas été embauchée. Si elle n'avait pas le profil ou les compétences, soit, mais on ne peut pas, dans les commentaires, mentionner sa tenue vestimentaire ou une information qui serait discriminatoire. Il est important que le CIL mette en garde les opérationnels contre les risques.

Sur le site intranet de la direction juridique, j'ai mis en ligne de nombreuses fiches sur le CIL, la CNIL, les données sensibles ou personnelles, dans lesquelles je donne de nombreux conseils.

Il faut aussi animer un réseau. Le CIL d'un groupe de 48 000 personnes ne peut pas tout savoir, mais il doit disposer d'une cartographie, devenue obligatoire depuis la loi « informatique et libertés ». Je tiens donc un registre de toutes les bases du groupe Areva et je sais où elles sont. Comme l'a fort bien dit Chloé Torrès, l'éparpillement provoqué par le *cloud computing* peut être dangereux pour la sécurité et la confidentialité. D'ailleurs, le fameux règlement communautaire dont on a déjà beaucoup parlé introduit la notification des failles de sécurité. Je travaille main dans la main avec le Responsable de la Sécurité des Systèmes d'Information parce qu'il est le premier à connaître ces éventuelles failles. C'est lui qui me dira si le *hacker* a pu avoir accès aux données personnelles des salariés. De même, j'informe de mes missions. Très longtemps, les IRP se sont demandé pourquoi nous ne faisions plus de déclaration à la CNIL. Je suis donc venue au comité d'entreprise parler de ma fonction. J'ai expliqué que je travaillais étroitement avec la CNIL, que je veillais à la protection des données personnelles et qu'elles ne soient pas conservées indéfiniment.

Ainsi, si l'on fait par exemple une enquête de satisfaction, je m'assure que les données collectées à cette occasion sont détruites dès qu'elle est terminée. Quand nous faisons appel à un sous-traitant, je lui fais signer à ce dernier un accord de confidentialité dans lequel il s'engage à détruire les données personnelles collectées une fois son enquête achevée et à restreindre l'accès à ces données aux besoins et personnes en charge de l'enquête.

Je veille aussi à faire respecter le droit des personnes. J'informe les salariés qu'on collecte leurs données en vue d'un traitement informatique, et leur indique l'usage qu'il en sera fait. De même, je veille au respect de leur droit d'accès, de leur droit à modification, voire à suppression, s'exerce. Un salarié qui a quitté le groupe Areva a le droit de vérifier que celles qui le concernent ont été supprimées. Je m'assure enfin que les données sont bien « adéquates », c'est-à-dire pertinentes et légitimes. Par exemple, l'article 9 du code civil accorde le droit à l'image à chaque individu. La photo est aussi une donnée personnelle et la loi « informatique et libertés » s'applique. Pour l'annuaire intranet d'Areva, les salariés se voient demander s'ils acceptent que leur photo y figure. Au moment de leur embauche, ils signent une autorisation, sur laquelle ils peuvent revenir quand ils le souhaitent.

Le règlement communautaire va consacrer le droit à l'oubli. Techniquement, il sera très difficile à mettre en œuvre mais il est indispensable.

M. Laurent Gouzènes, membre du conseil scientifique de l'OPECST. On n'a pas parlé des vols d'identité numérique. À l'occasion d'un mail censé être destiné à la banque, les données peuvent être détournées et les comptes vidés. Il est très difficile ensuite de prouver la fraude et d'être rétabli dans ses droits. De même, des usurpations complètes d'identité ont eu lieu sur Facebook, par duplication pure et simple de comptes, si bien que l'on ne peut plus

distinguer le vrai du faux. Si les deux fraudes se conjuguent, la situation devient très critique car, faute de preuve, vous n'avez plus de contact avec votre banque et votre vie professionnelle et privée risque d'être très perturbée. L'isolement peut être total.

M. Sophie Nerbonne. Vous avez raison de souligner ce risque, qui constitue, aux États-Unis, le principal problème. Se développe ainsi un marché autour des « nettoyeurs » du net qui veillent à l'« e-réputation » de leurs clients. La CNIL reçoit également des plaintes à ce sujet.

M. Jean-Yves Le Déaut, premier vice-président de l'Office. En préparant cette audition, je me suis immergé dans ce monde que je connaissais mal et j'ai détecté quelques anomalies qui mériteraient attention. J'ai ainsi vu la photo d'une conseillère municipale du Sud de la France, honorablement connue, utilisée pour illustrer des messages de nature très différente. Il y a aussi moyen, en jouant sur les liens, d'afficher des messages sur le mur Facebook d'un tiers.

M. Stéphane Grumbach. Ne faudrait-il pas envisager un service public de l'identité numérique ? Aujourd'hui, beaucoup utilisent leurs identifiants Facebook pour s'authentifier et accéder à de nombreux services, s'épargnant ainsi une gestion des mots de passe de plus en plus compliquée.

M. Jean-Yves Le Déaut, premier vice-président de l'Office. C'est une des suggestions sur laquelle nous allons travailler.

M. Gérard Berry. J'attire l'attention sur l'impossibilité concrète de mettre en œuvre le droit à l'oubli à cause des procédures de *back up* généralisées dans les entreprises. Y a-t-il une législation sur ce point ? N'oubliez pas que les informations ne se contentent pas de circuler : elles sont aussi reproduites en maints exemplaires.

Mme Chloé Torrès. Le droit à l'oubli, c'est-à-dire la possibilité de disparaître des réseaux sociaux, est technologiquement neutre : il vaut quel que soit le nombre de duplications. Il existe pour chaque donnée une durée de conservation légale qui varie selon sa nature. Lorsqu'un salarié quitte l'entreprise, elle doit archiver les données qui le concernent aussi longtemps que le prévoit la prescription légale. Au-delà, il doit y avoir destruction. Il y a là, à mes yeux, un vrai chantier à ouvrir, car cela implique de mettre en œuvre un plan d'action sur plusieurs années. Adopter en amont une approche *privacy based design* pour les nouvelles applications permettra de se mettre en conformité à l'avenir. Pour le stock, c'est une autre affaire.

M. Gérard Berry. On risque de se trouver dans la même situation que pour le droit maritime : il existe mais il n'y a personne pour le faire appliquer.

M. Serge Abiteboul. Tout est une question de coût. Si la traçabilité a été prise en compte dès le départ, il y a moyen de détruire l'information, mais il faut avoir gardé les pointeurs dessus. Techniquement, c'est lourd mais possible. Et cher.

Par ailleurs, il peut y avoir conflit entre les règles, par exemple entre la durée légale et l'exigence de destruction du propriétaire des données.

Mme Chloé Torrès. Pour demander et obtenir la destruction de ses données, il faut justifier d'un motif légitime. Les exigences d'un salarié ne sont pas sans limite. En revanche, il peut y avoir un conflit de lois quand des bases centralisées sont soumises à plusieurs

législations nationales. Les groupes internationaux doivent veiller à adopter une politique de durée de conservation des données harmonisée, qui ne soit pas trop coûteuse. Plus le problème est pris en amont des projets, mieux c'est.

M. Jean-Yves Le Déaut, premier vice-président de l'Office. Vous paraît-il possible que les données soient stockées sur la toile pendant un temps limité ?

M. Olivier de la Boulaye. Certainement, puisqu'il existe des logiciels pour cela. D'ailleurs, des sociétés commencent à proposer des services sur mobile qui utilisent des données éphémères. L'enjeu est le coût et la finalité de la requête.

M. Laurent Gouzènes. Ne sous-estimez pas non plus l'impact économique de ces réseaux américains qui vantent et commercialisent des produits américains réglés grâce à PayPal, une banque américaine, et livrés par une messagerie américaine. Ce sont autant de richesses qui disparaissent chez nous. On peut voir dans ce système une sorte de taxe Internet, qui coûte à la France quelques dizaines de milliards par an, et se mesure aussi en dizaines de milliers d'emplois perdus. Ces réseaux constituent aussi une arme économique au service de leur pays.

Enfin, j'avais été stupéfait de voir qu'après les attentats du World Trade Center, tout Internet s'était arrêté : plus rien ne marchait. Une telle panne est-elle encore possible aujourd'hui ? Les DNS – les systèmes de noms de domaine – étant pilotés par les Américains, nous ne maîtrisons rien et l'Europe peut se retrouver entièrement paralysée parce qu'un avion a été précipité sur une tour en Amérique.

M. Jean-Yves Le Déaut, premier vice-président de l'Office. On a posé le problème ce matin dans le domaine militaire et évoqué la gouvernance mondiale d'Internet.

M. Laurent Gouzènes. Même si elle ne saute pas aux yeux, la vulnérabilité de notre économie est bien réelle.

Mme Hélène Legras. Dans ce cas précis, le réseau a peut-être été victime de sa sur-fréquentation. Quand l'information de l'attaque des tours jumelles a été diffusée, les gens se sont tous connectés à Internet pour voir en direct ce qui se passait. Et le réseau s'est effondré.

M. Michel Cosnard, président-directeur général de l'Inria. C'est une lourde charge que de proposer une synthèse de quatre tables rondes qui ont rassemblé vingt-cinq orateurs et suscité de multiples questions. Je remercie ceux qui ont contribué à la richesse des débats, et souhaite que cette réunion en appelle d'autres du même type.

La première table ronde de la matinée, consacrée à la place du numérique dans la gestion de la menace stratégique, a proposé un état des lieux en matière de cybersécurité. Dans ce domaine, le nombre d'attaques augmente de manière exponentielle. M. Chauve a montré la gradation d'une menace, qui va de la simple revendication ou de l'affichage de messages sur des sites officiels, par le biais du hacking, jusqu'au cyberespionnage, voire au cybersabotage. Les attaques sont imputables à des empilements chancelants de technologies. La maîtrise technologique doit pouvoir s'appuyer sur la confiance pour qu'on puisse construire une politique industrielle.

M. Grumbach nous a alertés sur le fait que les questions de souveraineté s'étendent au domaine des données, notamment personnelles. Il juge important que la France et l'Europe

disposent d'une stratégie de récolte et de stockage, afin d'exploiter et de transformer ces données.

M. Pailloux a expliqué la stratégie de réponse élaborée par l'ANSSI. Elle se développe selon trois axes : conserver la capacité de protéger les informations essentielles, renforcer la sécurité des informations globales, promouvoir la sécurité dans le cyberespace. Selon lui, il existe une « hygiène informatique » que chacun doit respecter.

M. Bockel a présenté les grandes lignes de son rapport d'information sur la cyberdéfense, domaine où des progrès importants ont été accomplis. S'il faut donner la priorité à ce secteur, on doit aussi renforcer la cybersécurité et définir une stratégie européenne. M. Bockel propose également de créer une cyberréserve citoyenne – pour mobiliser des citoyens sur le territoire national en cas d'attaque massive –, d'adapter la législation au problème de la cybercriminalité et de rendre obligatoire la déclaration d'incidents. La communauté nationale doit être sensibilisée à ces enjeux majeurs.

M. Rihan Cypel nous a informés que le Livre blanc sur la défense, en préparation, ferait de la cyberdéfense un sujet majeur de sécurité nationale, de protection des entreprises et de lutte contre la cyberescroquerie. Il a plaidé pour la création de filières universitaires, en rappelant que les risques pouvaient aussi être considérés comme des opportunités économiques.

M. Latty a détaillé les mesures prises par le ministère de la défense dans le cadre d'un schéma directeur de cyberdéfense et de cybersécurité.

Au cours de la deuxième table ronde, consacrée à la fiabilité et à la sécurité numérique des systèmes d'armes, M. Brugère a rappelé les étapes d'une conception sûre : établissement d'une chaîne de confiance ; maîtrise des technologies critiques ; développement d'expertises pointues liées à la sécurité des systèmes de défense et des infrastructures critiques ; mécanismes de surveillance et de détection ; partenariats de confiance.

M. Terrier a développé la notion de conception sûre. Tous les objets embarquant aujourd'hui de l'intelligence, ils doivent, pour communiquer, disposer d'une capacité d'adaptation et d'ouverture ; de ce fait, ils sont plus fragiles face aux attaques, et leur conception est plus délicate. Il a plaidé pour la mise en place d'une ingénierie système et logicielle à partir de briques fiables, dont les capacités ont été démontrées formellement.

M. Ripoche a indiqué que les risques, qui dépassent le cadre des équipements, s'étendent aux composants logiciels et, par-là, aux armes de défense. Il a souligné l'importance de la dualité civil-défense pour coordonner les efforts de recherche. Il a aussi montré l'intérêt et la fragilité de l'interopérabilité des systèmes d'armes dans des alliances comme l'OTAN. Le risque est gérable, à condition d'y consacrer les moyens.

M. Moliner s'est intéressé à la sécurité des grands systèmes de communication, à l'heure où des milliards d'objets sont connectés à Internet et où explose le trafic de données. Disposer de réseaux fermés étant impensable, la confiance devient un enjeu essentiel.

M. Malis a rappelé le rôle majeur qu'ont joué les évolutions technologiques dans les grandes confrontations, des guerres napoléoniennes à la Seconde Guerre mondiale. La maîtrise industrielle et technique est indispensable. Il faut considérer que l'ennemi est

intelligent et s'intéresser à sa doctrine, impératif que l'on sous-estime parfois dans le domaine du numérique.

M. Mallet a rappelé le caractère exponentiel des cyberattaques et l'aggravation de la menace, bien que des stratégies de défense soient en cours d'élaboration. L'échelle de la menace dépasse les limites habituelles de la guerre ou de la dissuasion. La capacité de certains États à prendre le contrôle d'infrastructures ou d'entreprises ouvre des espaces insoupçonnés. Des groupes non étatiques peuvent développer des stratégies pour utiliser ces failles et ces espaces, afin de mener des guerres asymétriques. Le monde numérisé offre cependant des outils pour résister. Même si nous sommes toujours à la merci d'un Pearl Harbor numérique, nous devons collectivement construire notre capacité de défense. M. Mallet a présenté l'organisation du ministère de la défense, depuis la chaîne de commandement opérationnel jusqu'aux investissements humains et techniques. Enfin, il a rappelé la dimension sociale et citoyenne du problème, en reprenant la proposition présentée par M. Bockel de créer une réserve citoyenne de cyberdéfense.

L'après-midi a été consacré aux moyens de prémunir la société contre le risque de dépendance numérique. Au cours de la première table ronde portant sur la sûreté numérique dans la gestion courante, M. Berry a rappelé l'origine et l'importance des bugs, en insistant sur la formation. Il juge préoccupant qu'on ne réserve pas au génie logiciel la même place qu'au génie mécanique.

M. Erman a montré que la protection des données allait devenir une préoccupation de sécurité nationale, ce qui est déjà le cas aux États-Unis.

M. de la Boulaye a traité de la sécurité des données dans le cadre de la domomédecine.

M. Dowek a présenté des cas de dysfonctionnement des systèmes informatiques.

Quant à M. Bolignano, il a évoqué les travaux conduits dans le cadre de la preuve de programme.

Au cours de la dernière table ronde, portant sur l'installation insidieuse d'une vulnérabilité numérique tous azimuts, M. Oullier a distingué la notion d'addiction et celle de dépendance, en rappelant qu'il n'y avait pas lieu d'assimiler certains nouveaux comportements à des problèmes cliniques.

M. Valleur a étendu la réflexion aux jeux sur Internet. L'éducation et la formation apportent des réponses dans ce domaine. Le développement de la qualité des jeux en réseau est la meilleure prévention de l'addiction. On parle parfois de « *serious games* ». Peut-être faut-il être plus sérieux pour jouer en réseau, sans perdre de vue la dimension ludique.

M. Grumbach, qui s'interroge sur les transformations durables de la société, a posé le problème de la protection de la vie privée, envisagé dans le cadre des réseaux sociaux par M. Abiteboul. Celui-ci identifie quatre leviers pour agir : la loi, les associations de consommateurs, l'éducation et la recherche.

Mme Nerbonne a montré que les internautes sont moins bien protégés que les citoyens. La loi relative à l'informatique et aux libertés étant devenue insuffisante, un règlement européen est en cours d'élaboration, car chacun doit pouvoir s'opposer ou consentir à l'utilisation de ses données personnelles.

Mme Torrès a expliqué qu'il existe un socle juridique protégeant ces données. Elle fait appel au législateur pour qu'il remplisse le vide juridique concernant leur propriété.

À partir de l'exemple d'Areva, Mme Legras a réfléchi sur la protection des données concernant les employés et sur le rôle joué par le correspondant « informatique et libertés ».

Un débat s'est élevé ensuite sur le vol de l'identité numérique, qui peut justifier la création d'un service public de l'identité numérique.

Un des maîtres mots de nos échanges a été l'éducation, qu'il s'agisse de se doter d'experts en matière de sûreté, de sécurité ou de fiabilité, ou tout simplement de comprendre le monde. L'OPECST a encore beaucoup de travail devant lui !

M. Jean-Yves Le Déaut, premier vice-président de l'Office. Au cours de cette journée, beaucoup de sujets ont été abordés. Le développement du numérique et les risques qu'il présente sont un sujet très vaste, dont ni l'État ni le Parlement ne doivent se désintéresser. Nous avons travaillé en amont de la législation et de la régulation, pointant la nécessité d'instaurer un contrôle, mais, pour avoir déjà travaillé ici sur la cybercriminalité en 2005, nous savons combien il est difficile de mettre en place des règles de droit dans un domaine international et dématérialisé. Des constantes apparaissent cependant au niveau national, notamment la nécessité de développer la formation et la recherche, en ménageant la dualité du civil et du militaire. C'est ce que fait Thales, sous l'égide de Prix Nobel de physique Albert Fert. Le soutien à la recherche, comme le rôle des associations et du citoyen, est un enjeu essentiel pour le législateur.

Je vous remercie.

La séance est levée à dix-huit heures.