N° 2541

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUATORZIÈME LÉGISLATURE

Enregistré à la présidence de l'Assemblée nationale

le 2 février 2015

N° 271

SÉNAT

SESSION ORDINAIRE 2014 - 2015

Enregistré à la présidence du Sénat

le 2 février 2015

RAPPORT

au nom de

L'OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES

sur

SÉCURITÉ NUMÉRIQUE ET RISQUES : ENJEUX ET CHANCES POUR LES ENTREPRISES

PAR

Mme Anne-Yvonne LE DAIN, députée, et M. Bruno SIDO, sénateur

Tome II : Auditions

Déposé sur le Bureau de l'Assemblée nationale

par M. Jean-Yves LE DÉAUT,

Président de l'Office

Déposé sur le Bureau du Sénat

par M. Bruno SIDO,

Premier vice-président de l'Office

SOMMAIRE

Pages

SOMMAIRE 3

COMMISSION DES AFFAIRES ÉTRANGÈRES, DE LA DÉFENSE ET DES FORCES ARMÉEES DU SÉNAT 9

CONSEIL DE L'EUROPE 15

M. ÉRIC SADIN, ÉCRIVAIN ET PHILOSOPHE, AUTEUR DE « *L'HUMANITÉ AUGMENTÉE : L'ADMINISTRATION NUMÉRIQUE DU MONDE* » 21

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL) 25

NOV'IT 39

CONSEIL DES INDUSTRIES DE CONFIANCE ET DE SÉCURITÉ (CICS) 47

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS (CLUSIF) 55

CLOUDWATT 61

CONSEIL NATIONAL DU NUMÉRIQUE (CNNUM) 69

FÉDÉRATION FRANÇAISE DES TÉLÉCOMS (FFT) 79

PRÉSIDENCE DE LA RÉPUBLIQUE 87

TOTAL 95

GENDARMERIE NATIONALE - DIVISION DE LUTTE CONTRE LA CYBERCRIMINALITÉ – SERVICE TECHNIQUE DE RECHERCHES JUDICIAIRES ET DE DOCUMENTATION 103

DIRECTION GÉNÉRALE DE L'ARMEMENT 111

DIRECTION DE LA PROTECTION ET DE LA SÉCURITÉ DE LA DÉFENSE (DPSD) 119

CLUB DES DIRECTEURS DE SÉCURITÉ DES ENTREPRISES (CDSE) 131

OPEN-ROOT 139

CONFÉRENCE DES DIRECTEURS DES ÉCOLES FRANÇAISES D'INGÉNIEURS (CDEFI) 145

ASIP SANTÉ 151

DIRECTION GÉNÉRALE DE LA COMPÉTITIVITÉ, DE L'INDUSTRIE ET DES SERVICES (DGCIS) 159

MEDEF 163

DÉLÉGATION INTERMINISTÉRIELLE À L'INTELLIGENCE ÉCONOMIQUE 171

ÉCOLE SUPÉRIEURE D'INFORMATIQUE ÉLECTRONIQUE AUTOMATIQUE (ESIEA) OUEST 181

COMPTE RENDU DE L'AUDITION PUBLIQUE DU 16 AVRIL 2014 : ÉDUCATION AU NUMÉRIQUE 189

MME MYRIAM QUÉMÉNER, MAGISTRAT, SPÉCIALISTE DES PROBLÈMES DE LA CYBERSÉCURITÉ 229

COMPTE RENDU DE L'AUDITION PUBLIQUE DU 19 JUIN 2014 : SÉCURITÉ DES RÉSEAUX NUMÉRIQUES 237

COMPTE RENDU DE L'AUDITION PUBLIQUE DU 26 JUIN 2014 : SÉCURITÉ NUMÉRIQUE DES OPÉRATEURS D'IMPORTANCE VITALE (OIV) 343

LISTE DES PERSONNES ENTENDUES PAR LES RAPPORTEURS 409

Remerciements

Les rapporteurs remercient vivement la centaine de personnes entendues au cours de leur étude :

- Les personnes entendues lors de la préparation de l'étude de faisabilité – dont les auditions ne sont pas retranscrites dans le présent tome –, à savoir successivement :
    - **Mme Chi Onwurah**, membre de la Chambre des communes, porte-parole du parti travailliste pour le commerce, l'innovation et la formation, en charge de la cybersécurité au sein du Cabinet fantôme ;
    - **M. Philippe Mirabaud**, lieutenant-colonel, chargé de mission cybersécurité et numérique au cabinet du directeur général de la Gendarmerie nationale ;
    - **M. Marc Mossé**, directeur des affaires publiques et juridiques, *Microsoft France* ;
    - **M. Stanislas Bosch-Chomont,** responsable des affaires publiques, *Microsoft France* ;
    - **M. Bernard Ourghanlian**, directeur technique et sécurité, *Microsoft France*, administrateur au *Syntec-numérique* ;
    - **M. Luc-François Salvador**, président directeur général de *Sogeti* ;
    - **M. Jean-Marie Simon**, directeur général d'*Atos France*, premier vice-président du *Syntec-numérique* ;
    - **M. Florent Skrabacz**, responsable des activités sécurité *Steria*, *Syntec-numérique* ;
    - **M. Gérard Berry**, membre de l'Académie des sciences, membre de l'Académie des technologies, professeur au Collège de France ;
    - **Mme Pascale Briand**, directrice générale de l'Agence nationale de la recherche (ANR) ;
    - **M. Jean-Yves Berthou**, docteur en informatique, responsable du département services et technologies de l'information et de la communication à l'Agence nationale de la recherche (ANR) ;
    - **M. Patrick Pailloux**, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ;
    - **M. Bruno Ménard**, vice-président du Club informatique des grandes entreprises françaises (CIGREF), qui a autorisé l'Office à

faire figurer en annexe du présent rapport le jeu sérieux sur la sécurité numérique destiné aux entreprises.

- les personnes dont l'audition figure dans le présent tome ;
- les personnes qui ont accueilli les rapporteurs lors de leurs entretiens :
  - ✓ à la Commission européenne, à Bruxelles :
    - **Mme Isabelle Pérignon**, conseillère au cabinet de Mme Vera Jourova, commissaire européenne à la justice, aux consommateurs et à l'égalité des genres ;
    - **M. Damien Levie,** chef d'unité « États-Unis, Canada » à la direction générale du commerce de la Commission européenne (DG TRADE), adjoint au négociateur en chef sur le traité de libre-échange UE/EU ;
    - **M. Marco Dueerkop**, chef d'unité à la direction B (Services et investissement, propriété intellectuelle et marchés publics) de cette direction générale ;
    - **M. Pascal Rogard**, conseiller « télécommunications, société de l'information » à la représentation permanente de la France auprès de l'Union européenne ;
    - **M. Jakub Boratynski,** chef d'unité « Confiance et Sécurité » à la direction générale « Réseaux de communication, contenu et technologies » (DG CNECT) de la Commission européenne
  - ✓ à Bruz au centre de la **Direction générale de l'armement (DGA-Maîtrise de l'information)**, à Nancy au **Laboratoire de haute sécurité (LORIA),** à Élancourt, chez ***Thales*****,** pour visiter son Centre opérationnel de cybersécurité, à Montigny-le-Bretonneux chez ***Bertin Technologies***.

Les rapporteurs expriment aussi leurs remerciements aux membres du conseil scientifique de l'OPECST qui ont bien voulu les conseiller, en particulier :

- **M. Michel Cosnard**, président de l'Institut national de recherche en informatique et en automatique (INRIA) ;
- **M. Daniel Kofman**, professeur à Telecom ParisTech, directeur du LINCS, qui a animé l'audition ouverte à la presse sur « *L'éducation au numérique* » du 16 avril 2014 ;
- **M. Gérard Roucairol**, président de l'Académie des technologies, membre du conseil scientifique de l'OPECST, qui a été entendu et a participé à l'audition ouverte à la presse sur « *L'éducation au numérique* » du 16 avril 2014 ;

et à :

- **M. Pierre Lasbordes**, ancien député, ancien membre de l'OPECST, pour son animation de l'audition publique ouverte à la presse sur la « *Sécurité des réseaux numériques : cadre juridique, risques, aspects sociétaux* » du 19 juin 2014.

Les rapporteurs tiennent à remercier particulièrement les représentants de la Direction de la protection et de la sécurité de la Défense (DPSD), ainsi que **les responsables de la société Intrinsec** qui ont organisé pour les membres de l'Office des séances de démonstration de prises de contrôle, rapides et indétectables, d'appareils numériques à distance.

Les rapporteurs adressent également leurs remerciements **aux personnes qui les ont conseillés** dans le choix d'un expert en sécurité informatique issu de l'INSA.

NB : Les soulignements et les caractères en gras sont le fait du secrétariat de l'Office ; les premiers marquent le début d'un développement relatif à un thème particulier tandis que les seconds mettent en valeur un propos particulièrement remarqué.

Les comptes rendus des interventions ont été validés par leurs auteurs.

COMMISSION DES AFFAIRES ÉTRANGÈRES, DE LA DÉFENSE ET DES FORCES ARMÉEES DU SÉNAT

M. Jean-Marie Bockel, sénateur, Rapport d'information n° 681 (2011-2012), fait au nom de la commission des affaires étrangères, de la défense et des forces armées du Sénat,
« *La cyberdéfense : un enjeu mondial, une priorité nationale* »

5 février 2014

Sans être un spécialiste du numérique, j'ai découvert le sujet au fur et à mesure des auditions menées pour l'élaboration du rapport sur la cybersécurité, notamment celles avec l'ANSSI, l'état-major, etc., et ai effectué un travail de néophyte destiné à nourrir le Livre blanc sur la défense qui était en cours de rédaction pour aboutir aux conclusions de ce rapport.

Ce rapport n'a pas porté seulement sur la dimension militaire mais sur des aspects divers qui relèvent de la souveraineté de l'État.

Les enjeux de cyberdéfense, de souveraineté nationale et le monde de l'entreprise sont arrivés à un tel degré d'espionnage, de cyberespionnage, et de cybermenaces potentielles en termes de saturation, de délits, de casse informatique, que **la sécurité économique est devenue un sujet politique et un enjeu national**. À partir du moment où le phénomène de cyberespionnage prend une telle ampleur, il devient un problème d'abord pour les entreprises concernées qui se font siphonner leur savoir, leur connaissance mais cela devient aussi un problème pour des filières économiques tout entières et pour le pays lui-même.

D'emblée, j'ai voulu **inclure la dimension économique dans le rapport sur la cyberdéfense**, sous deux angles : tout d'abord, la limitation des effets du cyberespionnage en termes de perte de richesse ; ensuite, l'élaboration de propositions sur le monde économique lorsqu'il est opérateur d'importance vitale. La notion d'opérateur d'importance vitale est limitée à quelques dizaines d'entreprises, mais demain, avec tous les réseaux d'entreprises existant autour de chaque opérateur d'importance vitale, ce chiffre sera largement dépassé. En effet, ce sont des mesures particulières qu'il convient de prendre qui vont au-delà de l'espionnage qui peuvent aussi concerner **le service public comme le secteur privé, l'un comme l'autre pouvant être paralysé par des cyberattaques**.

Ce n'est pas forcément une attaque étatique qu'il faut craindre, mais plutôt celles de criminels voire, dans certains cas, de concurrents potentiels

ou encore dans le cadre de conflits non explicites ou larvés. Par exemple, des puissances comme la Chine, qui pratique systématiquement l'espionnage industriel, pourraient, face à telle ou telle politique européenne occidentale se sentir agressées dans leurs intérêts et pourraient, en réponse, sans aller jusqu'au conflit, s'attaquer à un pan de souveraineté d'un pays, y compris à son économie ou à ses entreprises.

Dans le rapport sur la cybersécurité, sont cités les exemples de l'Iran et de l'Arabie Saoudite. L'attaque par le virus *Stuxnext* contre les centrifugeuses du complexe militaro-industriel iranien a cassé la constitution d'une force nucléaire ; de même, *Saudi Aramco* a eu 30 000 ordinateurs détruits.

L'enjeu stratégique et militaire s'entremêle avec l'enjeu économique, en l'occurrence l'exploitation du pétrole. Il peut y avoir de l'espionnage tout comme une situation conflictuelle. **Mais même en l'absence de guerre, une série de risques intermédiaires existe qui peut, à travers l'économie au sens large, perturber gravement la souveraineté d'un pays.** Par rapport à cette réalité, il doit exister une gradation dans la réponse.

Première réponse possible : ce qui est vrai pour le citoyen de base, à travers la perte de ses coordonnées bancaires ou autre, vaut pour l'entreprise, y compris pour la PME ; il faut désormais connaître ce que le directeur général de l'ANSSI appelle **l'hygiène de base numérique**. Ce que tout un chacun peut apprendre (codes, processus de sécurité en fonction de l'enjeu de sécurité…). **En suivant ces règles, les entreprises peuvent éviter 90 % des risques.** À l'inverse, aujourd'hui, comme cette démarche n'est pas suivie, tout peut arriver.

Deuxième réponse possible : <u>l'obligation de déclaration de tout incident.</u>

Dans le monde actuel, être attaqué est perçu comme un aveu de faiblesse ; surtout quand on travaille pour la défense et qu'on ne souhaite pas perdre de marchés. Dans l'exemple des attaques analysées dans le rapport sur la cyberdéfense, comme celle contre *Areva* ou contre le ministère de l'économie et des finances, il n'y a pas eu de casse ni d'atteinte à la sécurité nucléaire. Cependant, toute société complètement informatisée offre de nombreuses prises à la pénétration informatique, ce qui rend ses entreprises vulnérables. Même si *Areva*, comme toute grande entreprise internationale, n'a pas de systèmes ouverts, elle aurait cependant été espionnée de manière massive et systématique, ce qui l'a rendue vulnérable et beaucoup d'informations, de savoirs, de systèmes lui ont été subtilisés. Les conséquences exactes de l'attaque subie par *Areva* demeurent inconnues.

Quand la victime d'une attaque informatique la déclare à l'ANSSI, celle-ci s'adresse à son tour à des entreprises de type *Thales* ou autres pour venir au secours de l'entité attaquée. En effet, **malgré leur poids et leur**

intelligence, les grandes entreprises ne sont pas forcément capables de faire face à une attaque.

En cette matière, les États-Unis d'Amérique possèdent quelques années d'avance sur la France en raison de l'existence de dispositifs publics à la disposition des autorités politiques, militaires ou économiques.

Quant aux Allemands, ils ont mis en place des dispositifs assez pointus incluant une capacité liée à des moyens publics.

Le Livre blanc sur la défense et la sécurité civile porte également sur des sujets civils ; à cet égard, ce que fait la DGA, à Bruz, en matière de recherche et de développement est à la pointe de la technologie.

Des ingénieurs spécialisés de l'ANSSI sont également à la disposition du monde économique, des militaires, auprès de l'État-major.

Dans les trois années à venir, le suivi des engagements pris dans le Livre blanc et la loi de programmation militaire permettront probablement à la France d'atteindre le même niveau que les Britanniques ou les Allemands. Sur certains points, les Français sont même déjà meilleurs qu'eux, notamment pour aider les entreprises.

L'obligation de déclaration constitue une bonne manière de parvenir à changer les mentalités. Comme tout le monde est attaqué tout le temps, et prioritairement ceux qui ont de la valeur, donc être attaqué prouve sa valeur et dire que l'on a été attaqué témoigne de la confiance en sa force même s'il ne s'agit pas de le clamer sur la place publique.

Enfin, il est nécessaire de **mettre en place un dispositif de résilience**, c'est-à-dire d'une capacité à répondre à une attaque de façon plus appropriée. Néanmoins, une protection absolue ne peut exister.

Le scandale Snowden a montré l'énormité des moyens américains, ce qui n'empêche pas la France de pouvoir protéger son économie au moins aussi bien que les États-Unis d'Amérique. Il ne s'agit que de quelques centaines de millions d'euros à y consacrer, pas de milliards. Cet effort mérite d'être accompli.

Demain, il faudra construire l'Europe de la cybersécurité. Ce qui sera complexe car tout dispositif de protection dépend de la solidité de son maillon faible ; il en va de même pour les dispositifs de cyberdéfense de l'OTAN. En matière de cybersécurité, on aime fonctionner en bilatéral parce qu'on sait avec qui on échange, ce qu'on échange et à quel prix.

La norme et la politique industrielle viendront de l'Union européenne.

L'Estonie est passée du jour au lendemain de la paperasserie à la dématérialisation ; les Néerlandais se réveillent, les Suisses commencent à réfléchir. Beaucoup de pays ne sont pas au niveau. Au Sénat, un **projet de résolution européenne** a été élaboré sur cette question.

Enfin, troisième point, au niveau mondial d'énormes efforts sont nécessaires pour l'établissement de règles dans le domaine économique, ce qu'illustre bien l'affaire Snowden. S'il y a une règle du jeu, à travers, par exemple, une **convention onusienne**, cela peut intéresser même les Chinois. Ceux qui ne respecteront pas cette norme seront connus de tous. Ainsi, seul un intérêt supérieur pourrait conduire certains à transgresser la règle.

Au niveau européen, il est nécessaire de **travailler ensemble à un certain nombre de normes et également de développer une dimension industrielle**.

La cybersécurité recèle un potentiel de développement économique considérable, que ce soit au niveau des équipements, des systèmes, etc., avec *Bull* qui exporte des systèmes complets de sécurité, *Thales, Cassidian, Sogeti,* ou *Alcatel* et tout un réseau de PME en France et dans l'ensemble de l'Union européenne. Ce potentiel est à développer en souveraineté nationale ou au niveau mondial.

Le Gouvernement vient de mettre en place **trente-quatre filières industrielles** et une des mesures envisagées a pour référent M. Patrick Pailloux, directeur général de l'ANSSI, et porte sur le **développement des industries de la cybersécurité** – ce qui était une des propositions de mon rapport.

Les industriels se sont regroupés autour de M. Hervé Guillou, président du Conseil des industries de confiance et de sécurité (CICS), pour créer un groupe de pression afin de suivre ce plan. **Un groupe informel de parlementaires** s'est d'ailleurs également constitué, auquel j'appartiens, pour voir comment accompagner les industriels dans leur démarche porteuse de force en matière de sécurité et également riche d'autres potentiels.

Derrière cela se dessinent aussi **les emplois de demain**. **Pendant deux ans, cela va être la guerre pour débaucher les meilleurs spécialistes de la sécurité informatique.** Des départements dans les **écoles d'ingénieurs**, les **universités**, pourront se tourner vers ces formations indispensables.

Parmi ces spécialistes, il existe des *hackers* patriotes à la française qui sont passés par certains moules notamment en matière de comportement mais ce type de profil reste marginal.

La loi de programmation militaire précise que les opérateurs d'importance vitale, au nombre de 200-250, des administrations, des entreprises, seront tenus de déclarer leurs incidents ; de même, des investigations pourront être menées au niveau de l'ANSSI.

Les conséquences les plus graves des attaques contre les opérateurs d'importance vitale résultent de l'espionnage. Lorsque le ministère de l'économie des finances a été attaqué à la veille d'un sommet entre chefs

d'État, il avait été jugé que cela n'était pas un sujet marginal même si aucun chiffrage n'avait pu être donné en termes d'impact.

Les Chinois ont des bataillons entiers de *hackers* qui sont des militaires. Quand on voit comment les Chinois avancent à pas de géant dans le domaine aéronautique ou spatial, cela permet de déduire qu'ils ont forcément pris des éléments ailleurs.

J'ai relevé, lors d'un dialogue avec notamment la société *Huawei*, que les routeurs au cœur des réseaux par lequel passent toutes les communications sont des **chevaux de Troie idéaux**. Jusqu'à présent l'ANSSI n'a pas référencé les routeurs de cœur de réseau de la société *Huawei*.

La prudence s'impose donc à tous les niveaux, notamment à ceux des équipements sensibles. En matière de cryptologie, la France est à la pointe.

CONSEIL DE L'EUROPE

Mme Sophie Kwasny, chef de l'unité de protection des données personnelles

5 février 2014

Plusieurs travaux du Conseil de l'Europe sont pertinents en matière de numérique même s'il ne s'agit pas véritablement de risque numérique mais du cadre législatif relatif aux droits de l'homme qui permet d'incriminer des atteintes touchant au numérique.

Il s'agit davantage de cerner le cadre juridique qui permet de protéger les personnes, d'abord grâce à la protection des données personnelles à travers des actions du Conseil de l'Europe concernant le monde entier : la **Convention sur la cybercriminalité** et la **Convention sur la protection des données**, qui a déjà trente-trois ans. Les rédacteurs de ce texte avaient bien saisi la vocation universelle de la matière et permis à des États d'adhérer à cette convention qui est, à l'heure actuelle, ratifiée par quarante-six États dont quarante-cinq sont des États européens étant précisé que, pour le Conseil de l'Europe, l'Europe s'étend jusqu'à la Russie, à la Turquie ou, selon la formule, « *de l'Atlantique à l'Oural* », le quarante-sixième État signataire étant l'Uruguay. Parmi les quarante-sept États membres du Conseil de l'Europe, seules la Turquie et Saint-Marin ne l'ont pas ratifiée.

Depuis l'affaire Snowden, au-delà des aspects économiques à ne pas négliger, se pose un grave problème de surveillance de masse. Plusieurs États, dont des États européens, ont appelé, dans le cadre des Nations unies, à l'élaboration d'un traité international protégeant le droit au respect de la vie privée. En plus du droit à la liberté d'expression, du droit à la liberté de réunion, d'association, du droit à la vie privée, **le droit à la protection des données est un pilier des démocraties**.

Face à cet appel aux Nations unies pour légiférer, le Conseil de l'Europe estime avec pragmatisme que, en termes de délais, il serait plus rapide de ratifier la Convention sur la protection des données, unique outil existant ouvert à la signature de tous les États du monde. La France, qui est partie à la convention, ne devrait pas manquer de se faire l'écho des bénéfices de cette convention.

Les Nations unies, pour l'instant, se bornent à considérer le respect de la vie privée alors que la convention accorde un droit à la protection des données comme étant un droit permettant l'exercice de plusieurs droits de l'homme et libertés fondamentales : du respect de la vie privée, certes, mais

également de la liberté d'expression et de la liberté d'association. **Traditionnellement, protection des données et libertés d'expression et d'association sont perçues comme étant en contradiction ; il y a toujours un équilibre à trouver, ce qui n'est pas facile.** Avec les questions de surveillance de masse, on voit plusieurs acteurs américains, notamment M. Edward Snowden, exprimer une attente plus forte à l'égard du droit à la liberté d'expression également. Il s'agit donc de protéger les données personnelles, la vie privée et d'autres droits fondamentaux.

Depuis le traité de Lisbonne, **l'Union européenne a compétence exclusive en matière de protection des données** mais tout ce qui était anciennement du troisième pilier, à savoir la police et la coopération judiciaire, est du domaine de la compétence partagée.

La protection des données dans la convention du Conseil de l'Europe est une matière qui s'applique de manière complétement horizontale incluant le commerce, le marché intérieur et la police exercée par les autorités publiques.

Il y a trente-trois ans, la convention était le premier instrument juridique au niveau européen. En 1995, l'Union européenne a adopté une directive qui est toujours en vigueur. En janvier 2012, la Commission européenne a élaboré une proposition de règlement et une autre de directive. Alors que le règlement concerne, de matière générale, les données et le secteur privé, le projet de directive traite de la police et de la coopération judiciaire.

Les vingt-huit États de l'Union européenne sont parties à la convention et veillent à ce que la convention n'entre pas en contradiction avec ce qui se construit à Bruxelles.

La convention comprend une vingtaine d'articles, les articles principaux traitant de la protection des données *stricto sensu* étant les articles 5 à 12. Ce texte général se concilie très bien avec ce que fait l'Union européenne en la matière d'autant qu'elle se sert de cette convention comme d'un instrument à l'égard des États tiers. **Au niveau des vingt-huit États signataires, l'Union européenne est allée beaucoup plus loin que la convention** qui a pour ambition d'uniformiser à un certain niveau et permettait à terme aux États tiers de légiférer sur la base des droits de l'homme.

Le règlement européen en préparation s'appliquera directement aux États. Le Parlement européen doit adopter son rapport sur ce projet de règlement à l'occasion de la session plénière de mars 2014, juste avant les élections européennes.

Pour l'instant, cela bloque au niveau du Conseil de l'Union européenne car les États de l'Union ont déjà adopté le principe d'un report, ce qui pose un problème de calendrier puisque la nouvelle législation ne pourra être en place avant la fin de l'année 2014.

Quand le règlement sera adopté, son application directe en droit national interviendra au bout de deux ans. Le cadre de l'Union est très fort pour ses États membres et leur permet aussi de peser fortement dans le cadre du dialogue transatlantique. Pour l'Union européenne, la convention constitue vraiment un outil pour négocier avec les États tiers.

Dans cette convention, un article sur la sécurité des données impose des obligations et il faudrait en tirer parti pour **mettre en place des notifications des violations de sécurité des données personnelles**.

Le projet de règlement prévoit des sanctions très lourdes en termes financiers, ce qui n'est pas le cas dans la convention. L'objectif de la convention est d'y faire adhérer le plus grand nombre possible d'États, à charge pour ceux-ci d'adopter des législations nationales conformes.

Avec l'adoption de ces nouveaux textes, la loi de 1978 sera remplacée par le règlement européen qui nécessitera des lois d'application.

La France suit l'élaboration de ces textes de très près. La CNIL agit au sein du groupe de l'article 29 qui réunit tous les équivalents de la CNIL dans les vingt-huit États européens. Même si ce groupe n'a pas de pouvoir décisionnel, il suit de très près cette négociation.

La CNIL s'efforce de faire en sorte que le justiciable puisse s'adresser à l'autorité de contrôle de son pays ; des négociations sont en cours sur ce point.

C'est la commissaire européenne, Mme Neelie Kroes, néerlandaise, qui est en charge de tous les volets Internet et Mme Viviane Reding, luxembourgeoise, est la commissaire justice.

Lorsque le Parlement aura adopté son rapport et que le Conseil de l'Union, c'est-à-dire les gouvernements des États membres, aura adopté sa proposition, le trilogue entre la Commission européenne, le Parlement et le Conseil pourra commencer.

Le règlement, qui émane de la commissaire Viviane Reding, a été adopté par la commission dans son ensemble. Il est maintenant débattu par les gouvernements ; pour le moment, en mars 2014, la négociation est en cours au Parlement.

En janvier 2012, la Commission européenne a mis sur la table cette proposition et, depuis, le Parlement européen et le Conseil travaillent sur ce projet. Le Conseil souhaite maintenant que le délai soit reporté.

Déjà, **la France va beaucoup plus loin que la Convention car elle met en œuvre, au niveau national, des mesures plus protectrices que celles prévues par la convention. D'ailleurs, les vingt-huit États européens vont aujourd'hui beaucoup plus loin dans leur droit national** dont la convention constitue la base, une sorte de socle minimal, même si ce n'est pas le langage utilisé en matière de droits de l'homme.

Aujourd'hui, les données ne sont plus franco-françaises ni situées exclusivement en France mais en Afrique ou ailleurs. Concrètement parlant, à partir du moment où quelque chose circule sur Internet, c'est très difficile de le localiser comme cela se constate avec le nuage numérique.

Les États-Unis d'Amérique n'ont pas l'intention d'adhérer à la convention et ils ne le pourraient d'ailleurs pas car, dans le système américain, il existe des distinctions très nettes entre secteur privé et secteur public. Dans le secteur privé ; certains secteurs comme celui de la santé sont très protégés alors que, pour *Facebook, Google*, le même type de réglementation n'existe pas. Après, c'est le quatrième amendement de la Constitution qui s'applique en matière de surveillance policière. Les États-Unis n'ont pas de loi générale sur ce thème même si le président Obama a présenté une proposition de *Bill of rights* sur ce thème ; pour l'heure, le Congrès ne l'a pas suivi. Pour le moment, quelles que soient les pressions, les États-Unis ne s'orientent pas vers ce genre de protectionnisme.

Les États-Unis ont protégé la santé, la finance, le crédit, par exemple. Certains États américains sont allés plus loin que d'autres dans la réglementation, les disparités existent donc à un niveau géographique.

Les contre-pouvoirs technologiques sont toujours plus forts que les textes juridiques. Tout est proportionnel à la cible, au danger ou autre. **Il est important de sensibiliser chacun à la nécessité de se doter d'outils adaptés réduisant les vulnérabilités actuelles.** Mais les sociétés qui sont des sociétés cibles, qui dépensent des millions pour la sécurité informatique, ne sont pas à l'abri d'attaques. Il y a une surenchère à la fois du côté des cybercriminels et de la sécurité à leur opposer.

Il y a aujourd'hui des logiciels qui permettent l'anonymisation sur Internet.

Un outil, qui s'appelle *Tor*, a permis de protéger des dissidents et des cyberdissidents dans des pays moins démocratiques que les nôtres. Le régime pouvait savoir que M. Untel s'était connecté à *Tor*, mais, ensuite, il ne pouvait tracer les connexions opérées.

Le Conseil de l'Europe est aussi assez actif en matière de gouvernance de l'Internet. Cela inclut les aspects politiques et également l'infrastructure, notamment la gestion par l'*ICANN*. C'est toujours à partir de la vision des droits de l'homme, de la démocratie que **le Conseil de l'Europe prône un Internet ouvert** et le principe de l'absence de préjudice (« *do no harm* ». Il faut que les États s'abstiennent d'actions de nature à créer un préjudice à la structure et au réseau Internet.

Actuellement, **l'*ICANN* est la manifestation d'une hégémonie américaine dans la gestion du réseau.** Toutefois, M. Fadi Chehade qui vient d'être nommé à la tête de l'*ICANN* souhaiterait changer cela ; des bureaux de l'*ICANN* s'ouvrent un peu partout dans le monde et une réflexion sur l'avenir de l'Internet est en cours.

L'*ICANN* sait qu'il y aura de plus en plus de demandes de révision du système si elle n'évolue pas d'elle-même.

Le Conseil de l'Europe tient à ce que l'Internet ouvert continue de bénéficier de façon égale à tout le monde, comme actuellement, conformément au principe de sa construction. Le Conseil est engagé dans les travaux de réflexion sur l'*ICANN* qui serait, une fois restructurée adéquatement, tout à fait à même de continuer à garantir cette neutralité.

En juin 2013, une déclaration du Comité des ministres du Conseil de l'Europe a souhaité que soient mis en place des **contrôles à l'exportation des technologies de surveillance**.

Le système d'attribution des noms de domaine fonctionne mais pose certains problèmes en matière de liberté d'expression. Le postulat de base est que l'*ICANN* fonctionne et que son système est suffisamment ouvert.

Le 10 mars 2014, à Paris, se tiendra le premier Forum français sur la gouvernance de l'Internet auquel participera le Conseil de l'Europe, notamment afin de contribuer à ces réflexions importantes et faire la promotion de nos savoirs en la matière.

M. ÉRIC SADIN, ÉCRIVAIN ET PHILOSOPHE, AUTEUR DE « *L'HUMANITÉ AUGMENTÉE : L'ADMINISTRATION NUMÉRIQUE DU MONDE* »

5 février 2014

Au cours de l'évolution du numérique, il s'est passé quelque chose de l'ordre de l'empirique : **des modèles se sont constitués sans qu'il y ait une conscience collective ou individuelle de l'évolution en cours**. Vers la fin des années 1990, le modèle de la gratuité généralisée sur Internet s'est accompagné de la connaissance continue des navigations et des internautes eux-mêmes.

Google a mis au point des algorithmes sophistiqués pour opérer des recherches par rapport aux infrastructures numériques, aux services offerts, aux usagers. Le modèle s'est constitué au fur et à mesure en fonction de la connaissance continue, évolutive, des comportements de navigation des internautes, de la connaissance des personnes elles-mêmes. En retour, il s'est passé la plus grande exploitation commerciale possible, ciblée, et qui a autorisé la revente des données collectées à des entreprises intéressées par ces informations.

En outre, la sophistication algorithmique, ainsi que l'arrivée des *smartphones* en 2007, ont amplifié ce mouvement de production continue et amplifiée de données qui a induit, grâce au stockage, la possibilité de connaître les comportements au moyen notamment d'un certain nombre de **lacunes dans les clauses de consentement**.

Le second point, c'est qu'il est apparu une **collusion entre le commercial et les instances étatiques**. Le commercial a induit des usages d'ordre sécuritaire. Ce qui s'est passé avec la *NSA* a des effets collatéraux sur tous les utilisateurs. *Facebook* a communiqué sur mandat quantité d'informations car il y avait des portes dérobées, des *back doors,* dans sa structure.

Il faut remarquer que **plus s'établissent des rapports tactiles, familiers, charnels avec des objets numériques, plus s'affirme une dimension non perceptible puisque les objets numériques recèlent des méthodes d'analyse, de traitement qui, sans être cachées, sont invisibles**.

Si **la numérisation massive semble irréversible**, il est probable et souhaitable qu'il y ait un avant et un après l'affaire Snowden car **un mouvement de conscience semble s'opérer** alors qu'une certaine ignorance entourait auparavant ces questions.

Ce mouvement technologique, extrêmement important, finit par infléchir le comportement des citoyens et des sociétés sans qu'il y ait eu acceptation par la délibération démocratique de certaines dimensions.

Jamais il n'y a eu de mouvement technologique aussi massif pouvant à ce point effriter, voire remettre en question, des acquis historiques, particulièrement la vie privée.

Ce n'est pas le cas de toutes les avancées technologiques : par exemple, l'aviation n'a pas remis en cause d'acquis démocratiques.

Actuellement débute l'ère des capteurs, des puces électroniques. De plus en plus, des capteurs placés sur le corps rapporteront des témoignages, actifs ou passifs, des comportements de chacun. Les capteurs situés dans l'environnement des individus vont témoigner en continu. **Il y aura de plus en plus une quantification des personnes** (niveau de vie, pouvoir d'achat, compétence professionnelle, accointances entre les individus, connaissance permanente de l'étudiant en ligne, etc.), ce qui va encore intensifier **la connaissance continue des comportements**.

Entendu par le comité éthique, économique et social européen à Bruxelles, qui informe la commission et le Parlement, j'ai été considéré quasiment comme un révolutionnaire alors que je soulignais simplement des évidences face au laisser-faire généralisé qui gagne la planète entière face au numérique et souhaitais simplement que soit imposé à tous les groupes de l'Internet de **proposer des clauses de consentements explicites**, de **permettre à chacun de supprimer les données le concernant à n'importe quel moment**, de **favoriser un droit à l'oubli**.

Des lois en la matière seraient souhaitables pour **encourager la conscience de l'utilisateur du numérique** ; les grands groupes devraient rendre possible la visibilité des choix opérés sur Internet ; **des chartes** globales ou au cas par cas devraient expliciter, selon des modalités extrêmement compréhensibles, ce que tel ou tel choix technique suppose. À l'inverse, aujourd'hui, comme celles de *Facebook*, les clauses des contrats sont illisibles. D'où l'acceptation générale des règles imposées.

Aujourd'hui, le cadre général indispensable à l'échelle européenne n'existe pas alors que **l'Union européenne devrait pouvoir donner un cadre aux nouvelles technologies** car, comme l'économie numérique est au cœur de la croissance américaine, aucun changement ne viendra des Américains. **Des exigences éthiques doivent être imaginées** pour que l'Union européenne puisse peser.

Des processus techniques extrêmement simples pourraient être mis en œuvre pour permettre l'application des lois dans l'Union européenne.

Face à tous ces mouvements rapides, le législateur est-il suffisamment au fait des évolutions technologiques du numérique ?

Dans cette société de transparence où tout le monde sait tout sur tout et sur chacun, **l'instauration de l'acceptation explicite sur Internet de ce qu'implique son utilisation est très importante**. **Une charte de l'utilisation du numérique est indispensable.**

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL)

M. Gwendal Le Grand, directeur des technologies et de l'innovation

12 février 2014

Depuis une dizaine d'années, le centre de gravité des intérêts de la CNIL s'est complètement déplacé et prend de plus en plus en compte la dimension économique des données à caractère personnel et les modifications profondes induites par l'informatisation de la société dans son ensemble. Ce que l'on voit aussi, à une échelle macroscopique, c'est **le passage d'une informatique de gestion des systèmes à une informatique de la donnée. Aujourd'hui, la valeur est dans la donnée** ; des géants de l'Internet traitent de la donnée. Beaucoup d'entreprises gèrent de la donnée, de l'information et vont en tirer de la valeur.

La quantité de données produite par l'humanité, depuis son origine jusqu'en 2003, c'est à peu près cinq téraoctets de données, soit cinq mille milliards d'octets et, en 2010, il suffisait de deux jours pour produire l'équivalent de cette information.

Cette tendance n'est pas près de s'arrêter ; aujourd'hui, on parle d'informatique, de numérique ambiant, d'Internet des objets ; des études de *Bi Intelligence* ou de l'IDATE prédisent que, en 2018, il devrait y avoir dix-huit milliards voire quatre-vingts milliards d'objets connectés, ces objets échangeant des données, produisant des données qui ensuite sont traitées par les systèmes.

La CNIL s'est adaptée à cette mutation profonde de la société et elle essaie d'anticiper au mieux les risques dans cet environnement. C'est d'autant plus important que les entreprises qui traitent les données à caractère personnel, traitent de manière indifférenciée les données industrielles, les données de leurs clients, des données de prospects, des données de salariés qui sont bien souvent des données à caractère personnel.

Les problématiques de sécurité des systèmes d'information, de protection des données industrielles des entreprises recoupent donc très largement les problématiques de protection des données à caractère personnel pour lesquelles la CNIL est compétente.

Trois points vont préciser l'action de la CNIL dans cet environnement : d'abord, les aspects stratégiques pour les entreprises et

l'ensemble des acteurs liés à la donnée. Quelle est la valeur de la donnée ? Quels sont les problèmes créés d'un point de vue informatique et libertés par les traitements de donnés utilisés aujourd'hui ?

Deuxièmement, la sécurité des systèmes d'information : dans la loi informatique et libertés, l'article 34 indique que, lorsqu'on traite des données de caractère personnel, on est tenu de garantir leur sécurité. Pour cela, la CNIL a produit un certain nombre d'outils pour aider les entreprises à sécuriser leur système de données.

Troisième aspect : comme la sécurité repose beaucoup sur l'humain, un accompagnement des entreprises a été mis en place. Plus largement, vis-à-vis du grand public, des actions sont menées autour de l'éducation numérique.

Sur le premier point, quant à l'aspect stratégique pour les entreprises et pour l'ensemble des acteurs du traitement de données à caractère personnel, les données personnelles sont devenues indispensables à l'économie moderne. On parle de pétrole du numérique, de puissance du futur… On invente de nouveaux termes pour qualifier les données à caractère personnel et montrer qu'elles ont de la valeur et qu'elles alimentent tous les services de la société de l'information.

L'action menée récemment par la CNIL vis-à-vis de *Google*, en partenariat avec ses homologues au niveau européen, a conduit à conclure que la politique de confidentialité de *Google* n'était pas conforme aux règles européennes ; l'information donnée aux personnes lors de l'utilisation de ces services était insuffisante, les utilisateurs ne disposant pas d'un contrôle suffisant sur les combinaisons des données ; enfin, *Google* ne précisait pas la durée de conservation, comme demandé dans la loi informatique et libertés.

C'est la raison pour laquelle, au début de l'année 2014, la formation restreinte de la CNIL a prononcé une sanction financière contre *Google* qui a interjeté appel de cette sanction. Non pas pour son côté financier mais pour l'obligation de publier cette sanction sur le site de *Google :* www.google.fr. Un référé suspension contre cette obligation a été rejeté par le Conseil d'État la semaine dernière et, cette semaine, samedi et dimanche derniers, sur le moteur de recherche, un avis indiquait que *Google* avait été condamné à publier le fait qu'il avait été sanctionné pendant quarante-huit heures.

Ce cas montre bien que, pour un grand nombre de sociétés, **les plates-formes sont en compétition pour collecter un maximum de données personnelles** et aussi pour capter les clients dans leur écosystème. Aujourd'hui, si vous achetez un *smartphone*, quel que soit son système d'exploitation, une des premières choses qui va vous être demandée sera de créer un compte qui incitera à pousser l'ensemble de vos données dans les services du *cloud computing*. Évidemment, il y a des fonctionnalités qui sont offertes pour passer d'un terminal un autre ou pour sauvegarder vos données, mais vous devenez souvent, aussi, captif de l'écosystème de cette

société-là. Par ailleurs, de plus en plus de données sont traitées en raison de la multiplication des capteurs et de plus en plus d'informations sont envoyées à cette société.

En parallèle, émerge un second marché de la donnée, celui de l'*open data*. En libérant les données de leur collecteur initial, on crée les conditions d'une nouvelle utilisation *via* de nouveaux services innovants. Dans l'*open data*, dans bien des cas, ce seront des données statistiques et non des données à caractère personnel.

Enfin, on voit l'explosion des objets connectés. La CNIL mène actuellement une étude sur la quantification de soi grâce à tous les objets utilisés dans la sphère « santé bien-être » : balances connectées, tensiomètres connectés, etc., pour comprendre à quels acteurs ces données peuvent être transmises. Tout cet écosystème a beaucoup de valeur.

Des études ont été publiées, dont une étude du *Boston Consulting Group*, qui évalue à 315 milliards de dollars, en 2012, la valeur économique de ces données qui, en 2020, devrait être de mille milliards de dollars, ce qui est une valeur considérable et un potentiel très important en matière d'innovation.

Les données qui circulent concernent aussi bien les entreprises ou leurs salariés que les personnes privées ; elles vont toutes circuler sur les mêmes canaux d'information. Évidemment, cela crée des risques puisqu'il est possible, dans certains cas, de capter ces données, de les analyser.

Ces risques ont été pris en compte depuis plusieurs années par la CNIL. En 2012, la CNIL a publié une recommandation à destination des entreprises qui envisagent de recourir au *cloud computing* pour leur expliquer la démarche à suivre. Dans les recommandations de la CNIL, le **risque d'accès d'autorités étrangères aux services d'informatique en nuage** avait bien été identifié. Autre exemple, il y a quelques années, la CNIL a été très active sur les affaires *PNR* et *Swift*. Quand le président de la CNIL de l'époque, M. Alex Türk, avait été auditionné par l'Office, il en avait beaucoup parlé et ce sont des sujets sur lesquels la CNIL a été très présente pour obtenir le maximum de garanties en faveur de la protection des données à caractère personnel.

Quant à l'accès par les autorités étrangères dans le cadre de l'affaire *Prism*, c'est un sujet que la CNIL avait beaucoup anticipé. Dès mars 2013, un cycle d'auditions, avec des conclusions en septembre 2013, avait été organisé, donc avant l'affaire *Prism*.

Cette affaire a montré qu'il y avait une **possibilité d'accès à tout type de données**. En effet, le *Patriot Act* concerne toute sorte de données. Les « *any tangible things* », selon les termes de la loi, peuvent être n'importe quel objet, des livres, des enregistrements, du papier, des documents, aussi bien des données personnelles que confidentielles, que des données liées à des activités commerciales. Il y a derrière cela des enjeux en termes de

protection des données et d'intelligence économique assez importants. De plus, les champs d'application du *Patriot Act* et de la loi *Foreign Intelligence Surveillance Act* (*FISA)* sont extrêmement larges puisque la compétence territoriale s'étend à toutes les personnes morales et physiques américaines mais également aux sociétés étrangères dès lors qu'elles ont un bureau, une boîte de dépôt ou une activité en rapport avec le territoire américain. Rien ne garantit qu'une société européenne installée aux États-Unis d'Amérique en soit exclue.

Les sociétés destinataires d'une demande des autorités américaines se fondant sur la législation *FISA* sont soumises à une obligation de discrétion très stricte qui leur interdit de communiquer sur ce sujet. Il est très difficile d'avoir de l'information sur l'étendue des accès qui sont réalisés.

Au-delà de ces questions, les sites des grandes sociétés de l'Internet publient des rapports de transparence, *transparency reports*, qui montrent comment ces sociétés répondent aux demandes des différentes autorités dont le nombre ne cesse de s'accroître.

La différence entre le taux de satisfaction des demandes émanant des États-Unis par rapport au taux de satisfaction des demandes provenant d'autorités européennes comme la France est significative. Pour les autorités américaines, cela approche 100 % de réponses, de 90 % à 100 %, mais cela n'est plus que de 50 % pour les autorités françaises.

L'affaire *Prism* est une opportunité aussi bien du point de vue de la protection des données à caractère personnel que pour les entreprises françaises du secteur de la sécurité et du *cloud computing*, par exemple. Une étude de *l'Information Technology and Innovation Foundation (ITIF)* a montré que l'affaire *Prism* pourrait coûter plus de 30 milliards de dollars aux entreprises américaines dans les trois années qui viennent du fait d'une crise de confiance entraînant une perte de parts de marché pour ces sociétés de *cloud computing*.

Une autre étude du *Cloud Security Alliance* de 2013, indiquait que 10 % des sociétés interrogées déclaraient avoir annulé des projets de *cloud computing* après l'affaire *Prism*. Cela traduit une crise de confiance face à certains acteurs américains de ce secteur. Vu avec un regard européen, cela peut constituer **des opportunités pour les entreprises françaises qui offrent des services numériques dans les nuages plus transparents, conformes à la législation communautaire relative à la protection des données personnelles**. Un certain nombre d'acteurs, comme *OVH* ou *Cloudwatt*, faisaient déjà de la localisation des serveurs sur le territoire français un argument commercial sur le plan des données personnelles comme pour certains aspects de la sécurité des systèmes d'information.

La CNIL a toujours été très attentive aux questions de sécurité des systèmes d'information car c'est une mission qui lui est conférée par la loi informatique et libertés. L'article 34 de cette loi dispose que **les entreprises,**

en tant que responsables de traitement des données, doivent garantir la sécurité des données qu'elles traitent ; c'est le manquement à cette obligation qui est le plus fréquemment retenu par la CNIL avec 18 % du total des manquements retenus en 2012.

L'obligation de sécurité, l'incitation à la mise en place de **bonnes pratiques de sécurité** n'est pas uniquement du domaine de compétence de la CNIL puisque l'ANSSI a été très active dans ce domaine-là et que l'Office est très attentif aux travaux de l'ANSSI, qui partage avec la CNIL des préoccupations communes dans le domaine de la sécurité.

Les règles d'hygiène numérique de l'ANSSI sont partagées par la CNIL qui a développé ses propres outils en matière de sécurité informatique. En 2010, la CNIL a publié un guide à destination des PME qui donne des conseils basiques dans le domaine de la sécurité, indique des précautions minimales. En 2012, la CNIL a publié un guide avancé de gestion des risques s'appuyant sur la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité), qui est une méthode de l'ANSSI reconnue en matière de sécurité que la CNIL a adaptée à la protection des données à caractère personnel.

Les actions de la CNIL et de l'ANSSI sont complémentaires. En général, en matière de sécurité des systèmes d'information, **on s'intéresse aux risques pour l'entreprise, alors qu'en matière de protection des données, on s'intéresse aux risques pour les personnes**. Les mesures techniques à mettre en place dans chacun de ces cas sont souvent similaires. Par exemple, le chiffrement des données garantit la confidentialité des échanges, ce qui protégera la personne mais aussi l'entreprise.

La CNIL a réalisé un guide de gestion des risques en deux parties traitant des données des entreprises et des données à caractère personnel et proposant un catalogue de mesures à mettre en place. Un responsable de sécurité aujourd'hui va savoir appliquer les deux méthodes de protection tout à fait correctement. Dans les algorithmes de chiffrement, il y a des renvois au référentiel général de sécurité (RGS) publié par l'ANSSI pour qu'il y ait une cohérence entre les instruments recommandés.

À propos des relations entre la CNIL et l'ANSSI, il existe des situations de travail en commun et d'autres où la CNIL a sollicité les conseils de l'ANSSI et inversement. Celle-ci a audité les systèmes de la Fédération nationale de la mutualité française et d'*AXA* pour la qualité de l'anonymisation des feuilles de soins électroniques. La CNIL a participé à des formations dispensées à l'ANSSI. La CNIL effectue des sensibilisations et des formations dans le cadre de la loi informatique et libertés et il y a des personnels actifs à la CNIL qui sont des anciens employés de l'ANSSI. Il existe des comités de pilotage, par exemple sur l'identifiant national de santé, où les deux instances sont représentées. Il y a quelques années, le Livre blanc, intitulé « *Le guide pratique du chef d'entreprise face au risque numérique* », a été élaboré en commun avec la participation de la CNIL et de

l'ANSSI. La CNIL participe à la commission de normalisation de la sécurité des systèmes d'information à l'AFNOR. Enfin, l'ANSSI a mis en place récemment un groupe de travail sur la qualification de sécurité des systèmes de *cloud computing* et la CNIL y participe.

Au-delà de l'obligation de sécurité de l'article 34, une nouvelle obligation figure dans la loi depuis 2011, avec la transposition du paquet télécoms, à savoir la notification des failles de sécurité qui s'applique aux opérateurs qui doivent, quand ils subissent une violation de données à caractère personnel, la notifier à l'autorité compétente, à savoir la CNIL. Quand la violation est suffisamment sensible et susceptible de porter atteinte aux données de la vie privée des personnes concernées, il faut également informer ces personnes.

La transposition dans la loi informatique et libertés du règlement européen n° 611/2013, adopté le 24 juin 2013 et entré en application le 25 août, précise les modalités décrites dans la directive et demande notamment que les délais de notifications aux autorités d'une faille de sécurité soient de vingt-quatre heures et de soixante-douze heures pour compléter cette notification, le contenu de la notification est détaillé dans le règlement.

Le 3 février 2014, une réunion de l'ensemble des opérateurs a eu lieu à la CNIL pour leur rappeler l'ensemble de leurs obligations ; les délais de notification des failles n'étaient, pour ainsi dire, jamais respectés. Un communiqué de presse sur le site de la CNIL rappelle les obligations des opérateurs. La CNIL a d'ailleurs mis en place une procédure sur son site pour que les opérateurs puissent notifier électroniquement les violations à la CNIL et pour leur permettre d'évaluer le niveau de gravité de la violation qu'ils subissent.

Le troisième point, c'est le volet accompagnement et éducation au numérique, en plus du volet technique. La sécurité c'est aussi une affaire liée aux pratiques des personnes. La CNIL conduit des actions d'accompagnement des entreprises et d'autres à destination du grand public.

Pour les entreprises, la CNIL se réorganise actuellement pour répondre au mieux aux besoins de ses clients, de ses usagers, des entreprises en contact direct avec la CNIL, pour mettre en place une vision centrée sur la personne afin de mieux appréhender les besoins en matière de sécurité.

Par exemple, les recommandations sur le *cloud computing* ont été précédées d'une consultation de l'ensemble des acteurs ; l'avis des entreprises offrant des services de stockage en nuage et celui des PME souhaitant les utiliser ont été recueillis ; un jeu de recommandations a été produit incluant des clauses contractuelles qui peuvent être reprises dans les contrats à venir.

Faut-il rappeler que le *cloud computing* peut se définir comme l'informatique en nuage où la ressource informatique est externalisée auprès d'un prestataire qui s'en charge et fournit des ressources de calcul ou

d'infrastructures loin des locaux de l'entreprise. L'avantage réside dans la flexibilité offerte par le service ainsi que dans le fait que la prestation informatique puisse généralement être payée à la demande, au service.

Le problème dans les services de *cloud computing* est qu'il y a souvent peu **de garanties sur la localisation des données. Il s'agit-là d'une préoccupation majeure des entreprises, surtout depuis l'affaire *Prism*.** Certains acteurs comme *OVH* ou *Cloudwatt*, acteurs français, essaient de mettre en avant un certain nombre de garanties dont la localisation des données.

Les conseils de la CNIL aux entreprises consistent à leur donner des clés pour leur permettre de mieux choisir une offre de nuage numérique, intégrer la protection des données à caractère personnel et éviter la fragilisation du patrimoine informationnel des entreprises.

La CNIL explique que ce nuage numérique peut être utilisé pour certaines données mais pas pour toutes. Il faut bien cerner les exigences techniques et juridiques pour choisir une offre car **la plupart des offres d'informatique en nuage sont des offres de contrat d'adhésion qu'il sera impossible de négocier**, notamment pour les PME. À l'inverse, les services pour les grosses entreprises pourront être négociés ligne par ligne mais seront plus chers.

L'hébergement des applications « métier » de votre messagerie peut être géré dans l'entreprise ou par un prestataire informatique.

Le stockeur de données assure des systèmes de sauvegarde et stocke sur plusieurs sites, ce qui garantira une sauvegarde sur ces autres sites.

Il existe différents types d'informatique en nuage : le *SaaS* (*Software as a Service*), pour le logiciel, le *PaaS* (*Platform as a Service*), pour la plate-forme de développement, ou l'*IaaS* (*Infrastructure as a Service*), pour l'infrastructure.

Autre exemple d'accompagnement des entreprises par la CNIL, il s'agit des **pactes de conformité**. Des instruments sont mis à la disposition des entreprises d'un secteur particulier pour leur permettre de se mettre en conformité avec la loi informatique et libertés. La protection de la vie privée est alors intégrée dès la conception des produits.

Dans ce cadre, la CNIL a développé un partenariat avec la Fédération des industries électriques, électroniques et de communication (FIEEC) – mille milliards d'euros de chiffre d'affaires cumulé – qui a beaucoup travaillé sur la problématique des compteurs intelligents, les objets connectés et les services situés en aval du compteur. Un groupe de travail CNIL-FIEEC a été mis en place pour intégrer dans les nouveaux services innovants la problématique informatique et libertés. La CNIL permet un saut de confiance pour les industriels et les usagers. **Les produits qui respectent**

les exigences de la loi informatique et libertés jouissent d'une meilleure image auprès de leurs acquéreurs potentiels.

C'est la même démarche qui a conduit la CNIL à participer au Comité de la filière industrielle de sécurité, le CoFIS.

Par rapport à l'éducation du grand public au numérique, la CNIL a pris l'initiative de constituer un collectif pour l'information numérique du grand public, candidat à la grande cause nationale 2004, rassemblant une cinquantaine d'organisations qui considèrent unanimement qu'il y a urgence à diffuser la culture du numérique, à former les différents publics, à tous les âges de la vie, pour **permettre à chaque individu d'être un acteur du numérique informé et responsable et d'exercer de manière effective ses droits et devoirs dans ce domaine**.

Si cette offre d'éducation numérique était retenue comme une grande cause nationale, cela permettrait d'avoir un accès privilégié aux médias afin de toucher un très large public.

Cette modalité d'action a été choisie pour changer d'échelle dans les actions pédagogiques à mener. Ces nouvelles actions permettront de donner une réelle visibilité nationale à un sujet absolument crucial qui est en train de transformer la société de manière très profonde.

À propos de la confiance à accorder aux services de *cloud computing*, le stockage peut être distribué dans des infrastructures du réseau informatique avec une partie des informations vous concernant se trouvant sur un serveur ou un autre en fonction des ressources louées par le fournisseur de services de nuage. Les données peuvent migrer d'un serveur à un autre au cours de la journée ; cela est techniquement possible et dépend de la disponibilité des réseaux et de la manière dont ils sont organisés. C'est totalement invisible pour l'utilisateur.

Vous consommez un service et ne savez pas où sont stockées vos données.

Les services sont offerts à une multitude de sociétés et l'allocation de ressources est dynamique. Par exemple, pour prendre une image dans le monde électrique, une centrale nucléaire va produire beaucoup d'électricité à un moment et il y aura des pics de production et de consommation et, dans le réseau, ce sera la même chose. De même pour le stockage en nuage, davantage de ressources seront consommées selon les heures. Beaucoup de sociétés offrent des services au niveau mondial et les ressources seront allouées de manière dynamique en fonction des besoins.

Il existe différents types de services de *cloud computing*. De grosses sociétés d'Internet répartissent leurs services partout sur la planète et pourront allouer des ressources à d'autres sociétés qui offrent des services d'hébergement en fonction de leurs propres besoins. À l'inverse, d'autres

sociétés offrent des services qui sont sur un ou deux centres de données et il sera possible de savoir où sont les données.

Ensuite, il y aura différents services de stockage en nuage : des nuages publics et des nuages privés. Sur le service de nuage public, les données seront stockées sur une machine offrant également des services pour d'autres sociétés. Cela peut induire des problèmes de porosité des données. Cela est arrivé. **Dans les systèmes de nuages privés, l'étanchéité des données pourra être garantie** par rapport à celles d'autres sociétés hébergées dans le même centre de données. Il existe encore des services hybrides de *cloud* privé dans lesquelles il est possible d'obtenir davantage de ressources à un moment donné pour faire face à un débordement en ayant alors recours à un service de nuage public.

D'un point de vue conceptuel, des fournisseurs de prestations informatiques offrent leurs services à beaucoup de sociétés : hébergement, service de calcul, plates-formes de développement, service de messagerie, services de veille, etc. Tout cela permet d'éviter de gérer tous les outils bureautiques dans l'entreprise avec leurs mises à jour. Cela simplifie une partie du travail d'administration.

Mais, en même temps, il y a une certaine perte de maîtrise des données. Une seule question à se poser : la sécurité est-elle toujours garantie ? Puis-je récupérer mes données ? Et, dans la mesure où toutes les données ont été confiées, le client devient-il captif du service ou a-t-il la liberté de pouvoir obtenir le même service chez un concurrent ?

Cette dimension de **la portabilité des données est absolument cruciale pour l'innovation** et elle est très importante du point de vue de l'informatique et des libertés. Cette portabilité des données, bien connue dans le monde de la téléphonie mobile avec la portabilité du numéro, permet de garder la maîtrise et de choisir le fournisseur qui correspond à vos besoins.

Quelle assurance de sécurité a-t-on lorsqu'on utilise les services de l'informatique en nuages ? Quand on confie ses données à quelqu'un d'autre, on perd une partie de la maîtrise de ses données.

Dans les conseils de la CNIL liés au passage au stockage en nuage, une démarche est décrite à destination des entreprises souhaitant utiliser de tels services. Il leur est indiqué les étapes qu'elles doivent suivre si elles souhaitent passer au stockage en nuage en toute sécurité. Elles doivent d'abord commencer par **recenser leurs données en distinguant celles qui sont très critiques pour continuer à les gérer en interne plutôt que de les externaliser**. Ensuite, une **analyse des risques** est effectuée pour comprendre l'attente en matière de sécurité juridique et technique du stockage en nuage.

Par exemple, l'hébergement des données de santé doit respecter un cahier des charges extrêmement précis. Cela est absolument nécessaire. Après avoir identifié les besoins, l'analyse des offres présentes sur le marché

doit être accomplie pour voir si elles correspondent au degré d'exigence attendue.

Il est également important de **pouvoir auditer la solution de stockage en nuage offerte**. Est-ce que la société, elle-même auditée, laisse accéder aux rapports d'audit la concernant ?

En termes de missions, la CNIL et l'ANSSI sont complémentaires mais leurs domaines de compétence sont un peu différents. La loi informatique et libertés oblige à mettre en place des mesures de sécurité pour garantir la protection des données personnelles. C'est la raison pour laquelle la CNIL a publié des **guides de sécurité** dont les conseils rejoignent pour beaucoup les conseils dispensés par l'ANSSI. Dans le guide listant les mesures de sécurité à mettre en place pour la gestion des risques, il est fait référence à des documents publiés par l'ANSSI. **Les règles d'hygiène de sécurité publiées par l'ANSSI sont totalement partagées par la CNIL.**

Il faut toujours distinguer les publics auxquels on s'adresse et être plus ou moins prescriptifs selon les cas.

À travers des groupes de travail, des actions lancées par les uns ou par les autres, il y a nombre d'actions communes à la CNIL et à l'ANSSI.

Il n'y a pas de redondance dans les activités mais des regards complémentaires et différents. La CNIL s'intéresse davantage à la sécurité des traitements des données et à la protection des personnes alors que l'ANSSI va s'intéresser davantage à la sécurité des entreprises. Certaines recommandations des deux organes peuvent être communes et sont toujours en cohérence.

Le champ de compétence de la CNIL est beaucoup plus large que celui de l'ANSSI puisque les libertés individuelles englobent la sécurité des systèmes d'information.

Aujourd'hui, le traitement des données personnelles est informatisé et doit être traité de manière cohérente dans le domaine technique.

Parmi les actions techniques menées par la CNIL au cours de ces dernières années, certaines ne recoupent pas du tout des sujets de compétence de l'ANSSI. La CNIL a, par exemple, travaillé sur la publicité comportementale.

L'ANSSI a constitué un **groupe de travail** auquel la CNIL participe **sur les offres de sécurité du stockage des données en nuages**. Le rôle de chacun est différent à cet égard.

La CNIL s'est aussi exprimée sur les moteurs de recherche, sur les réseaux sociaux, sur la manière de se protéger en tant que personne ou en tant qu'entreprise traitant des dossiers incluant des données personnelles.

Les prismes selon lesquels seront abordées ces questions sont totalement différents et, encore une fois, complémentaires.

Par rapport aux préoccupations de surveillance des salariés par leur employeur, la CNIL a publié, il y a quelques années déjà, un **guide à destination des employeurs** permettant de juger diverses situations au sein de l'entreprise. Toutefois, **la surveillance doit toujours respecter les droits des personnes concernées**. Un audit sur ce sujet a été publié.

Actuellement, il existe une sorte de paradoxe : les personnes ont beaucoup d'attentes en matière de protection des libertés, de contrôle de la diffusion de leurs données (droit à l'oubli, au déréférencement…) et, en même temps, elles utilisent les nouveaux instruments numériques et publient beaucoup d'informations personnelles sur les réseaux sociaux notamment. Cela n'est pas sans évoquer une certaine forme de schizophrénie.

La CNIL agit vis-à-vis de chacun des acteurs. Il est impossible d'aller à l'encontre du développement technologique et de la manière dont la société évolue face à ce type de nouveaux instruments. La CNIL s'adresse aux sociétés de réseaux sociaux pour qu'elles respectent au mieux la législation relative à l'informatique et aux libertés. Il est important qu'elles proposent une ergonomie des sites suffisamment bonne pour **que des processus simples permettent l'effacement des données et les paramétrages des partages de données**.

La CNIL conduit aussi une action de sensibilisation des personnes. Des vidéos, dont une à destination des adolescents, figurent sur le site de la CNIL pour les mettre en situation et les aider à **utiliser les instruments numériques de manière responsable**.

Depuis la loi informatique et libertés de 1978, il y a eu la directive n° 95/46/CE d'harmonisation minimale du 24 octobre 1995 fixant des obligations ; elle définit tous les principes de protection des données, transposés en droit français en 2004 ; cette directive a instauré le G29, le groupe rassemblant les CNIL européennes.

D'autres modifications de la loi sont intervenues, notamment en 2011, pour les notifications de violations de données à caractère personnel lors de la transposition par ordonnance du paquet télécoms. De 2004 à 2011, il y a eu également des modifications pour permettre à la CNIL d'accorder des labellisations.

Depuis le début de l'année 2012, une discussion est en cours sur l'évolution du cadre juridique européen. Le 24 janvier 2012, la commission européenne a présenté un **projet de règlement européen sur la protection des données à caractère personnel** ; ce projet vise à remplacer la directive de 1995.

Il y a eu une grosse activité des groupes de pressions, notamment des Américains, pour peser sur ce règlement : le Parlement européen a reçu quatre mille amendements. Une centaine d'amendements de compromis ont

été préparés et un vote au Parlement devrait intervenir avant la fin de la législature. Les discussions sont toujours en cours au Conseil.

À propos de l'attribution des noms de domaine et notamment des noms associés aux titulaires de domaines qui ont été récemment modifiés, la CNIL avec le G29 sur **la durée de conservation des noms associés aux titulaires de domaines ne respecte pas le droit européen**. À ce sujet, **le groupe du G29 a demandé à l'*ICANN* de créer des exceptions pour que les conservations des informations concernant les titulaires de domaines respectent le droit européen.**

La CNIL travaille beaucoup avec ses homologues européens notamment au sein du G29 qui se réunit très régulièrement, aussi bien au niveau des commissaires qu'au niveau technique. Il existe aussi le réseau de la Conférence internationale des commissaires. Le G29 est également présent dans des organismes internationaux comme, par exemple le groupe à l'*ISO* qui édicte toutes les normes en matière de sécurité de protection de la vie privée.

Je suis officier de liaison pour le groupe de l'article 29 pour les normes *ISO* développées en matière de protection des données.

Au niveau français, nous travaillons également avec l'ensemble des acteurs quand la CNIL élabore des recommandations, par exemple sur l'informatique en nuage, sur la biométrie, sur la publicité ciblée sur Internet, avant l'adoption d'une recommandation.

On travaille également avec les organismes de recherche à travers des conventions de partenariat. Par exemple, une convention de partenariat avec l'INRIA porte sur l'écosystème des *smartphones* avec l'application *Mobilitics*. Ce logiciel donné à des volontaires de la CNIL permettait de voir les données personnelles qui étaient ouvertes aux accès à partir de ce téléphone afin de comprendre qui collecte quelles données et dans quelle proportion.

Ce test est extrêmement intéressant car il permet de se rendre compte de l'étendue de la collecte : environ la moitié des applications accédait à la géolocalisation et ensuite il y avait **76 localisations par jour effectuées en moyenne**. Des partenaires extérieurs à la CNIL se sont associés à cette opération.

Cela est important de s'appuyer sur les compétences existant en France comme à l'étranger pour comprendre les difficultés rencontrées relatives aux personnes que l'on cherche à protéger. De plus, comme pour les géants de l'Internet, les questions qui se posent sont les mêmes dans le monde entier, il faut travailler de concert avec nos homologues européens.

Des recommandations pratiques sont à mettre en place pour la sécurisation des données. Ce qu'il faut voir, c'est l'utilité pour les entreprises, comme pour les personnes, du travail effectué par **la CNIL qui**

aide les entreprises à prendre en compte, très en amont, les préoccupations informatique et libertés pour que, lorsque leurs produits arrivent sur le marché, ils soient respectueux de la loi. Cela leur permet de valoriser cette sécurité aux yeux de leurs clients.

La CNIL a cette image de gendarme de la protection des données mais son rôle de conseil auprès des entreprises s'est beaucoup développé. De plus en plus d'entreprises viennent voir la CNIL au moment du développement de leurs projets et demandent une assistance pour être certaines de respecter la loi.

En général, les entreprises sont satisfaites de leur contact avec la CNIL car, arrivées avec des problèmes, elles repartent avec des solutions.

Souvent des traitements parfaitement légitimes doivent être mis en place mais encore faut-il les effectuer dans le respect de la loi. Dans beaucoup d'exemples, même par rapport à des géants de l'Internet, des modifications substantielles sont obtenues par la CNIL afin que les garanties soient assorties aux systèmes mis en place. Cela bénéficie tant aux utilisateurs français qu'aux utilisateurs européens voire mondiaux.

Les agents de la CNIL sont tous très investis dans leurs missions et enthousiastes car l'utilité du travail quotidien est évidente. En partant de la carte bancaire et en passant par le passe *Navigo* ou le téléphone, la CNIL travaille sur tous ces objets du quotidien et obtient des avancées en matière de protection des données liée à leurs usages.

Les cartes bancaires actuelles incluent une puce avec contact mais également une puce sans contact. L'été dernier, il y avait à peu près quinze millions de cartes sans contact en circulation. Par exemple, sur cette carte-ci figure un petit logo avec des vaguelettes signifiant qu'une puce sans contact est intégrée à la carte. Cela permet d'effectuer des paiements sans glisser sa carte dans le terminal de paiement. Cela a commencé par les paiements de petits montants pour fluidifier ceux-ci.

Quand ces cartes sont apparues, il était possible avec un téléphone de lire directement le contenu de la puce incluant le nom du porteur de la carte, le numéro de la carte, la date d'expiration et l'historique des transactions.

La CNIL, l'Observatoire sur la sécurité des cartes de paiement et la Banque de France ont demandé à l'ensemble des acteurs de la carte bancaire de changer ce système et des garanties ont été obtenues. En conséquence, le nom du porteur et l'historique des transactions n'apparaissent plus dans ces puces. La sécurité de ce moyen de paiement peut être encore améliorée. Voilà un exemple de mesure concrète.

Autre exemple : le passe *Navigo* est également doté d'une puce contact et d'une puce sans contact à propos de laquelle la CNIL a

recommandé que seules figurent dans le passe les trois dernières données de validation.

Si on met des cartes bancaires dans un lecteur – paiement jusqu'à sept euros auprès de la RATP – et avec l'aide d'un logiciel gratuit sur Internet, on peut lire le contenu de la puce contact sans aucune authentification, mais vous ne verrez que les trois dernières données de validation mentionnant également la station de métro empruntée ainsi que l'heure de passage. La limitation aux trois dernières données est importante pour garantir la liberté d'aller et venir.

Pour certaines formules de passe *Navigo* le nom, le prénom et la photo se trouvent dans la base commerciale du système de transport de la région parisienne. Il existe un autre type de passe qui s'appelle *Navigo « découverte »* qui est un passe déclaratif, dans le sens où même si le nom du porteur y figure, les informations nominatives ne se trouveront pas dans la base de données du transporteur. Quand ce passe *Navigo* a été lancé, la CNIL a constaté que la RATP ne le mettait pas du tout en avant dans ses offres et que, en conséquence, très peu de gens utilisaient le passe *Navigo « découverte »*.

Il a fallu une recommandation de la CNIL, ainsi que d'autres actions, pour inciter la RATP et les transporteurs de la région parisienne à mettre en avant le passe « *découverte* » et ce qu'il pouvait apporter. Par conséquent, il y a eu de la publicité effectuée et davantage de personnes aujourd'hui utilisent ce type de passe.

Il y a cependant certains avantages à disposer d'un passe nominatif, par exemple, en cas de perte du passe nominatif, il est possible d'en créer un nouveau incluant l'abonnement déjà acquitté. La CNIL souhaitait que la personne puisse choisir en toute connaissance de cause et ne soit pas forcée à utiliser un système qui induit une plus grande traçabilité.

Le passe « *découverte* » s'est beaucoup développé. Maintenant, les commerciaux en stations connaissent tous l'existence du passe *Navigo « découverte »*.

Pour être efficace et démultiplier l'action de la CNIL, il existe notamment le réseau des correspondants informatique et libertés, ce qui permet de diffuser la culture informatique et libertés, par exemple dans les entreprises.

La CNIL dispense également des formations aux correspondants informatique et libertés et conduit beaucoup d'actions vis-à-vis du grand public, ce qui encourage les entreprises à prendre ces aspects en compte, notamment dans leurs offres de services, ce qui différenciera leurs offres de celles de concurrents.

NOV'IT

M. Jérôme Notin, président

19 février 2014

Aujourd'hui, en France, les entreprises, les administrations et les particuliers font de plus en plus confiance à des logiciels antivirus étrangers. Nous faisons donc confiance à des logiciels propriétaires et **fermés** qui sont **installés sur les postes de travail et les serveurs et qui ont accès à toutes les données tout en échangeant de manière chiffrée avec l'étranger**. Cela, philosophiquement, pose un problème.

Lors de l'élaboration du Livre blanc sur la défense, on parlait beaucoup des problèmes éventuellement causés par les Chinois qui souvent font des choses peu louables. Il s'agit là d'intelligence économique et non de lutte contre le terrorisme Le ministère de la défense et l'ANSSI ont conscience de ce problème depuis longtemps. Les recherches sur la cryptologie permettraient de trouver des solutions sur certains points.

En parallèle, les Américains enregistrent absolument tout et, même s'ils sont incapables de tout déchiffrer aujourd'hui, ils estiment qu'ils pourront y parvenir dans quelques années. Le vrai chiffrement étatique demeure cependant très difficile à déchiffrer. Le type de chiffrement est d'ailleurs effectué en fonction des différents niveaux de classification de l'information.

Il y existe un gros problème de souveraineté, de confiance dans les outils, antivirus ou autres. Par définition, toute l'information conservée sur des machines est concernée, où que ce soit.

Cela fait plus de dix ans que je travaille dans le domaine de la sécurité, avec des recherches et des réflexions sur les innovations. Et il n'y a eu aucune évolution que ce soit sur les matériels ou logiciels, toujours russes ou américains, ou en tout cas pas de vraies solutions opérationnelles pour les entreprises, les administrations et les particuliers.

Un exemple de la domination étrangère et de la perte de souveraineté est donné par les outils de gestion des événements des systèmes d'information. Ce sont de véritables pieuvres qui se mettent au-dessus des antivirus, des routeurs, des pare-feu, des serveurs, de tout ce qui est informatique. Ces outils ont normalement une intelligence leur permettant de corréler des éléments. Ce qui permet, par exemple, de repérer une attaque depuis la Chine, ou, un dimanche, de constater qu'une machine

de votre réseau se connecte à d'autres machines et envoie beaucoup d'informations.

Thales propose cela mais avec un outil américain *Arcsight* financé par le fonds *In-Q-Tel*, lui-même financé par la *CIA*.

Heureusement, l'État conduit des réflexions sur ce type d'outils et travaille sur un appel à projet qui a pour objectif principal de **disposer de sondes souveraines. Des technologies maîtrisées, ni américaines ou chinoises, seront employées pour développer nos propres outils de surveillance réseau**. Ce que l'État a imaginé, en tant qu'outil de supervision de sécurité globale du système, ce sera le but ultime car il sera capable de voir ce que les autres outils ne voient pas.

Un antivirus est là pour protéger mais il ne peut être infaillible. En revanche, ce système global sera au-dessus de toutes les strates d'information.

Le contrat moral que DAVFI (Démonstrateurs d'antivirus français et internationaux) avec l'État est de pouvoir **fournir un outil qui va bien plus loin que ce que font aujourd'hui les antivirus**. Nous sommes très bien partis pour y parvenir ; les résultats sont très encourageants. La première partie des modules, actuellement testée, permet déjà de faire beaucoup plus que ce que permettaient les antivirus actuels, en particulier sur les capacités de détection de codes inconnus, qui est le vrai défi technique et le vrai besoin opérationnel.

Dans le contexte actuel des communications, n'importe qui peut devenir une cible potentielle et faire l'objet de tentatives de déstabilisation de la part de puissances étrangères. Aujourd'hui, si on ne réussit pas à pénétrer mon téléphone, on aura quand même des informations sur moi par des éléments détournés comme la géolocalisation. Par recoupement, on aura un profilage.

La *NSA* croise les communications. Dans le monde du renseignement, plus on a de l'information, plus c'est intéressant même pour les services français. Le renseignement informatique au sens très large aide les services dans leur mission, dans la lutte contre le terrorisme ou dans l'intelligence économique.

Un exemple bien connu, en matière de vente d'avions, dans la concurrence entre *Airbus* et *Boeing*. Quand M. Édouard Balladur était Premier ministre, il a pris l'avion pour l'Arabie Saoudite et il n'y avait que deux personnes connaissant le prix qui allait être proposé pour cette vente qui allait être signée. Le Premier ministre a passé une communication téléphonique depuis l'avion avec une des deux personnes en charge de la négociation mentionnant ce prix et, à l'atterrissage, il été constaté qu'une offre financière juste un peu meilleure venait d'être effectuée par *Boeing*.

À l'époque les communications chiffrées n'existaient pas ou étaient très peu efficaces. Et la *NSA* avait déjà mis en place *Echelon*. Maintenant elles existent mais ce n'est pas forcément pour autant que les hommes politiques les utilisent. *Teorem* existe : ce téléphone sécurisé permet de chiffrer les données, de chiffrer la voix, de tout chiffrer. Mais il reste dans la boîte à gant des voitures des autorités.

L'exploitation du renseignement consiste à chercher une aiguille dans une botte de foin, mais plus on a de moyens plus cela est facile.

Pour revenir à DAVFI, il comprend aujourd'hui cinq entités et, dans le consortium, il y a une vingtaine de personnes. Fin octobre 2014, on arrête le financement dans le cadre du Programme d'investissements d'avenir (PIA) et nous allons initier la commercialisation, tout en continuant la recherche et développement.

Ma formation est commerciale et M. Éric Filiol est docteur en informatique. Des doctorants travaillent au sein du laboratoire. Ce sont des permanents qui se concentrent sur le développement informatique, la sécurité, la cryptologie et la virologie opérationnelles, dans un laboratoire qui comprend en outre une bonne douzaine de semi-étudiants ; il y a également des ingénieurs.

M. Éric Filliol travaille depuis très longtemps dans ce domaine-là, notamment au ministère de la défense. Il casse les antivirus et organise un concours sur ce thème nommé *Iawacs (International Alternative Workshop on Aggressive Computing and Security*). Les antivirus sont testés avec des codes malveillants.

Dans DAVFI, le laboratoire travaille également beaucoup sur la protection même et aussi sur les tests d'antivirus pour qu'ils soient résistants aux attaques.

Aujourd'hui, les acheteurs publics ont la tâche difficile lorsqu'il s'agit de choisir des antivirus notamment lorsque le critère du prix prend le pas sur d'autres considérations. L'intérêt est de mettre au point des produits qui détectent toutes les variantes d'un virus et pas seulement le virus *stricto sensu*.

De nouveau, à propos de la souveraineté numérique, Mme Angela Merkel a très mal pris les écoutes opérées en Allemagne par les Américains. En France, l'État prend de plus en plus conscience de la nécessité d'une protection en matière numérique. C'est le rôle du politique de travailler à l'Europe de la défense en y incluant le numérique.

L'informatique est connue pour bénéficier de découvertes parfois effectuées par des individus solitaires. *Apple* et *Google* en ont fait la démonstration.

Des entreprises sensibles injectent dans leurs systèmes des mises à jour de logiciels sans connaître ce qu'il y a dedans. Or, le vrai virus est furtif

et des portes dérobées sont mises en place avec le but qu'elles ne soient pas découvertes.

Énormément de données ont été exfiltrées quotidiennement de chez *Areva* qui ne s'en est aperçu qu'au bout de plus de deux années, probablement grâce à la mise en place d'un système de supervision. *Nortel,* société canadienne, s'est fait piller pendant des années et a disparu à cause de cela.

Les rôles de la CNIL et de l'ANSSI sont complémentaires. La CNIL a un rôle fondamental à jouer par rapport aux libertés individuelles. Ainsi, l'ANSSI essaie de mettre en place des procédures conformes à l'esprit de la CNIL. Il faut respecter toute leurs préconisations mêmes si cela n'interdit pas d'aller plus loin. La CNIL est très au fait des problématiques du monde de l'entreprise.

La fonction géolocalisation est très utilisée par *Google* ; elle est juste déclarative mais, sur une application, si vous répondez que vous refusez la géolocalisation, l'application peut ne pas fonctionner. Certaines applications sont considérées comme saines et utiles ; en revanche, il est possible d'envoyer une fausse localisation, par exemple l'adresse de la *NSA* ou d'autres : c'est ce que nous avons fait dans notre solution de mobilité sécurisée *Uhuru Mobile*.

La quantité d'informations recueillies par les services alliés n'a plus rien à voir avec celles recueillies il y a encore dix ans ; cela permet des recoupements sur plusieurs années.

Dans beaucoup d'applications fournies par *Google* figure la géolocalisation. En général, les gens ne sont pas choqués par cela.

Notre rôle est un rôle de protection, par exemple grâce aux antivirus sur le poste de travail. **Pour la partie téléphonie, une véritable protection des données peut être obtenue grâce au chiffrement des données, de la voix, des *SMS*.**

Les ministères de l'intérieur et la défense imposent des normes et des outils au sein de leurs services. On a relevé énormément le niveau de sécurité en France. Il y a quelques domaines d'excellence dont la cryptologie au ministère de la défense.

Les Américains imposent de fait les standards et les normes et, assez rapidement, dans deux ou trois ans, ils seront capables de casser les codes et déchiffreront les informations stockées par eux.

La *NSA* a volontairement réduit le système de chiffrement de la société privée *RSA*.

Le nuage informatique, qui existe depuis une dizaine d'années, devrait permettre globalement de faire baisser la consommation d'énergie puisque la puissance de calcul est déportée dans les centres de données.

À propos de variantes de l'obsolescence programmée, il est totalement anormal, par exemple, qu'*Apple* ne permette pas de changer la batterie sur un téléphone.

Chaque fois que *Microsoft* sort une nouvelle version, cela crée un besoin absurde, très dommageable puisque cela contraint à utiliser de nouvelles applications. *GNU/Linux* aurait pu être une solution.

La Gendarmerie nationale a l'intelligence, très particulière au sein du système français, de vouloir comprendre et maîtriser l'informatique et les nouvelles technologies en général. Elle a donc adopté le logiciel libre.

Le monde industriel est toujours en retard pour la sécurité des produits informatiques par rapport aux usages. Quand les *iPhones* sont arrivés, ces téléphones personnels ont été utilisés au lieu de ceux de l'entreprise qui étaient d'ancienne génération. Les entreprises n'avaient à l'époque pas les moyens de sécuriser le système et ces nouveaux usages. Sur le téléphone, la récupération de toutes les informations peut causer de vraies difficultés aux entreprises en cas de perte ou de vol. Il y a des solutions mais il faut offrir des téléphones aux collaborateurs pour être dans un monde maîtrisé. Cela peut permettre d'accéder aux applications personnelles mais **les gens n'ont pas conscience des problématiques de sécurité au sens très large**.

La sécurité, ça coûte cher, c'est pénible, ce sont des contraintes. Mais quand vous êtes *Areva* ou *Nortel* **cela coûte encore plus cher de ne pas avoir de sécurité**. Au sens très large, la sécurité informatique peut être comparée à la sécurité incendie où, financièrement, certains hésitaient à franchir le pas. C'est pourquoi on a prévu des contrôles obligatoires en matière d'incendie pour sortir du « *Tant qu'il n'y a pas de pépin, tout va bien* ». Pour le numérique, les pompiers seraient l'ANSSI et les extincteurs seraient les antivirus ou les pieuvres (*SIEM*) déjà évoquées précédemment.

Dans le cadre européen, la défense du patrimoine européen risque vite d'être taxée de protectionnisme. Surtout, le principe de libre concurrence risque de faire accuser de favoritisme les sociétés européennes. On sait toutefois très bien que les États-Unis d'Amérique ou la Chine sont parmi les pays les plus protectionnistes.

Un État européen est en avance en matière de cyberdéfense : l'Estonie. Déjà en avance en matière de numérique, elle l'est encore plus après avoir été attaquée massivement en 2008. Beaucoup de délégations françaises, dont l'ANSSI, sont allées en Estonie. Le centre de Tallinn est très connu. Les Anglais sont également en avance dans ce domaine par rapport à la France.

Les noms de domaine ne sont pas le plus gros problème. **Il existe des protocoles libres et des associations qui pourraient être utilisés mais constitueraient potentiellement une déclaration de guerre. Aujourd'hui,**

Internet ne peut plus être contrôlé par un État mais doit l'être par une organisation internationale pour ce qui relève des noms de domaines.

En revanche, il est parfois dangereux de se voir imposer des normes pour l'Internet ou des « standards » comme l'*Unified Extensible Firmware Interface* (*UEFI*). **Tous les États participent à la définition des normes dans des réunions internationales où 80 % des présents sont des Américains. Ils y défendent en premier lieu leur intérêt économique qui va parfois à l'opposé de celui des États tiers ou des utilisateurs du réseau**.

Le monde du logiciel libre a de très fortes inquiétudes parce que, potentiellement, avec le système qui va être mis en place par l'*UEFI*, il ne sera très difficile voire impossible d'intervenir sur un ordinateur pour changer le système d'exploitation.

Il existe des moteurs de recherche *DuckDuckGo* ou *Qwant,* très performants, qui n'enregistrent rien de vos requêtes. *Qwant* est d'ailleurs français.

Un standard est quelque chose que tout le monde utilise ; une norme fixe des règles d'utilisation.

On ne peut pas s'inspirer de solutions adoptées dans autres États car elles sont souvent obsolètes ou faites pour leur propre intérêt. Évidemment, les sociétés doivent gagner de l'argent mais il faut avoir des systèmes de protection globaux et jouer un rôle face aux citoyens.

Il existe un logiciel libre à adapter sur des systèmes mobiles, conçu à partir d'une base *Linux* permettant d'améliorer la protection assurée par les antivirus qui ne peuvent pas protéger totalement les entreprises. **Plusieurs couches de protection sont nécessaires** : la première, la deuxième, la troisième, etc., **et, au-dessus, un outil de supervision**. Même avec le meilleur des antivirus, le système d'information n'est pas totalement protégé.

Dans le domaine de l'informatique industrielle, une prise de conscience est nécessaire au niveau des systèmes, *SCADA,* informatiques industriels. Il s'agit de logiciels particuliers, des systèmes de contrôle maintenant interconnectés et parfois directement reliés à Internet. **Il s'agit de systèmes fermés pour lesquels on n'a pas toujours pris en compte le concept de sécurité, la mutualisation des réseaux induisant ainsi une certaine fragilité.** C'est ainsi que, aux États-Unis d'Amérique, un jeune de seize ans a réussi à couper le système de climatisation d'un hôpital puis a essayé de rançonner cet hôpital. Il est anormal que l'interruption de la climatisation d'un hôpital soit possible depuis Internet.

Pour des raisons de coût, les mêmes protocoles et infrastructures sont utilisés mais c'est au détriment de la sécurité.

À Paris, il existe le système des valves électriques qui va alimenter en eau la ville de Paris, le système des pompiers, celui du service des espaces verts, etc. ; cinquante réseaux municipaux ont été identifiés et de nouveaux

usages vont encore apparaître. Le génie civil coûte très cher. Le système nucléaire possède son propre réseau mais l'armée, pour l'usage courant, utilise les réseaux publics. D'où la nécessité du recours à la cryptographie, ce qu'elle fait très bien.

Il faut espérer que les compteurs électriques intelligents soient sécurisés mais, aujourd'hui, ce n'est pas le cas. À travers eux, il est possible de savoir quand les personnes sont là, à quelle heure elles arrivent, quand elles allument la lumière, le four, etc. Les Allemands auraient même été capables, à partir des fréquences, de déterminer la chaîne de télévision regardée. **Toutes ces données ne sont pas ou mal sécurisées et passent par les fils électriques.**

C'est un faux progrès. On va donner ces informations à des entreprises privées qui vont les revendre à d'autres entreprises privées. La technologie permettra de savoir exactement ce que vous consommez, de connaître vos habitudes. Il s'agit là de la protection des citoyens et de la vie privée.

De même, dès que vous jouez sur un téléphone, vous êtes localisés. Il y a eu un scandale récemment avec le jeu *Angry Birds*, qui permettait à la *NSA* de vous localiser si vous aviez installé ce jeu.

CONSEIL DES INDUSTRIES DE CONFIANCE ET DE SÉCURITÉ (CICS)

M. Hervé Guillou, président

M. Jean-Pierre Quémard, vice-président security and technology communication intelligence and security (Airbus Defence and Space)

M. Gérard Moisselin, ancien préfet

26 février 2014

M. Hervé Guillou. –Le Conseil des industries de confiance et de sécurité (CICS) a vocation à s'occuper d'un ensemble de questions de sécurité considérées comme critiques ou souveraines. Il intervient sur le périmètre suivant : sécurité des frontières terrestres, maritimes et aériennes, sécurité des citoyens, sécurité des infrastructures, sécurité des transports au sens de flux, et non pas des aéronefs ou des automobiles mais des flux de transports de personnes et de biens et, enfin, la cybersécurité dans ses trois dimensions : sa **couche physique**, c'est-à-dire les télécoms, les tuyaux, les ordinateurs, sa **couche virtuelle, logiciels,** protocoles, serveurs, etc., et, dans sa **couche informationnelle**, informations, propriété de l'information, traitement de l'information.

Ce syndicat, cette filière ont été créés parce que le sujet de la sécurité en France est plutôt bien engagé en termes industriels puisqu'il a bénéficié d'une histoire dynamique dans le domaine de la défense. La France a une industrie de défense historiquement puissante, très forte technologiquement. Cette industrie de défense, depuis le début des années 2000, a pu et a su transformer une bonne partie de ces technologies en technologies utilisables dans le secteur de la sécurité. Depuis 2003, des positions sur le marché mondial ont été prises dans le domaine de la sécurité (frontières, sécurité maritime, communications sécurisées…). *Thales*, sur la lancée, a aussi pris des positions très fortes dans le domaine de la vidéosurveillance ; le *Morpho*, filiale du groupe *Safran* a pris des positions, par exemple, dans le domaine de la morphotechnologie, de la gestion d'identité. Et puis, de l'autre côté, du côté civil de la force, nous avons une industrie dynamique avec des sociétés comme *Gemalto*, *Alcatel*, des PME très nombreuses qui ont aussi contribué à ce domaine de la sécurité.

Finalement, les forces technologiques sont dispersées dans la chaîne de valeurs et dans un marché pas très bien organisé. Dans une foire sur la sécurité, vous trouvez de tout, depuis les *T-shirts* en carbone, les systèmes de surveillance des frontières, l'aéronautique, l'électronique, les logiciels, les services. On a alors pensé qu'il était indispensable de se regrouper pour

passer à l'étape suivante afin de poursuivre le développement dont nous avons besoin, sans avoir un moteur de fusée du côté du ministère de la défense aussi fort qu'il était avant. C'est une industrie extrêmement intéressante pour la France actuellement car elle représente environ **9 milliards d'euros de chiffre d'affaires**, **50 000 emplois de haute technologie** peu délocalisables, **70 % d'export, 10 % de croissance par an**.

Du côté de la puissance publique, il y a le même phénomène de dispersion que dans l'industrie, c'est pourquoi le Premier ministre a décidé de lancer la filière sécurité, en octobre 2013, pour rassembler également la puissance publique autour des sujets transverses de la sécurité que sont l'expression des besoins, la mobilisation des ressources financières autour de la recherche et du développement, des questions de souveraineté, la question de la normalisation, la position vis-à-vis de Bruxelles, etc. Il n'y a pas d'administration de la sécurité ; dans les pays européens, le sujet de la sécurité est très dispersé entre les divers départements ministériels, il n'y a pas de ministres de la sécurité. Aux États-Unis d'Amérique, le département sécurité (*Department of Homeland Security*) couvre tout sauf la cybersécurité qui est liée à la défense dans la fameuse *NSA*. Tous les pouvoirs régaliens sont concentrés au même endroit ce qui inclut la recherche et le développement.

Les Anglais ont lancé une initiative un peu similaire quoique moins complexe, en 2005, avec l'ancienne responsable du *MI5*. C'est elle qui a lancé l'initiative nommée *National Resilience* qui était une vision assez large de la résilience physique et économique. En France, on a lancé, en 2014, la filière de sécurité avec un certain nombre de grands sujets : analyse capacitaire des besoins à long terme, questions de politiques industrielles, technologies critiques, recherche et développement, recherche et technologie et puis quelques sujets transverses comme les questions de la souveraineté, les questions européennes, l'export… Nous sommes très satisfaits de cette initiative qu'il faut concrétiser car le cyber est un des axes les plus actuels de cette filière sécurité.

Le sujet de la cybersécurité est bien plus qu'une mode, bien plus qu'une question de renseignements, de libertés publiques, c'est aussi un véritable sujet de souveraineté, un sujet de politique économique, de risque, et un sujet de résilience et de sécurité pour les pays. La cybercriminalité s'exprime sous toutes ses formes.

Par analogie, quand on a ouvert au XVI^{e} siècle un milieu d'échanges qui s'appelait la mer, comme un moyen de communication, s'est développé exactement ce qu'il se passe aujourd'hui dans la cybercriminalité. Dans un milieu ouvert, sans véritables règles, se développent des pirates, des corsaires et des marins militaires. Dans le cyberespace, nouveau lieu d'échange d'informations, se développe de la criminalité pure et simple, il existe des pirates, des corsaires qui sont les agences parapubliques plus ou moins officielles qui, elles aussi, gèrent par procuration la bataille

économique. Les militaires sont les organismes de défense et d'attaque de ce cyberespace.

Il se passe des choses extrêmement importantes en ce moment, en raison du déséquilibre entre les défenseurs et les attaquants dans le cyberespace, qu'il ne faut pas limiter aux télécoms – le cyberespace étant l'ensemble constitué par la couche physique, la couche virtuelle et la couche informationnelle. Même les *switches* dans les télécoms, tout cela est en train de devenir virtuel. La couche, que l'on croit physique, des télécommunications est en train de devenir aussi une couche virtuelle. Dans ces trois couches, le déséquilibre entre les défenseurs et les attaquants n'a jamais été aussi grand, peut-être, depuis l'apparition des sous-marins nucléaires.

Les attaquants n'ont pas de contraintes économiques parce que ça ne coûte presque rien de se livrer à une attaque, cela coûte beaucoup moins cher que de s'acheter une frégate, que d'envoyer des commandos entraînés. Il n'y a donc pratiquement pas de limites économiques. **Les attaquants ont une liberté, une ubiquité quasi totale.** Ils ont une impunité quasi totale. Sauf sur quelques sujets, comme la pédophilie, **personne ne sait quelles sont les lois à appliquer** étant donné l'absence de frontières en ce domaine.

Le problème est que, dans le cyberespace, le juge ne sait pas lui-même déterminer sa compétence. Prenez l'exemple de *Sony* qui s'est fait voler 150 millions de cartes bleues. Le pirate est passé par six pays différents et quatre serveurs qui ne sont pas dans le pays de la société attaquée. Il est très difficile d'attribuer une attaque à quelqu'un de précis et, ensuite, il est difficile de savoir le type de droit à y appliquer et de connaître la juridiction compétente.

À l'inverse, certains défenseurs, y compris nous-mêmes en tant que citoyens, placent de plus en plus de richesses sur ce média, notamment les transactions bancaires, des informations personnelles, commerciales. Aujourd'hui, dans l'économie globale, une société qui se veut globale place tout sur Internet.

Dans le monde bancaire, il existe une tradition de sécurité à partir des cartes à puce qui ont fait des progrès considérables ; le cœur de tout cela repose sur une identité fiable ; tout dépend de cela.

Les défenseurs placent de plus en plus de richesses sur Internet : le bureau d'études, le système d'information, la *supply chain* pour parler avec ses fournisseurs. Surtout, le nombre de points d'entrée dans le système est de plus en plus important. **Il y avait 500 millions d'adresses *IP* en 2003 et il y en a maintenant 12 milliards, bientôt 13 milliards et, probablement, 80 milliards d'adresses *IP* en 2020. Il s'agit-là de la deuxième révolution numérique.**

Deux questions critiques se posent : le déséquilibre entre les attaquants et les attaqués et donc une attractivité économique au crime

devenue supérieure au trafic de drogue et, deuxièmement, une explosion complètement irréversible qui est la connexion de trois mondes jusqu'ici technologiquement disjoints. Ce sont le monde de l'informatique générale, avec *Microsoft, Atos, IBM*, *Capgemini* ; le monde de l'informatique dite industrielle, avec *Siemens*, *Schneider*, les automates dans les usines, la robotique, les outils de bureau d'études, et le monde de l'informatique dite embarquée avec *Dassault électronique*, *Thales,* qui est l'informatique dans les véhicules et les objets. C'est aussi le cas des *iPods*, *iPhones, etc*.

Ces trois mondes sont de plus en plus connectés. Par exemple, vous voulez surveiller une raffinerie, vous pouvez le faire par le logiciel de gestion partout dans les usines. Le monde de l'informatique industrielle et le monde de l'informatique générale sont de plus en plus connectés. Quant à l'informatique industrielle et l'informatique embarquée, un exemple l'illustre : un *Airbus* a déjà sept points d'entrée : un lien lors des incidents logistiques, un lien avec l'usine ou avec *Air France*, un autre avec les passagers, un avec la police, etc. L'année prochaine votre voiture, votre réfrigérateur auront leurs entrées ; cela est irréversible. Donc, **le nombre d'entrées dans le système va se multiplier probablement par dix en moins de dix ans**. Sans affoler les foules, c'est tout de même un sujet de préoccupation.

Internet a représenté des progrès fantastiques de productivité et de croissance mais cela apporte aussi des vulnérabilités. C'est aussi une chance pour l'industrie de développer de nouveaux produits. C'est un monde qui est assez fragmenté entre des grands groupes très spécialisés et une myriade de PME fragiles et subcritiques qui n'ont pratiquement pas accès à l'export. C'est un domaine où on a beaucoup d'atouts mais aussi beaucoup de choses à faire.

M. Jean-Pierre Quémard. – Il serait ainsi nécessaire de **demander que tous les opérateurs d'importance vitale aient un niveau de sécurité minimal** ; **de développer, pour les besoins français, une structuration de la demande et de l'offre**. Il y a énormément de PME qui développent toutes la même chose plutôt que des produits complémentaires ; s'adressant à un tout petit marché, elles ont énormément de mal à se structurer pour aller à l'export, ce dont les Allemands et les Anglais sont capables. La PME ne peut aller à l'export pour trois raisons : la réglementation export est très compliquée ; la PME n'a pas connaissance des appels d'offres ; elle n'est pas capable de travailler sur les aspects de normalisation car l'interopérabilité doit permettre de se connecter sur l'étranger et permettre surtout de déposer des brevets, d'avoir un avantage concurrentiel en développant certaines fonctions.

La gouvernance de <u>la normalisation en France</u> est catastrophique. Tout simplement parce que la normalisation est le pré carré de l'AFNOR ; on ne peut passer que par l'AFNOR. Tous les grands pays font comme cela sauf que, **en France, on paie trois fois pour accéder aux normes**. La première fois

pour avoir le droit de participer au groupe AFNOR, la deuxième, pour envoyer travailler des experts et, encore une fois, pour acheter la norme que vous avez produite car vous ne pouvez l'utiliser sans l'acheter. Cela est aberrant. Au Japon, cela n'est pas du tout comme ça car non seulement les entreprises ne payent pas mais elles sont payées pour participer au processus de normalisation.

Dernier point, il faut structurer et renforcer l'offre nationale de cybersécurité en aidant les entreprises à travailler ensemble pour éviter une concurrence excessive.

M. Hervé Guillou. – **Les PME françaises ne sont pas suffisamment solides pour servir les grands opérateurs comme *EDF*, *Peugeot*, *Michelin* ou *Total*.**

Du côté de l'émergence du marché, il faut **promouvoir par la voie législative les outils permettant aux infrastructures publiques ou privées de se protéger**. Il est utile de se protéger par la voie de la normalisation technique, des certifications de produits mais aussi à travers la gouvernance de l'entreprise. Aux États-Unis, on oblige les sociétés cotées à effectuer une déclaration annuelle de risque.

Quant au volet des assurances, **il n'y a pas aujourd'hui d'offre d'assurance en cybersécurité.**

Tout ce qui contribuera à dynamiser la demande et à créer un écosystème favorisant l'investissement dans le domaine de la protection sera utile.

Du côté de l'offre, il y a deux volets, extrêmement techniques, où l'**on a besoin de solutions indépendantes des Américains**. Aujourd'hui, **100 % de l'offre émane des Américains**. Des entreprises valant plusieurs dizaines de milliards sont déjà dans ce secteur. L'État américain finance 80 000 emplois dans l'industrie.

M. Jean-Pierre Quémard. – Nous poussons à la création d'un label France pour les produits évalués et qualifiés en France. Si on déclare que les opérateurs d'importance vitale ne peuvent utiliser que des produits labellisés en France, cela va changer les choses.

M. Hervé Guillou. – Il y a trois sujets critiques qui sont les *SCADA*, qui sont des outils de protection des produits industriels, la gestion du temps réel avec les *Security Operations Centers (SOC)*, et puis tous les sujets liés à l'identité. On a raté le sujet relatif à la carte d'identité ; cela est très grave. S'il n'y a pas d'identité souveraine, ce n'est pas la peine. Plusieurs initiatives ont été lancées en ce sens.

M. Jean-Pierre Quémard. – La technique existe mais il faut **mettre en place une politique nationale d'identité numérique**. S'il y a un passeport

numérique en France, ce n'est pas grâce à la France, c'est grâce à l'Organisation de l'aviation civile internationale (OACI).

Il faut un outil de démonstration d'identité suffisamment fiable. Avec cette carte d'identité, à un moment donné pour avoir accès à un lieu, il suffit juste de prouver que vous habitez cette ville.

M. Hervé Guillou. – Il faut que ce soit suffisamment répandu et économiquement viable et que cette identité soit extensible aux objets. Avec le nuage, la dématérialisation du support va imposer un lien direct avec les données et le propriétaire.

Lors du vote de la loi sur la programmation militaire, en novembre 2013, plusieurs députés et sénateurs nous ont alertés. Les industriels ont fait une campagne mensongère pour pouvoir utiliser vos données de localisation dans leurs outils *marketing* et cela dans le seul souci de leurs intérêts commerciaux. Il y a là des enjeux économiques colossaux.

Le Parlement peut jouer un rôle très important dans l'éducation et la formation pour former des gens compétents. Ce constat est partagé par toute l'industrie.

Il ne s'agit pas seulement de former des docteurs de l'université mais aussi des techniciens dans des écoles de formation technique comme Compiègne, Grenoble ou Troyes. On développe aussi un nouveau *master* en cybersécurité ; il y a aussi le niveau du doctorat.

Il existe un besoin colossal de formation des décideurs publics et privés. L'équivalent anglais de l'ANSSI fait payer, un par un, tous les comités exécutifs et toutes les directions générales. Cela est fondamental. Il y a un problème générationnel. Le PDG moyen, le directeur moyen, repassera le problème à son directeur informatique qui, en général, n'y connaît rien.

Les dirigeants et les *leaders* d'opinion, publics ou privés, savent que, derrière, c'est la question de l'hygiène informatique. **La cybersécurité est une question d'hygiène.** Il s'agit d'éducation du grand public. Tout comme on se lave les mains quand on la grippe, il faut un minimum d'hygiène informatique.

M. Jean-Pierre Quémard. – Il y a là, derrière, une question de données massives (*big data*). Souvent la corrélation entre une multitude d'informations va permettre de dresser un profil. Effectivement, le fait que vous achetez quelque chose, à un certain droit, que vous avez telles habitudes, ce n'est pas important individuellement. Mais l'ensemble de toutes ces choses-là commence à devenir significatif. Ce n'est pas un problème de nuages, c'est un problème de données massives.

M. Jean-Pierre Quémard. – Tout cela va très vite. Il faut anticiper, accompagner et mettre en place des dispositifs adaptés. Il faut que la personne qui développe un outil, un logiciel ait en tête les règles qui permettent d'apporter des garanties.

M. Hervé Guillou. – Il est encore temps d'agir. **Le plus urgent c'est que le législateur crée un environnement légal pour que la France soit un pays où l'on puisse faire des affaires de manière sûre** car cela aura la double vertu de ne pas pénaliser nos entreprises et notre économie et d'attirer les investisseurs. Si l'environnement français sécurisait les entrepreneurs étrangers, ces derniers souhaiteraient venir en France.

Par exemple, il faudrait **obliger les entreprises cotées à déclarer leurs risques** divers, **contraindre les organismes d'importance vitale à utiliser des solutions labellisées en France** pour se protéger ; par exemple, dans le domaine législatif, **obliger les agences à discuter d'une couverture cyber qui ne soit pas limitée au remplacement des postes informatiques**. **Aujourd'hui, le risque cyber a bien plus d'impact que bien des risques figurant dans les rapports annuels.**

190 milliards d'euros de pertes sont dus au risque lié à la cybersécurité dont une part importante du fait de la fraude à l'identité. **Le marché mondial de la cybersécurité, c'est 50 milliards d'euros** dont la moitié aux États-Unis d'Amérique. La France, l'Allemagne et la Grande-Bretagne représentent 12 milliards d'euros.

Les Indiens n'ont pas de compétence dans ce domaine. Les Russes sont compétents en cryptographie mais ne sont pas une référence en matière de cybersécurité. Ils possèdent certaines entreprises de bon niveau, des agences publiques extrêmement bonnes mais ont peu d'envergure et ne sont pas très bien organisés.

M. Jean-Pierre Quémard. – En conclusion**, il y a urgence à agir** dans le domaine de la cybersécurité. 2014 et 2015, constituent le bon moment pour cela.

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS (CLUSIF)

M. Lazaro Pejsachowicz, président du Club de la sécurité de l'information français (CLUSIF)

26 février 2014

Je reviens du Forum international sur la cybercriminalité où j'ai dû introduire huit mots nouveaux dans le glossaire de la cybersécurité. Si je vous parle de cela tout de suite, c'est qu'il existe une espèce de guerre des mots et, derrière cette guerre des mots, se cache une guerre commerciale. Malheureusement, la sécurité se construit dans ce contexte, ce qui complique la comparaison et la compréhension des entreprises, etc. Il faut déjà faire du *marketing* des mots car il faudrait que les gens comprennent ce qu'ils achètent, ce n'est pas facile.

En particulier, le mot à la mode « cyber » est utilisé à toutes les sauces. « cyber » veut dire « électronique » et aussi « extérieur » mais certains utilisent ce mot pour parler de leur contrôle de base interne.

CLUSIF n'est pas une organisation de responsables de sécurité interne des entreprises mais un rassemblement de professionnels de la sécurité qui ambitionnent de mettre en place des solutions de sécurité dans les entreprises et aussi des professionnels de sécurité qui fabriquent des produits, qui les vendent, qui les installent, etc. Tous les types de professionnels de la sécurité sont donc membres du CLUSIF et s'accordent sur le fait que leur mission est que l'entreprise puisse se protéger de la meilleure façon.

Une des raisons pour lesquelles les entreprises ont du mal à se protéger de la meilleure façon, c'est la compréhension des problématiques qui est en partie liée à la compréhension des termes. On parle de cyberespace, de numérique, d'information, etc. Le CLUSIF ne nie pas le phénomène cyber ni la multiplication des moyens par lesquels l'informatique s'exprime. Tout au contraire, on essaie de les appréhender tous mais le cœur de notre préoccupation c'est que les entreprises puissent protéger leurs informations. Le problème de la protection de l'information a été vu trop souvent comme la nécessité de posséder les outils et les prestataires nécessaires pour cette protection. Il faut bien que les entreprises vivent... Mais ça ne se réduit pas à cela. Nous considérons que **les entreprises doivent avoir elles-mêmes les moyens de comprendre comment se protéger**.

De ce point de vue, pour nous, l'arrivée de M. Patrick Pailloux à l'ANSSI est tout à fait positive. Dans le dernier rapport de l'ANSSI, il est écrit : « *Arrêtez d'acheter n'importe quoi ! Maîtrisez ce que vous avez déjà acheté !* ».

On peut se demander si les préoccupations de l'ANSSI sont tout à fait opérationnelles mais c'est l'objectif qui est important. L'entreprise doit pouvoir maîtriser son information. C'est ce que vise le CLUSIF.

Deux études importantes du CLUSIF sortent chaque année : le panorama de la cybercriminalité qui analyse les attaques intervenues au cours de l'année, étudie leurs conséquences du point de vue de la protection des entreprises et donne des perspectives aux entreprises à partir d'exemples d'attaques qui peuvent se généraliser. La deuxième étude porte sur **la menace informatique et la sécurité**. Cette étude consomme près du quart de notre budget ; il s'agit d'une enquête auprès des entreprises, des internautes pour recenser les risques qu'ils ont rencontrés, les incidents, les sinistres en résultant, les mesures mises en place et les pratiques nouvelles à adopter en réaction aux attaques.

Pour le CLUSIF, encore une fois, l'objectif constant est que l'entreprise comprenne elle-même. Certes, des prestataires de services dotés de personnels spécialisés contribuent beaucoup à ce que l'entreprise comprenne mais cela n'est pas suffisant car **il faut que l'entreprise possède elle-même de vrais experts, des budgets de formation et de veille importants**. Lorsqu'il s'agit de protéger l'information, toutes les entreprises n'ont pas les mêmes besoins, les mêmes risques et ne vont pas subir les mêmes attaques ni les mêmes incidents. **Il faut donc cerner les besoins de chaque entreprise à partir d'une analyse interne et pas simplement externe, en recourant à des experts généralistes formés à détecter les risques des entreprises.**

Si je suis si sensible à l'emploi du mot « cyber », c'est simplement parce qu'il est utilisé pour laisser croire qu'il est possible de sortir le risque de l'entreprise, de manière à pouvoir dire ensuite que tout le monde doit faire face au même risque, le cyberrisque, alors que cela est inexact.

Certes, il faut analyser les tendances actuelles, les attaques externes, la criminalité qui s'organise de façon désorganisée. Depuis trois ans, dans les panoramas de la cybercriminalité dressés par le CLUSIF, il a été montré comment s'organisait cette criminalité. C'est quelque chose de très particulier. Nous-mêmes, pendant longtemps, avons parlé des grands criminels, or, aujourd'hui, **on n'a pas besoin d'être grand criminel pour nuire sur Internet. Il s'agit plutôt de coopératives de délinquants** pour chercher un nom de domaine par-ci, un mot de passe par-là, etc., c'est quasiment comme des services. Ce schéma a été mis en évidence à travers des exemples d'attaques. En réalité, **il n'y a pas un grand talent derrière la délinquance informatique qui est à la portée de n'importe qui**.

À propos du recours aux nuages, quand je vais sur *Google*, je ne vais pas dans un nuage mais bien sur *Google*. Le rôle de l'État est de dire que, si vous choisissez d'aller dans un nuage, c'est votre responsabilité. **Quand je stocke des données chez quelqu'un, cette personne doit être responsable de leur sécurité qu'il s'agisse ou non d'un nuage.** Le rôle essentiel de l'État c'est d'indiquer là où on peut stocker et là où on ne peut pas.

En général, personne ne comprend quand on évoque des zones de non droit, or c'est un problème majeur. Pour les Américains ces zones n'existent pas. Si on peut faire confiance, sur certains points, à son fournisseur, il faut garder en tête ce qui est vital pour l'entreprise et, comme c'était déjà le cas à l'époque de l'hébergement, **il est vital pour l'entreprise de garder la maîtrise de ses informations**. Si l'entreprise pense que la sécurité de sa messagerie, son espace collaboratif, n'a pas d'importance pour elle et que l'économie réalisée vaut la peine, le CLUSIF n'intervient pas sur ces appréciations mais s'interroge simplement sur la réalité de l'économie réellement réalisée. La même opinion avait été émise sur les hébergeurs et, par la suite, les entreprises ont été conduites à tout rapatrier constatant d'ailleurs qu'elles ne maîtrisaient plus rien alors que le CLUSIF avait alerté sur le caractère risqué de cet hébergement.

Il faut d'abord que l'entreprise s'interroge sur ce qui est important pour elle, sur ce qui est vital pour continuer à le maîtriser. Une entreprise ne déléguera pas sa politique produit mais ne se rendra pas forcément compte que ses informations ont une importance analogue. L'objectif du CLUSIF c'est que les entreprises comprennent cela par elles-mêmes et conduisent elles-mêmes leurs expertises. À noter qu'il y a des entreprises où les responsables de sécurité ne sont consultés qu'après la mise des informations de l'entreprise à l'extérieur, sur *Google* ou autre, ce qui revient à donner le bâton pour se faire battre. En résumé et de manière générale, on peut externaliser ce qui n'est pas stratégique pour l'entreprise.

En général, **le CLUSIF ne parle pas des attaques sans parler des risques**.

Lorsqu'une entreprise affirme subir dix mille attaques par jour, en réalité, il ne s'agit pas de véritables attaques mais de ce qui a été arrêté par le pare-feu. Le besoin de vendre des outils de sécurité peut conduire à l'emploi d'un tel langage inapproprié. Il ne faut prendre en considération que ce qu'une personne normale appellerait intrusion. Sinon, tout devient grave et alors il est impossible de repérer le risque réel.

Il est réjouissant de voir que **la CNIL a pris comme un coup de jeunesse en parlant maintenant de risque au lieu de parler de mesures dans l'absolu**. La question est de savoir déterminer quand la faille de sécurité est grave et de connaître les solutions à y apporter à ce moment-là. Toute protection est faillible.

C'est pourquoi le CLUSIF émet très peu de recommandations de protection mais conduit plutôt des études de risque en montrant la manière de l'approcher.

La France a mis en œuvre des mesures de sécurité bien avant les autres pays. Quand le CLUSIF a été fondé, il n'y avait d'organisation de sécurité nulle part. Mais, à chaque fois, la France a été rattrapée. En créant la CNIL, la France était également en avance.

Mais il existe tellement de groupes de pressions en action en Europe, qu'il est difficile pour des centres de réflexion dotés de peu de moyens d'imposer des idées raisonnables ; la lutte est inégale. Cependant, demeurent la République et la confiance en l'efficacité de l'État.

La neutralité de l'État devrait être assurée par l'ANSSI, ce qui n'est que partiellement le cas actuellement car **l'ANSSI est obligée de se concentrer sur les opérateurs d'importance vitale (OIV)**. Or toute limitation dans le spectre de l'effort ou également la concentration de très grandes sociétés de services apporte peu à la sécurité. En revanche, **il existe un vivier de petites entreprises de sécurité qui sont une richesse française**.

Par ailleurs, le CLUSIF produit des analyses sur les menaces informatiques et la cybercriminalité, bien d'autres font de même sans pour autant pouvoir satisfaire les besoins des entreprises d'avoir des vrais chiffres permettant une meilleure appréciation du risque. **Seul un Observatoire mis en place par l'État pourrait être un endroit neural où les entreprises déclareraient leurs sinistres numériques sans crainte**. **Il serait souhaitable de pousser l'ANSSI à s'intéresser à la protection des entreprises au-delà des OIV** à propos desquels il faut d'ailleurs souligner certaines limites puisque *Bouygues* est OIV alors que la Caisse nationale d'assurance vieillesse (CNAV) ne l'est pas... Quand je travaillais pour *France Telecom*, j'ai reçu une formation de la DST qui montrait des *scenarii* dans lesquels la CNAV n'arrivait pas à payer les retraites, ce qui pourrait faire vaciller la République bien plus que *Bouygues*.

Certains parlent de l'effet papillon en sécurité et le secteur de la sécurité vit de la croyance en cet effet. À propos des *SCADA*, émerge toute la problématique de la sécurité de l'informatique industrielle ; or ce point central a été négligé.

Par exemple, dans le milieu médical, les appareils de radiologie sont aujourd'hui des ordinateurs et donc à protéger des virus. Les *SCADA* constituent un problème essentiel d'aujourd'hui. L'ANSSI a créé un groupe de travail sur ce thème qui a obtenu des résultats excellents ; ce document est surtout destiné aux gros opérateurs d'importance vitale. De son côté, le CLUSIF a créé un groupe de travail sur les *SCADA* qui visait toutes les autres entreprises. Il faudrait trouver un schéma permettant que l'effet papillon puisse être attaqué.

Face à la cybersécurité, toutes les entreprises et tous les pays sont dans la même situation. On peut citer certaines entreprises qui font des efforts, notamment beaucoup en France et probablement davantage en France qu'à l'étranger. C'est la culture de l'intelligence. On peut citer aussi des entreprises américaines et il existe aussi, en Europe, des organismes analogues au CLUSIF.

Avant de légiférer ou de prendre des décrets, il faut considérer la problématique en cause, comme l'a fait le rapport Lasbordes, prendre conscience des enjeux et élaborer un schéma avec le concours des acteurs pour **faire pénétrer et évoluer la sécurité partout**.

Beaucoup de grandes entreprises ne sont pas sensibilisées à la sécurité.

Je ne suis pas du tout favorable aux guides de bonnes pratiques. L'expertise doit être menée au sein de l'entreprise.

Beaucoup de personnes croient que la cybersécurité est un échec mais des Anglais sont intervenus récemment dans un colloque pour préciser que **lorsqu'on ne fait que de la conformité, on ne fait pas de sécurité**. Beaucoup de guides de bonnes pratiques ont été lancés mais ils sont conçus pour qu'on achète beaucoup de matériel et n'assurent pas la sécurité car ils ne prennent pas en compte les risques particuliers et donc ne préconisent pas vraiment des bonnes pratiques à mettre en œuvre et encore moins de l'expertise. Or **la difficulté est de produire de l'expertise pour l'ensemble des entreprises françaises**. Comment produire, avec l'ANSSI, des réflexions ?

La production d'une méthode d'analyse des risques par la CNIL, ça c'est révolutionnaire parce que cela permet de mettre en œuvre une analyse en rapport avec l'intelligence de l'entreprise concernée. Il faut être concret.

Le Congrès nord-américain a voté une loi interdisant à un dirigeant de société de dire qu'il ne savait pas. Une disposition analogue figurait déjà dans une loi de finances française. Il ne suffit pas d'acheter un matériel pour mettre en œuvre une mesure de bonne pratique, pour être en sécurité et pour pouvoir dire, quand un sinistre survient : « *On ne savait pas* ».

L'objectif est de transformer les intelligences individuelles en intelligence collective.

À ce jour, personne ne s'est amusé à attaquer le système d'information du CLUSIF ; malheureusement, on ne peut pas nous désorganiser de la sorte car notre système n'est pas encore très élaboré. Personne n'accède aux outils de travail collaboratif du CLUSIF. Encore une fois, **la criticité de chaque attaque est propre à chaque entreprise**.

À noter qu'un système rustique n'est pas mauvais. Il ne faut surtout pas démonter un système rustique au nom de l'obsession des gains.

Dans le même sens, peut être cité le cas d'un hôpital dont le système d'information est tombé en panne et qui ne pouvait plus accéder à la liste permettant de signaler qu'un appareil perfectionné ne fonctionnait pas et exigeait une réparation car cette liste elle-même se trouvait sur le système informatique en panne.

CLOUDWATT

M. Cédric Prévost, directeur de la sécurité et de la qualité des programmes

26 février 2014

Cloudwatt est un des deux *clouds* créés dans le cadre des investissements d'avenir, avec trois actionnaires principaux, *Orange, Thales* et la Caisse des dépôts, qui a pour mission de développer une infrastructure informatique en nuage pour fournir des offres de stockage et de capacité de traitement d'un certain nombre d'applications de manière fluide et performante.

En qualité de directeur de la sécurité de *Cloudwatt*, je suis certain que **mettre des données dans le nuage informatique (le *cloud*) augmente le niveau de sécurité**.

Il y a eu énormément d'évolutions dans l'informatique et les télécommunications, ces quinze dernières années, et le nuage représente, d'une certaine manière, l'aboutissement de ces différentes évolutions technologiques.

Aujourd'hui, **maîtriser un système d'information à l'intérieur d'une entreprise devient très complexe et nécessite des compétences extrêmement variées** parce que les utilisateurs veulent accéder, à n'importe quel moment, à l'ensemble de leurs applications, à partir de leur *smartphone*, en nomadisme, quand ils sont à l'étranger, en conférence, etc.

Le modèle du système d'information de l'entreprise, qui auparavant était tourné vers lui-même et maîtrisé par des responsables de l'informatique présents dans l'entreprise depuis plusieurs années, a complètement éclaté. **Désormais les données de l'entreprise sont tournées vers l'extérieur**. Les utilisateurs vont sur Internet, sur leur compte *Facebook* tout en travaillant sur leur logiciel de comptabilité et en échangeant des courriels avec leurs collègues d'un côté et leurs amis de l'autre.

Est alors apparu **un mélange complet entre la sphère professionnelle et la sphère privée** dans une vision complètement tournée vers le monde extérieur.

Les compétences nécessaires pour sécuriser correctement ce type d'infrastructures ne sont plus à la portée de la majorité des entreprises. Les TPE et les PME, voire certaines grandes entreprises, ne peuvent disposer d'un service informatique qui a toutes ces compétences.

Un opérateur de nuage dispose d'équipes d'exploitation disponibles sept jours sur sept et vingt-quatre heures sur vingt-quatre ainsi que d'équipes spécialistes de sécurité en charge de la construction du système informatique de l'infrastructure du nuage et dans la supervision au quotidien de son bon fonctionnement.

Globalement, pour la grande majorité des infrastructures, *Cloudwatt* a correctement réalisé, bien pensé des solutions modernes qui respectent les bonnes pratiques de l'hygiène informatique et de la sécurité offrant ainsi une bien meilleure sécurisation que l'informatique classique d'une entreprise.

En 2013, des spécialistes de la sécurité ont publié des statistiques sur les attaques principales sur les systèmes d'information. **98 % des attaques réussies et rendues publiques ont utilisé des vulnérabilités dont les correctifs étaient connus et exploitables depuis au moins trois ou six mois en moyenne.** Mais il n'y avait pas eu de mises à jour effectuées à temps.

Tout simplement, les équipes internes n'avaient pas réussi à tenir le rythme des mises à jour de sécurité des systèmes d'information alors que les failles en étaient connues.

Dans un espace homogène, par exemple en France, cela a du sens de localiser les données. Cela a probablement moins de sens dans des espaces aux réglementations rigides non homogènes. Cela permet de garantir que les règles juridiques qui s'appliquent aux données restent homogènes et que, s'il y avait un problème avec les fournisseurs, le client saurait avec quelles armes il devrait se battre et vers qui se tourner.

À titre d'exemple, dans l'Union européenne, les notions de propriété des données, de responsabilité, diffèrent d'un État à l'autre. Mais **quand on met ses données chez un opérateur de nuage français, allemand, italien ou espagnol, l'utilisateur est responsable des traitements réalisés sur ses données tandis que, auprès d'un opérateur américain, en vertu de la législation américaine, l'Américain devient propriétaire des données donc, indirectement, il y a transfert de responsabilité**.

Cloudwatt travaille énormément avec l'ANSSI et la CNIL. En effet, l'ANSSI est un acteur majeur en matière d'expertise. De plus, avant de rejoindre *Cloudwatt*, j'ai passé dix ans au ministère de la défense puis ai occupé les fonctions de DSI à la Présidence de la République, donc j'ai eu l'occasion de côtoyer énormément l'ANSSI. J'ai vu un certain nombre d'attaques et ai pris l'habitude de m'appuyer sur l'ANSSI et son expertise pour m'aider à contrer ces attaques.

Maintenant, je profite des possibilités de travailler avec l'ANSSI pour évaluer les infrastructures mises en place par *Cloudwatt* et tenter d'obtenir ses qualifications sur des points permettant d'offrir des garanties de sécurité plus importantes. On est en train de voir comment **mettre en place une certification, un label car il y a beaucoup d'offres de nuage à qualifier pour obtenir un nuage sécurisé**. L'ANSSI réunit des groupes de

travail sur ce thème. La finalisation de ces travaux devrait avoir lieu dans quelques jours.

Cloudwatt s'est fortement investi autour de l'ANSSI pour éditer des règles permettant de guider les clients dans les offres de nuages qui sont nombreuses. D'ailleurs, **tout le monde se dit fournisseur de nuage même si ce n'est pas vraiment le cas**. Il y a un véritable besoin à édicter un certain nombre de règles pour qualifier la qualité, en termes de sécurité au-delà de la confidentialité, il s'agit aussi de la disponibilité et de l'intégrité des données.

Cloudwatt suit beaucoup les travaux de la CNIL avec laquelle il entretient des relations directes sur les données personnelles mais il a aujourd'hui relativement peu d'échanges portant sur les données.

Enfin, le cadre réglementaire résulte tant de la loi relative à l'informatique, aux fichiers et aux libertés que du règlement européen qui est en train d'être revu et à propos duquel on ne sait pas trop quand et comment il va aboutir.

La différence entre hébergement et offre de stockage dans le nuage réside dans les services qui sont fournis. Chez *Cloudwatt*, les services sont facturés à l'usage ; le stockage des données ou l'utilisation des applications ne sont pas facturés au client s'il n'en fait pas usage puisqu'il n'y a pas eu utilisation du stockage ou de la puissance de calcul. À l'inverse, chez un hébergeur, que vous utilisiez ou non le serveur, vous payez. C'est un peu la différence entre un péage d'autoroute qui ne coûte que lorsqu'on circule alors que l'assurance de l'automobile doit être payée qu'on utilise ou non la voiture. Évidemment, globalement, si tous les clients venaient chez *Cloudwatt* et n'utilisaient rien, il y aurait un problème.

De plus, si vous réservez la puissance de cinq serveurs chez un hébergeur et que vous ayez besoin de cinq de plus, il ne peut pas toujours vous donner satisfaction alors que, chez *Cloudwatt*, même si vous en voulez cinquante de plus, potentiellement, vous pourriez les avoir.

C'est plutôt la manière dont on gère le nuage qui fait la différence avec l'hébergement. Quand vous êtes hébergeur, vous allez réserver des serveurs pour un client et, à partir de là, le client accèdera à ces serveurs. L'opérateur de nuage considère que tous les serveurs sont pareils et, à l'instant où vous voulez une machine pour exécuter quelque chose, vous prenez cette machine et on vous l'attribue ; cela est fait de manière complètement dynamique par une sorte de chef d'orchestre qui s'assure que, lorsque le client demande quelque chose, cela fonctionne. Tout cela est parfaitement cloisonné. On s'assure que telle machine récupérée par un client n'interfère pas avec une autre.

Pour le stockage, c'est exactement la même chose. Le client, à tout instant, peut arrêter d'accéder à ses données mais peut néanmoins continuer à être intéressé par les services, par exemple pour faire de l'archivage. Il n'y

a que lui qui puisse accéder à ses données, même s'il ne le fait pas. En fait, les données restent découpées en petits morceaux.

En revanche, si jamais le client a besoin de stockage, à partir du moment où il clôt son compte sans emporter ses données, il peut les récupérer à tout moment. Il dispose même généralement d'environ un mois pour cela après la clôture officielle de son compte. En effet, il arrive que le client ne fasse pas attention, c'est pourquoi *Cloudwatt* ne ferme pas immédiatement l'accès après la clôture du compte.

En fait, **les données sont automatiquement dupliquées pour en conserver l'intégrité et en améliorer les performances**. Quand on supprime des données, on supprime toutes les duplications ; aujourd'hui, **chaque donnée est copiée trois fois**.

Quand on utilise un serveur *web*, ce sont plusieurs serveurs qui sont mobilisés car la requête est redirigée vers un autre serveur et donc, dans ces cas-là, le client va demander que les machines qui remplissent le même rôle ne soient pas physiquement les mêmes afin assurer la continuité du service.

Le centre de stockage des données, le *data center*, de *Cloudwatt,* est situé en Normandie ; d'autres embryons de centres de stockage sont en Île-de-France. Avoir un seul *data center* n'offre pas assez de garanties pour le client.

Les machines et les *racks* sont fabriqués par *Cloudwatt* même si *Orange* est actionnaire.

Cloudwatt a un capital de 225 millions d'euros, dont 100 millions d'euros ont été apportés par *Orange*, 50 millions d'euros par *Thales*, et 75 millions d'euros dans le cadre des investissements d'avenir portés par la Caisse des dépôts.

Créé le 6 septembre 2012, *Cloudwatt* réalise près d'un million d'euros de chiffre d'affaires et plusieurs centaines de millions d'euros sont espérés en 2017 mais ce sera vraisemblablement légèrement inférieur.

En 2013, le marché mondial du nuage numérique ou *Cloud* est estimé à 130 milliards de dollars. En Europe, on est très loin d'avoir atteint les 40 milliards d'euros et même les 20 milliards d'euros. **Le marché européen décolle avec six ou sept ans de retard.**

Dans les entreprises, les personnes ne sont pas assez, voire pas du tout, formées à la sécurité informatique. À titre personnel, j'estime que, au sujet du numérique, la majorité des gens est extrêmement naïve, soit elle sous-estime en fait très largement les véritables menaces soit elle n'a en tête que les entreprises stratégiques, comme celles du secteur nucléaire, mais la situation ne se présente plus du tout de cette façon.

En réalité, depuis cinq à six ans, les menaces constatées proviennent de ***hackers*** qui tentent de casser les systèmes pour le plaisir. Par ailleurs, n'importe quelle société possédant des informations, des brevets un petit

peu sensibles, peut devenir la cible potentielle de ses **concurrents**. Elle peut même être la cible d'**États**, ce qui a été parfaitement illustré par l'affaire Snowden. Plus personne ne peut nier aujourd'hui que, en ce domaine, le gouvernement nord-américain s'est donné pour mission d'aider ses propres entreprises. La France doit faire exactement la même chose.

Il ne faut pas imaginer que la menace ne pèse que sur les grands groupes ou les grands groupes de défense ; **toutes les entreprises sont des cibles de choix. Mais leurs personnels ne sont pas sensibilisés à l'hygiène informatique.** C'est ainsi que, généralement, ils travaillent dans les trains, les avions, devant la machine à café de la pépinière d'entreprises où nombre de personnes ne se connaissent pas ; **les conversations professionnelles se poursuivent dans ces lieux alors que 95 % des gens autour d'un groupe qui parle de son travail sont des inconnus**.

Aujourd'hui, **le réseau *Wi-Fi* est fiable** et ce n'est pas l'aspect le plus inquiétant. À ma connaissance, les techniques de sécurisation du *Wi-Fi* ont un niveau de sécurisation similaire à celui des réseaux mobiles et, en fait, **la sécurisation des échanges dépend du niveau de sécurisation du serveur**. Si votre messagerie d'entreprise n'est pas chiffrée, alors il ne faut pas se connecter ni sur le *Wi-Fi* d'hôtel ni sur votre *Wi-Fi* à la maison et pas plus sur le *Wi-Fi* de l'entreprise s'il est en clair.

À l'inverse, **si vous disposez d'un canal de chiffrement, ce qui est aujourd'hui quasiment la règle, vous pouvez vous connecter sur le Wi-Fi car la sécurité est portée par votre application**.

Cloudwatt aborde la sécurisation de bout en bout, que les échanges passent par des *Wi-Fi* d'aéroports, personnels, ou d'entreprises.

Il y a des récurrences de **changement des clés de chiffrement en suivant notamment les recommandations de l'ANSSI,** très scrupuleusement. Très régulièrement, environ tous les deux ans, ses exigences montent de niveau en fonction de la menace technologique ou des vulnérabilités qui ont été découvertes. Il existe des règles claires.

Déjà, **si les quarante règles de base de l'informatique étaient suivies, on économiserait 95 % des attaques informatiques constatées aujourd'hui**.

Une éducation totale reste à faire pour inculquer une certaine vigilance. **Mieux vaut rater une information pour privilégier la sécurité que de cliquer pour ouvrir un document dont on n'est pas sûr**. D'autant que les attaques aujourd'hui sont beaucoup plus sophistiquées. Avant, les attaques étaient purement des attaques techniques, des virus, etc. ; **aujourd'hui, les seules attaques qui fonctionnent, sont des attaques très sophistiquées qui exploitent des vulnérabilités techniques et ont recours à de l'ingénierie sociale, à des sites *web* corrompus, etc**.

À ce jour, *Cloudwatt* n'a pas été victime d'attaques massives mais, quotidiennement, des attaques ont lieu du fait de personnes qui essaient de casser des mots de passe ce qui se détecte relativement facilement. *Cloudwatt* n'a pas subi non plus d'attaques en déni de service. En revanche, il se prépare à en subir parce qu'on est convaincu que cela ne peut manquer d'arriver même si on n'en connaît pas le moment.

Les attaques en déni de service généralement ne volent pas de données mais cassent le service en empêchant les clients d'y accéder. Ce sont des attaques en aveuglement. **Beaucoup de dispositifs de surveillance comportementale ont été mis en place. La sécurité dans le nuage, c'est une sécurité dynamique.**

Avant, on construisait des sortes de châteaux forts pour protéger l'informatique alors que, aujourd'hui, on en est plutôt à répartir partout au sein de l'architecture des modèles de chien de garde qui tournent de manière aléatoire au cas où quelqu'un serait parvenu à rentrer et, donc, on a comme des chiens partout et on est à l'écoute de n'importe quel aboiement qui permet d'aller vérifier s'il se passe quelque chose.

Chez *Cloudwatt*, nous sommes une centaine ; 70 % des personnes ont des profils techniques comme celui d'ingénieur système et les 25 % autres – pourcentage en train de décroître – constituent la couche administrative, l'encadrement.

Entre les sociétés analogues et *Cloudwatt*, la concurrence est très frontale. Il existe trois acteurs américains principaux dont *Amazon* qui est le *leader* du marché et dont le chiffre d'affaires est supérieur à celui des quinze concurrents qui le suivent dans le classement. *Amazon* a démarré il y a sept ans et c'est lui qui a créé le marché du nuage. Il a trois ans d'avance sur tous les autres. Personne ne pensait que ça allait marcher.

Lorsqu'*Amazon* s'est lancé, il a été obligé de surdimensionner ses effectifs, de les multiplier par dix pour absorber les pics de vente de Noël. Puis l'idée a germé d'utiliser les 90 % de cette capacité qui étaient inutilisés en la mettant à la disposition d'entreprises. Ses concurrents principaux sont les trois grosses sociétés américaines mais il y a aussi des concurrents sur le marché français, comme *Numergy*, le second nuage souverain, *OVH* et un peu *Orange*. On constate que, actuellement, **la concurrence se fait entre les acteurs européens et les acteurs américains qui ont une stratégie très claire consistant à étouffer le marché en baissant les prix pour éviter l'émergence de concurrents européens**.

Le sujet des noms de domaine a été porté par le ministre de l'industrie, notamment lors du dernier forum tenu à Séoul. Au niveau de *Cloudwatt*, le fait que l'*ICANN* soit une société de droit américain n'est pas de nature à nous traumatiser pour plusieurs raisons. D'abord parce que les Américains changent pas mal de discours depuis deux ans ; ils sont plus attentifs à ce que disent les autres acteurs. Les États-Unis d'Amérique

commencent à entendre l'inquiétude d'être mis sous contrôle et donc ils ont vu la nécessité d'ouvrir des discussions.

Il y a trois jours, le président de l'*ICANN* était en France et a exposé sa vision pour sortir du droit américain et s'implanter à Genève au lieu de New York. **Les noms de domaine aujourd'hui, sont une denrée essentielle au fonctionnement du *web*.**

L'*ICANN* fixe les règles selon lesquelles les noms de domaine sont attribués. Si les Américains se mettaient à déraper en ce domaine, il y aurait très rapidement un contre-feu alternatif car il y a tellement de monde, tellement de services sur Internet, que personne ne peut plus se permettre de bloquer le système.

Les actionnaires de *Cloudwatt* ont choisi de partir d'une feuille blanche, de construire totalement leur architecture et leurs offres sur des bases modernes, à **partir des meilleures pratiques de sécurité prônées par *Cloud Security Alliance*, qui est une association internationale, par l'*ENISA*, l'ANSSI, la CNIL, le CLUSIF, etc**.

L'autre choix n'a pas été celui d'une certaine **souveraineté franco-française** car la souveraineté vue par les Allemands n'est pas la souveraineté française**. *Cloudwatt* a plutôt souhaité donner à ses clients la maîtrise de ce qui se passe sur leurs données et le traitement de celles-ci.** On garantit l'interopérabilité du système, la réversibilité n'importe quand, sans aucune autorisation. Dès que le client s'arrête d'utiliser le service, il ne doit plus rien. Troisièmement, on garantit aussi **la localisation en France** et donc la **garantie de la soumission à la législation française et européenne**. L'autre aspect de la souveraineté, c'est que **l'on fabrique nous-mêmes**. **L'ensemble de l'architecture est construite par *Cloudwatt* avec des technologies « *open source* »**. Personne ne peut nous imposer de changer tel ou tel élément, de relever des tarifs quelconques. **Chacun doit maîtriser 100 % de la destinée de son système. C'est aussi cela la souveraineté.**

Il n'y a pas de compagnie d'assurance qui assure le nuage. Nous avons fait en sorte que l'architecture devra empêcher que tout le système tombe en panne d'un coup. Notamment grâce à la « **triplication » des données dans des endroits différents**. Même si un avion s'écrasait sur un centre de données, cela ne suffirait pas à mettre à bas l'organisation du système.

À noter que nos actionnaires sont aussi nos clients.

La Poste propose aussi ce type de services mais elle peut utiliser ceux de *Cloudwatt,* si elle le souhaite.

Il y a aussi le label de la CNIL sur le coffre-fort électronique. Cette initiative est très intéressante car elle permet de fournir à nos clients des éléments de qualification par des tiers externes qui sont des **tiers de confiance**. L'ANSSI est pour nous le garant objectif pour confirmer à nos

clients qu'on ne fait pas n'importe quoi. La CNIL est également un garant. Entrer dans le cadre de ce type de label, de certification, par des acteurs reconnus, est essentiel pour *Cloudwatt* d'autant que cela crée un vrai référencement, une vraie distinction d'avec **les opérateurs américains qui ne pourront jamais garantir la même chose**. En effet, leurs centres de données sont localisés aux États-Unis où toutes les exigences ne sont pas respectées.

Ainsi, il est possible de mettre en avant les offres européennes. La localisation en Europe ne pourra peut-être pas être imposée par la loi.

Mais les clients ont confiance en un certain nombre d'acteurs. La CNIL en est un et la mise en place d'un label CNIL ainsi que la sensibilisation des clients et l'évangélisation autour d'un certain nombre de points de vigilance sont absolument fondamentales. Cela permet d'éliminer un certain nombre d'offres qui ne répondent pas à ces critères. **Ces labels peuvent être mis en avant par la puissance publique même s'ils ne peuvent être exigés** car ce ne serait pas conforme au code des marchés publics.

CONSEIL NATIONAL DU NUMÉRIQUE (CNNUM)

M. Serge Abiteboul, membre du Conseil

M. Jean-Baptiste Soufron, secrétaire général

27 février 2014

M. Serge Abiteboul. – Je suis membre du Conseil national du numérique et directeur de recherche à l'INRIA et à l'École normale supérieure de Cachan (laboratoire LSV). Je suis un chercheur en informatique.

M. Serge Abiteboul. – La question de la sécurité a émergé une première fois à propos de la neutralité des réseaux qui a été le thème du premier avis du Conseil national du numérique, ensuite, lorsque le conseil a traité des plates-formes puis à l'occasion des questions d'éducation et, enfin, dans le rapport sur l'inclusion.

La sécurité numérique est également apparue dans les questions d'économie du numérique, à savoir dans les rapports de force entre les entreprises françaises et étrangères, également dans les questions d'éducation générale des gens au numérique et à propos du **besoin de construire un rapport quotidien au numérique qui soit plus informé et mieux structuré**.

Le Conseil national du numérique va maintenant s'intéresser davantage à la sécurité dans la mesure où il devait être saisi dans le cadre d'une concertation sur le futur projet de loi numérique pour recueillir l'avis de la société civile avant le dépôt du projet de loi. Le Conseil va monter en puissance sur ce thème.

À propos de la souveraineté numérique, sujet à la fois complexe et délicat, **quasiment toutes les grandes plates-formes qui gèrent les données se situent à l'étranger, en particulier aux États-Unis d'Amérique**. La question de la souveraineté nationale est donc posée à travers des aspects de renseignement et d'intelligence au sens large, au niveau économique également car beaucoup de valeur ajoutée passe maintenant par ces plates-formes puisque les clients des grandes entreprises transitent par elles ; **les grandes entreprises européennes perdent le contact direct avec leurs clients et donc des parts de marché**. Ce n'est pas une surprise si des pays comme la Chine ont décidé de développer leurs propres plates-formes.

M. Jean-Baptiste Soufron. – Le Conseil n'a pas encore rendu son rapport sur les plates-formes ; il travaille dessus depuis six mois et, déjà, il commence à apparaître que la situation européenne est pathologique ou, au moins, anormale.

Si l'on prend l'exemple de la Chine, on objectera que la Chine n'est pas une démocratie. Mais avec l'exemple du Japon, de la Corée du Sud ou de la Russie, et d'encore beaucoup de pays étrangers, il apparaît qu'ils ont su maintenir les entreprises et des moyens d'actions locaux qui permettent de conserver la majorité du marché local. Au Japon *Google* possède une part de marché d'environ 20 % à 30 %, de même en Corée du Sud ; c'est encore plus faible en Russie. Pour la vente en ligne et la fonction de service, c'est la même chose au Japon. **En France, la part de marché de *Google* en activité de recherches est de 90 %**.

En France, il y a des secteurs où les spécificités françaises demeurent en matière de services mais la situation est tout de même différente de celle du reste du monde. D'ailleurs, **c'est d'Europe que les sociétés étrangères tirent la majorité de leurs revenus**. Les grandes sociétés de services sur l'Internet sont nord-américaines mais ont des activités européennes et réalisent l'essentiel de leurs bénéfices dans l'Union européenne. Quand vous êtes une entreprise étrangère et que vous arrivez en Europe, vous développez naturellement vos bases d'ancrage dans plusieurs pays au lieu de partir d'un pays européen puis de vous implanter progressivement dans vingt-huit autres.

Autre exemple, celui de la barrière linguistique. Il est plus compliqué pour les entreprises de se développer dans les pays qui possèdent un système linguistique totalement différent. Au Brésil, ce n'est pas le cas mais il est à noter que cette complexité n'est que de démarrage et ne saurait justifier l'inaction.

Si l'on regarde la façon dont fonctionnent les services ou les sites *web* coréens, ils sont totalement différents des sites européens ou américains dans leur *design*, leur forme, leur structuration, leur compréhension du client, leur logique. Ce qui signifie que les Coréens ont su créer une valeur ajoutée locale, peut-être sous la pression de leurs consommateurs locaux alors que l'Europe n'a pas su faire de même.

M. Serge Abiteboul. – Tout le numérique s'est développé extrêmement rapidement et manque d'indicateurs pour analyser les situations.

M. Jean-Baptiste Soufron. – Le projet de loi sur le numérique est prévu pour le second semestre de cette année avec une concertation allant du mois de mars au mois de juillet 2014.

Le Conseil du numérique s'interroge sur les obligations en matière de notifications à l'Union européenne et aux autres pays européens quant aux aspects qui devraient être traités au niveau européen ou international.

De toute manière, le Conseil a indiqué que la concertation devrait comprendre un volet international, un volet européen et un volet national.

M. Serge Abiteboul. – La question de la confiance à accorder au stockage de données dans les nuages numériques conduit à des réponses très nuancées. En effet, il y a plusieurs façons de placer ses données dans des nuages numériques, c'est-à-dire sur un serveur, éventuellement près de chez soi mais, ce qui est important, c'est qu'il soit accessible de partout sur Internet. Dès ce moment-là, il y a des risques d'accès de personnes non désirées.

Dans le cas d'une petite entreprise plaçant ses données dans un nuage, le contrat conclu avec l'hébergeur mentionne que personne d'autre qu'elle-même n'a le droit de voir les données confiées. Si cela advenait, l'entreprise pourrait poursuivre l'hébergeur en justice.

À l'autre bout du spectre, vous choisissez de mettre vos données chez *Facebook* ou *Google mail* et vous ne payez rien mais il faut être conscient que, **si le service est gratuit, cela signifie que le profit est ailleurs**. En réalité**, c'est en monétisant les informations placées dans le nuage que des profits sont dégagés. Le prix à payer par l'utilisateur du nuage est la perte du contrôle sur ses données et le fait de les laisser à disposition.** Certes, chacun est supposé propriétaire de ses données sur *Facebook* mais autorise l'utilisation de ses données par *Facebook* notamment pour des analyses de son profil. De plus, ces données sont tout de même utilisées pour effectuer des analyses de données, de résultats, de tendances.

Il faut toujours se demander : qui paie pour le stockage ? Qui paie pour les applications ? Peut-on contrôler la confidentialité de données dans le nuage ?

C'est un problème de sécurisation des communications et des données. Des techniques de type cryptographique peuvent protéger raisonnablement. Mais, pour limiter le coût, on choisit des niveaux de cryptographie relativement bas qui sont probablement cassables par des techniques assez simples. **Selon les niveaux de cryptographies, le prix de la protection sera plus ou moins élevé.**

Le plus souvent, les faiblesses du système ne sont pas dans la cryptographie, car des cryptages très sophistiqués existent, mais dans les protocoles autour de celle-ci. Par exemple, comment peut-on accéder à vos données partout dans le monde ? Comme l'application doit récupérer une clé, tout un paquet de messages passent à cette occasion et cela risque d'être récupéré. C'est là où va se situer la faiblesse.

M. Jean-Baptiste Soufron. – Ce qu'il faut bien voir, c'est la différence entre le payant et le gratuit. D'un côté, le modèle gratuit repose sur des systèmes multifaces où les données sont peu sécurisées et, de l'autre, avec le modèle payant, le prestataire engage sa responsabilité.

C'est une piste que le Conseil du numérique a vu se dessiner à travers ses études sur la neutralité des plates-formes ou des réseaux. En fait, un effet de seuil va jouer pour l'entreprise qui propose ses services. En effet, **à partir d'un certain seuil, la plate-forme n'est plus seulement votre prestataire de services mais devient une infrastructure indispensable. À ce stade, une inversion totale se produit affectant la façon dont vos données vont être protégées ou utilisées et cela vous échappe de plus en plus.**

M. Serge Abiteboul. – Pour revenir à la souveraineté, il faut aussi souligner que, **à partir du moment où vous mettez vos données sur une plate-forme nord-américaine, vous êtes soumis à la loi américaine**. **Vos données peuvent alors être regardées sans qu'il y ait aucun contrôle des juges.** On peut estimer que le gouvernement américain ne va pas regarder ce que font les entreprises françaises mais, depuis le *Patriot Act*, et tout ce qui a constitué l'affaire *Prism*, cela est possible.

M. Jean-Baptiste Soufron. – Tout le monde est d'accord pour que le *Patriot Act* protège du terrorisme mais la question sur laquelle il faut s'arrêter c'est de se demander si ces regards autorisés sont organisés par un juge pour lutter contre le terrorisme ou bien si cela est possible à un fonctionnaire aux visées inconnues.

Il faut distinguer trois choses. D'abord la situation actuelle de mise en place des écoutes aux États-Unis parce que les données y sont présentes et où **personne ne se pose la question de la légalité des écoutes faites**. Si l'on regarde dans le détail, les pistes légales sont limitées.

Deuxièmement, le rapport demandé par le président Obama à un groupe d'experts a été décrié par la presse française mais, en réalité, ce rapport est assez remarquable. Parmi ses auteurs, figure notamment un grand constitutionnaliste américain. **Le rapport propose une régulation des écoutes au niveau international et territorial.** Ces pistes vont dans la bonne direction car elles sont à la fois favorables au monde des affaires, aux citoyens et elles permettent à l'administration de fonctionner. Ce rapport est très intéressant, très lourd. De plus, le président Obama semble avoir repris ce rapport à son compte même si, à l'heure actuelle, les personnes qui ont analysé ce rapport sont déçues de l'usage qui en a été fait. Mais le dialogue est en cours et **la prise de conscience s'accélère**.

L'avis du Conseil national du numérique sur la loi de programmation militaire a recommandé des concertations plus larges au niveau de la société civile puisqu'à la fois l'industrie, la recherche et la démocratie étaient concernées.

Deuxièmement, les règles internationales sur ce sujet sont relativement faibles, peu claires et, sans même aller jusqu'aux règles qui régissent l'espionnage entre États, **les règles relatives au droit applicable et au tribunal compétent en cas de litige relatif à la vie privée ne sont pas d'une grande clarté**. Ces sujets n'ont pas été vraiment abordés au niveau

international sauf la question de la gouvernance internationale, par exemple celle des noms de domaine.

Le Conseil national du numérique a appelé à la mise en place d'un traité international.

M. Serge Abiteboul. – À titre privé, j'estime que la loi de programmation militaire est pour le moins **ambiguë et dangereuse pour les libertés**.

Ce qui peut être inquiétant, c'est que, sans passer par un juge, il soit possible de commander à des fournisseurs de services Internet de se livrer à des écoutes – ce qui est prévu par la loi de programmation militaire.

Il faut se méfier des réponses simplistes. Il ne faut pas qu'un texte de loi puisse être compris de plusieurs manières.

M. Jean-Baptiste Soufron. – Le Conseil national du numérique invite toujours l'ANSSI et la CNIL à venir participer à ses travaux mais, pour l'instant, **le Conseil n'a pas vraiment travaillé sur la sécurité numérique**.

La CNIL travaille plutôt dans un esprit européen de protection des données qui a des avantages par rapport ce qui se pratique dans les pays anglo-saxons. En revanche, **il semblerait que la CNIL n'ait pas du tout réfléchi à la neutralité des réseaux ou des plates-formes**.

M. Serge Abiteboul. – Sur l'*open data*, le Conseil ne s'est pas exprimé mais a été auditionné par le sénateur Gaëtan Gorce, il y a quelques semaines, et, du point de vue du Conseil**, il n'y a pas d'opposition entre protection de la vie privée et protection de l'information publique**, au contraire.

Depuis longtemps, la CNIL est très axée sur la problématique des libertés fondamentales et **il serait souhaitable que soient développées quelque part des expertises sur le modèle économique des données**, que ce soit à la CNIL ou ailleurs.

Nous connaissons bien la CNIL mais nous avons une mauvaise connaissance des modèles alternatifs qui existent ailleurs, par exemple en Californie, en Allemagne – où les valeurs sur la protection des données sont très similaires à celles de la France mais où le système d'organisation est très différent. En effet, chaque länder dispose d'une sorte de CNIL locale.

À noter que cela fait un moment qu'il est question de renforcer le dispositif de la CNIL, aussi bien en termes de moyens que de champ de compétence.

M. Jean-Baptiste Soufron. – L'*open data* peut se réaliser en conservant les données privées. La protection des données ne saurait être une excuse pour ne pas publier des données publiques. Ayant été auditionnés, il y a peu de temps, par le Sénat, nous avions émis des propositions quant aux données qui ne doivent pas être diffusées et, plutôt que de faire de la CADA une structure qui répond au citoyen, il faudrait voir

pourquoi l'administration refuse de communiquer ses données et, alors, la CADA pourrait être saisie. Dans ce sens, cela changerait complètement la perception et le rôle de de la CADA qui est aujourd'hui une sorte de filtre entre les citoyens et l'administration.

Mais cette proposition mériterait d'être travaillée car il n'y a pas encore assez de propositions à mettre en balance les unes par rapport aux autres pour prendre une décision.

M. Serge Abiteboul. – Il serait intéressant que le Conseil national puisse travailler sur l'*open data* et les données personnelles.

Quoique pressé par des saisines, le Conseil national du numérique n'a pas été saisi sur ces sujets-là. Cependant, depuis l'origine, le Conseil est doté d'un pouvoir d'autosaisine qu'il n'a pas encore beaucoup utilisé, notamment pas sur les données personnelles.

Le Conseil a travaillé sur la neutralité des réseaux, la fiscalité de l'Internet, la concurrence et la neutralité des plates-formes, la loi de programmation militaire (autosaisine), le projet de loi égalité femmes-hommes, la proposition de loi de lutte contre le proxénétisme, le rapport inclusion, le rapport éducation, la santé.

M. Jean-Baptiste Soufron. – Le Conseil national est composé de trente membres bénévoles (un tiers de chercheurs, un tiers de représentants de la société civile, un tiers de représentants d'entreprises). Il s'appuie sur une micro administration de quatre personnes au secrétariat général et quelques stagiaires ; le Conseil n'a pas encore fêté sa première année d'existence.

Le Conseil réagit beaucoup à l'actualité. D'ailleurs, le Conseil avait réclamé une grande loi sur le numérique parce que, jusqu'alors, ce sujet était abordé de manière extrêmement éparse. Finalement cette grande loi arrive et, dans cette mesure, cela peut-il encore se justifier de s'autosaisir sur le sujet essentiel des données personnelles ?

Au-delà de l'axe des données personnelles, **l'axe des données économiques n'a pas encore été vraiment abordé**. Des expérimentations ont lieu, en France et dans le monde, mais il n'y a pas encore suffisamment de recul pour pouvoir traiter ce thème.

Quant à l'axe relatif aux données personnelles et à la protection de la vie privée, il a fallu plusieurs années pour que le public s'y intéresse. Cela a commencé par un scandale à Bercy, en 1974, avec le projet *Safari* relatif à la prévention anti-fraude quand quatre fonctionnaires du ministère des finances ont écrit un article dans *Le Monde*, sous pseudonyme, pour dénoncer ce mécanisme de croisement de données en l'absence de toute règle.

À l'époque, il est à souligner que la réponse française à ce scandale n'a pas été de lancer un mandat d'arrêt international contre ces quatre lanceurs d'alerte, à l'inverse de ce qui est advenu pour Snowden. La réaction

a consisté à lancer une mission d'enquête parlementaire suivie d'un projet de loi qui a entraîné la création de la CNIL et le vote de la loi de 1978 imposant l'autorisation préalable, l'accès aux données, la rectification de données, la suppression de données, etc.

Ces logiques sont devenues automatiques dans l'esprit des citoyens et des dirigeants mais quarante ans plus tard.

Aujourd'hui, quand une entreprise utilise des données commerciales, numériques, ce ne sont pas forcément des données personnelles mais des profils types. À partir de là, on connaît les goûts des personnes qui permettent de leur adresser des publicités en rapport avec ceux-ci mais sans que l'identification ait eu lieu.

En parallèle, les entreprises et les citoyens qui travaillent sur ces sujets ont commencé à élaborer des modes de régulation et de responsabilisation assez surprenants. Par exemple, quand les publicités s'affichent sur Internet, souvent un tout petit bouton situé en haut à gauche permet d'ouvrir un lien qui explique pourquoi cette publicité vous a été adressée. Un avis sur la publicité et son utilité est alors demandé… ce qui est encore une façon d'obtenir une information supplémentaire.

Si vous auditionnez M. Daniel Kaplan, membre du Conseil national du numérique, il vous expliquera la façon dont on met en place des mécanismes de gestion fine de données pour le citoyen appelé à préciser le type de données qu'il accepte de partager.

M. Serge Abiteboul. – De manière générale, **les gens ne sont pas informés de la protection des données et de ce qu'ils devraient ou pourraient faire.**

Quant aux moyens d'y remédier, c'est particulièrement critique dans les petites entreprises, les PME. Les grands groupes, eux, peuvent se payer une entreprise spécialisée qui peut les sécuriser très bien mais pour un coût important alors qu'une PME ne peut se payer un spécialiste de la sécurité. D'une certaine façon, **une PME constitue une cible facile pour des cyberattaques**. Quand une cyberattaque se produit, **la PME ne sait pas forcément comment réagir** ; cela peut donc être difficile et traumatisant pour elle.

De plus, **comme la PME ne sait pas à qui s'adresser, l'État pourrait l'aider**. Car c'est difficile de trouver un expert en sécurité qui vienne juste analyser le problème, voir ce qui s'est passé. **La plupart du temps, les personnes ne sont pas du tout capables de comprendre ce qui est advenu.** Il est probable qu'elles ne disposaient pas de la protection souhaitée et n'ont pas compris vraiment ce qui s'est passé pendant l'attaque. Les PME n'ont pas encore ce genre de culture alors que les grandes entreprises savent mieux se protéger.

M. Jean-Baptiste Soufron. – Quant au cadre juridique international, il faut évoquer le Traité transatlantique de libre-échange. **Ce traité comprend une partie numérique qui est aujourd'hui complètement sous-estimée par ceux qui négocient ce traité.** Plus on creuse, plus on se rend compte que ce point est essentiel dans ce texte qui contient de nombreux nouveaux concepts qui sont poussés dans la négociation et, parmi ceux-ci, il en est qui visent à **anéantir la possibilité pour les Européens de réguler les données**.

Le principe phare pour les Américains c'est **le *free flow information*, le libre échange des données entre pays.** À leurs yeux, tout ce qui le ralentit ou l'empêche doit être écarté. Devraient donc être écartées beaucoup de lois nationales et les clauses de compétence car seul le contrat qui vous lie à l'entreprise détermine l'autorité arbitrale ou le tribunal compétent dans le pays de l'entreprise.

De même, en matière de marchés, si un État, des entreprises françaises ou européennes choisissent un prestataire pour localiser et stocker leurs informations, un tel marché pourrait être contesté au titre du traité.

Pour la politique de données des entreprises, le problème réside en partie dans un manque de préconisations. **Un des risques numériques, très sous-estimé aujourd'hui, est la négociation sans précaution du traité de libre-échange transatlantique**, même si ce n'est probablement pas le risque principal pour les entreprises.

Peut-on abandonner toute souveraineté ? Dans la négociation sur la partie numérique du traité, il existe une différence d'énergie entre les États-Unis et l'Europe. Il serait sans doute nécessaire d'intégrer ce point dans les travaux de l'Office, d'autant que les négociations vont durer quelques années.

C'est un des paradoxes du règlement sur les données au niveau européen car, **dans le cadre de la négociation du programme transatlantique de libre-échange, c'est peut-être plus intéressant de les conduire en s'appuyant sur ce règlement que de se présenter sans.**

M. Serge Abiteboul. – Je suis déjà venu au Sénat pour une autre réunion sur les risques du numérique. L'Office considère-t-il aussi les opportunités offertes par le numérique ?

Il faut se demander ce que pourrait être **une loi protégeant mieux les entreprises** et aussi **aborder la question par une approche des opportunités**. Que faut-il faire pour aider les entreprises, pour les aider à développer de nouveaux modèles d'affaires ?

On travaille beaucoup sur les systèmes d'information personnels. Plutôt que de céder vos informations à de grandes entreprises qui sont plutôt américaines et perdre un peu le contrôle de vos données, ne serait-il pas possible d'avoir un modèle dans lequel il soit possible de **contrôler son information chez un prestataire européen** qui va protéger vos données,

s'occuper des relations que vous avez avec toutes les personnes qui vous vendent des choses ? Cette approche ne serait plus seulement défensive mais bien plutôt constructive.

M. Jean-Baptiste Soufron. – Deux entreprises françaises, *Lima* et *Cosy Cloud*, se sont montées pour proposer des solutions dans le nuage numérique. *Lima c*ommercialise un boîtier à placer au dos de votre *Freebox* et incluant un disque dur ; avec ce dispositif, vous avez votre petit nuage de stockages de données personnelles. Quant à *Cosy Cloud*, ce site permet d'accéder à des services documentaires et de les stocker directement chez vous. Cela change complètement le rapport à la propriété des données pour l'entreprise, au contrôle des données etc. C'est peut-être aussi là que se situent les opportunités de marché.

Ces entreprises font partie de la filière sécurité fait partie des trente-quatre plans du ministère du redressement productif.

Il faut accepter de se protéger mais ne pas rester bloqué sur cette protection.

FÉDÉRATION FRANÇAISE DES TÉLÉCOMS (FFT)

M. Yves Le Mouël, directeur général de la Fédération française des télécoms

M. Jean-Luc Moliner, président de la commission sécurité de la Fédération française des télécoms

M. Pierre-Yves Lavallade, directeur général adjoint, Fédération française des télécoms

27 février 2014

M. Yves Le Mouël. – Le Premier ministre a présenté tout récemment une série de mesures lors de sa visite à l'ANSSI. Un engagement a été donné et reçu par les opérateurs notamment d'**avoir des offres de messageries nationales qui soient sécurisées**, chiffrées, avec des messages électroniques transitant ou étant stockés sur des serveurs situés sur le territoire national. Les opérateurs se sont attelés à cette problématique et tout cela nous paraît aller dans le bon sens.

On a vu aussi qu'il y avait une avancée importante entre l'Allemagne et la France sur ces sujets-là et nous sommes en relation avec nos collègues allemands, nous regardons comment cela se déroule dans leur propre pays. Tout cela est positif car la sécurité n'a pas de frontières. Il faut se serrer les coudes si l'on veut essayer de faire barrage à ces attaques potentielles.

Nous sommes en relation assez régulières avec la CNIL sur différents éléments qui concernent non seulement les aspects sécurité mais, globalement, la relation que le citoyen peut avoir avec la numérisation de la société et on participe aux travaux de la CNIL sur ces différents aspects.

À l'heure actuelle, ce qui est important dans les projets de législation, c'est l'approche de la législation sur les données personnelles qui vise à harmoniser les modalités de traitement de ces données dans l'Union européenne et encadrer le transfert de ces données en direction des États tiers. Là encore, on a des problématiques de concurrence avec les entreprises extra-européennes, ce qui constitue pour nous un combat quotidien. De même, des aspects de fiscalité et de sécurité, des réglementations sont également à l'ordre du jour vis-à-vis de ces acteurs mondiaux ; notamment la problématique du statut du *Safe Harbor* qui est en jeu dans ce cadre-là, vis-à-vis de tous les utilisateurs de nos réseaux, de tous ceux qui mettent sur ces réseaux leurs données personnelles.

L'autre projet important à nos yeux est le projet de loi numérique qui permettra d'adapter la législation nationale sur le numérique à la révolution *data*, à la globalisation des échanges de données, avec un équilibre à conserver quant aux libertés fondamentales de nos concitoyens. Jusqu'où doit-on aller ? Jusqu'où peut-on aller ? Il ne faut pas qu'il y ait de rejets dans ce domaine-là. Il y a des éléments extrêmement sensibles sur ces sujets ; des organisations, des associations sont très vigilantes sur ces points ou sur ce qui peut apparaître comme un problème posé par telle ou telle orientation législative ou réglementaire.

On a aussi en ligne de mire l'évolution de toute la numérisation de notre société à travers le développement et le déploiement des objets connectés. Au salon de Barcelone, *GSMA*, il a été relevé que le marché des objets connectés se chiffre en dizaines de milliards. Il va falloir les gérer car ces objets seront en relation et donneront des informations sur la localisation et, éventuellement, sur un certain nombre de données qu'ils seront capables de capter sur les personnes ou sur les situations auxquelles sont confrontées ces personnes ou les objets qui les représentent. On est dans cette problématique face à quelque chose qu'il faut essayer d'anticiper et de gérer au plan national et également sur un plan beaucoup plus large. Pour nous, la façon de gérer passe par différentes définitions de protocoles qui sont importants ensuite à mettre en œuvre et à gérer d'où une responsabilisation grandissante des opérateurs.

La question centrale reste la mise en place du cadre européen unifié favorable à la sécurisation des données des citoyens européens avec cette problématique de la question de l'asymétrie réglementaire entre les entreprises nationales et les entreprises extra-européennes, mondiales, qui ont souvent une vision assez différente de la nôtre sur ces différents chapitres.

En résumé, trois priorités apparaissent pour l'entreprise : les problématiques de simplification. On sait que c'est au cœur des préoccupations actuelles des pouvoirs publics et il est clair que plus on rentre dans le souhait de vouloir réglementer et organiser, etc., plus on risque, au contraire, la complexification dans la mise en œuvre de différentes orientations. On est toujours soucieux de préserver cet équilibre entre l'objectif que l'on à atteindre, que l'on partage, qui est celui de la sécurité et de la sécurisation des installations, des transmissions etc., et le souci de simplification avec lequel on est déjà dans une problématique extrêmement lourde de gestion de différentes activités.

Le deuxième point, évoqué précédemment, est l'équité de traitement entre les acteurs nationaux et les acteurs mondiaux. Très souvent, ce que l'on perçoit c'est que, lorsque l'on veut gérer un problème, même si cela part de bons sentiments, on met en place une réglementation ou une législation qui s'adapte parfaitement aux acteurs nationaux, voire européens, qui sont soumis à cette réglementation tandis que les acteurs non européens ne

tombent pas, du fait de leur statut, sous le coup de cette législation. En conséquence, on charge de boulets supplémentaires les acteurs nationaux alors que ceux qui seraient visés, notamment par ces tentatives de législation, échappent à ces règles-là parce qu'ils n'ont pas les mêmes statuts, parce qu'ils n'ont pas les mêmes contraintes que les acteurs nationaux. Cela constitue un vrai souci aujourd'hui qui dépasse la France, qui est européen.

Autre souci que l'on a aussi, c'est cet équilibre entre les préoccupations du consommateur, du citoyen et les préoccupations de l'entreprise. Il faut que l'on arrive à trouver un équilibre de façon à ce que les citoyens ne soient pas pris dans cette loi du contrôle permanent qu'ils peuvent rejeter et qui les rendrait prisonniers de leur propre identité sur le numérique. En même temps, les entreprises doivent être aussi dans une situation qui ne soit pas pleine de contraintes excessives pour elles.

Quant aux autres aspects concernant vraiment les entreprises, la Fédération est un peu plus mal à l'aise pour y répondre mais c'est peut-être *Orange* qui pourra en parler.

Ce que l'on sait sur les entreprises et l'information du personnel au sein de ces entreprises, c'est que, aujourd'hui, très précisément, **chaque opérateur délivre des consignes extrêmement strictes pour chacun de ses collaborateurs sur les règles à respecter en matière de sécurité des données de l'entreprise** et il y a deux positions par rapport à l'usage d'Internet. Tout ce qui se passe sur l'Intranet de l'entreprise est très protégé mais les collaborateurs, de plus en plus, y ont accès pas seulement depuis l'entreprise mais aussi quand ils sont à l'extérieur. Il y a des consignes très strictes qui sont mises en œuvre pour cet accès sécurisé *via* des *Virtual Private Network (VPN)* ou autres. Tout cela fait partie de la politique de l'entreprise.

Il y a aussi un autre aspect des choses qui est l'intrusion de l'Internet au sein de l'entreprise. Il est difficile de priver certains collaborateurs de l'accès à Internet. Il faut donc aussi sécuriser cet accès Internet pour éviter d'ouvrir une faille de sécurité dans ce dispositif.

M. Jean-Luc Moliner, président de la commission sécurité de la Fédération française des télécoms. – Pour **certaines entreprises de télécoms considérées comme des entreprises d'importance vitale**, c'est le cas d'***Orange***, il y a des contraintes nouvelles qui apparaissent. Toute la population dite des administrateurs dispose de postes de travail qui ne sont reliés ni à la messagerie ni à Internet. Cela signifie qu'il leur faut un ordinateur portable spécifique pour intervenir sur un système à distance. S'agissant de la messagerie, ce que reconnaît aujourd'hui la législation, c'est que l'on peut utiliser son adresse personnelle au sein de l'entreprise pour envoyer un courriel personnel. Le courriel est considéré comme personnel dès lors que figure un intitulé dans l'objet précisant qu'il s'agit d'un message personnel. Des procédures existent pour permettre d'avoir des espaces dans lesquels ce qui est identifié comme étant personnel est interdit d'accès à l'entreprise.

Des procédures internes permettent de le garantir. Chacun a un dossier qui s'appelle « *personnel* » dans le disque dur et ce dossier est considéré comme étant inviolable par l'entreprise ; tout le reste concerne des données de l'entreprise. Il faut bien gérer cette problématique parce que, même si les gens travaillent, ils sont bien obligés de s'occuper pendant quelques minutes de leurs problèmes personnels, notamment en adressant des courriels. Tous nos employés aujourd'hui ont accès à l'Internet et, s'ils utilisent leur messagerie personnelle à des fins personnelles, cela relève de leur propre responsabilité. Il s'agit d'une question d'éducation des employés et l'entreprise doit s'efforcer qu'ils fassent bien la distinction entre l'information qui relève de l'entreprise et ce qui relève de leurs affaires propres et privées.

Parmi les cas d'attaque relevés aujourd'hui figurent des cas de *phishing*. Par exemple, lorsque les gens mettent leur *CV* en ligne sur un réseau social, la plupart des attaques procèdent de la manière suivante : l'attaquant passe par le biais de quelqu'un de l'entreprise qui est également inscrit dans ce réseau et accède à d'autres noms de l'entreprise car les gens sont souvent référencés avec la mention de leur adresse électronique professionnelle. Ils sont alors attaqués par l'intermédiaire de leur messagerie professionnelle par un courriel piégé qui a pour but de prendre le contrôle de leur ordinateur.

Le fait de s'exposer, si les gens ne sont pas très prudents sur le type de courriel qu'ils reçoivent, c'est quelque chose qui se produit tous les jours. Des centaines de courriels de ce type-là arrivent dans les entreprises ; c'est la vie de tous les jours dans les entreprises à l'exception d'une minorité d'entre elles, extrêmement sensibles, travaillant dans le nucléaire ou la défense, qui n'ont pas accès à Internet.

Dans les entreprises du monde des télécoms, il est assez difficile d'envisager de laisser les téléphones portables à l'extérieur des salles de réunion. Au contraire, dans des entreprises très sensibles, des mesures très strictes existent, notamment quand il s'agit de projets dits « confidentiels défense ». Des zones réservées au traitement de ces projets-là bénéficient de la précaution consistant à **laisser son téléphone portable à l'entrée** et **aucune connexion Internet n'est possible** à l'intérieur de ces espaces. Il s'agit de mesures complémentaires qui ne sont pas représentatives de la vie quotidienne de tous les employés.

Aujourd'hui, la sécurité est aussi une question d'éducation des employés qui devrait commencer par des **règles d'hygiène informatique apprises à l'école**. Lorsqu'on arrive sur le marché du travail, ce serait souhaitable d'avoir déjà des réflexes bien formatés, un peu comme en matière de sécurité routière. Dans ce domaine, des efforts ont été faits de la part des constructeurs automobiles pour renforcer la sécurité, active et passive, des véhicules, d'autres efforts sur les routes et les autoroutes pour éviter de construire des virages en épingle à cheveux après des kilomètres de

lignes droites et, ensuite, il y a eu une éducation forte des conducteurs et, enfin, il y a eu la sanction. Le parallèle avec la circulation routière est assez riche. Internet a vingt-cinq ans au maximum alors que la circulation routière a presque un siècle. Évidemment, Internet et le numérique ne font pas de morts mais **il y a beaucoup de brigands sur les autoroutes de l'information**, peut-être même est-ce l'endroit du monde où il s'en trouve le plus. En outre, **il n'y a pas beaucoup de police qui circule sur les autoroutes de l'information et l'utilisateur est assez peu informé** – il est même à classer dans la catégorie des grands naïfs, pour ne pas dire plus.

On est aujourd'hui dans un monde où l'éducation des consommateurs passe aussi par des normes de sécurité comme le font l'ANSSI et l'Union européenne sur ce sujet en essayant d'améliorer un peu la qualité des normes. Avec la difficulté que, dans l'industrie automobile, les normes ont été mondiales (*crash tests* acceptés au niveau mondial) alors que dans l'industrie de l'informatique, ce n'est pas du tout le cas aujourd'hui. Il y a une volonté européenne très forte de protection du consommateur, du citoyen, etc., qui n'est pas partagée par toute la planète aujourd'hui. Il n'y a donc pas d'aide à attendre d'un mouvement d'ampleur mondiale.

Aux États-Unis d'Amérique, la conception de la protection des citoyens est assez différente de la conception européenne car beaucoup de choses y sont permises qui ne sont pas autorisées en France.

À noter que ces mêmes actions sont autorisées au Royaume-Uni. Toute l'industrie du logiciel est aujourd'hui d'origine nord-américaine et peu de produits sont d'origine européenne ; à part les *SAP* qui sont d'origine allemande. D'ailleurs, même si des matériels sont conçus en Europe ou aux États-Unis d'Amérique, ils sont tous fabriqués en Chine.

La maîtrise du numérique dépend de l'endroit où la valeur ajoutée est créée. Ainsi, quand on paie 50 € pour un téléphone, à part la TVA qui est française, le reste est étranger.

Or, **on ne peut pas savoir ce qu'il y a derrière les composants à partir du moment où on ne les fabrique pas. Les entreprises doivent rechercher un équilibre permanent entre le risque et les opportunités.** C'est pour cela qu'il est assez difficile de légiférer en ce domaine car le contexte évolue à une rapidité stupéfiante et **les entreprises doivent procéder à des évaluations de risque**. C'est le métier des patrons de la sécurité dans les entreprises de limiter le risque pris. Si l'on part du principe que le téléphone n'est pas très sûr, à ce moment-là on va utiliser d'autres moyens : téléphone fixe, téléphone chiffré, etc. En permanence, il faut rechercher comment l'entreprise peut limiter les risques comme cela est fait pour le risque financier, les risques commerciaux et, maintenant, les risques informatiques à limiter au maximum. On ne sait pas les éliminer complètement car il y aura toujours une part de risque. Dans les bilans des sociétés, il y a souvent des provisions pour risques qui sont, en fait,

l'ensemble des risques que l'on n'a pas su éliminer et donc à classer parmi ceux contre lesquels on se protège de manière financière.

En matière de sécurité, il vaut mieux être curieux de nature sous peine de tomber dans la catégorie des naïfs.

Quand on regarde où sont situés les centres de production d'ingénierie du numérique, quand on fait un achat, il ne reste que la TVA pour l'État et la marge du revendeur local. C'est là une retombée de la mondialisation de l'économie.

Tous les opérateurs télécoms achètent beaucoup des technologies peu maîtrisées par les Européens aujourd'hui. Le *GSM* a été inventé par les Européens, normalisé au niveau mondial par les Européens puis, pour des raisons historiques et économiques, les centres de production et de recherche se sont déplacés dans d'autres endroits du monde.

La maîtrise de l'économie numérique s'apprécie en voyant comment nos industriels sont capables de fournir des solutions aux entreprises de télécommunications, aux entreprises de services, etc. Encore une fois, **parler de maîtrise c'est quand même très difficile quand vous ne concevez ni ne construisez tous les équipements que vous utilisez**. Nous sommes plutôt dans une gestion du risque et dans le fait qu'on essaie de diminuer au maximum les risques pour nos clients et pour nous-mêmes.

Orange possède ses propres infrastructures en France qui sont maîtrisées par des Français et sont situées en Normandie, le plus gros centre récemment créé étant à Val-de-Reuil. Mais ce n'est pas *Orange* qui a conçu les ordinateurs qui sont à l'intérieur du système, ce sont *IBM* et *HP*, mais tout ce qui se trouve à l'intérieur du centre est maîtrisé par *Orange*.

Yves Le Mouël. – Il y a une ambition nationale et européenne. Maintenant, il est difficile d'agir seul dans son coin, c'est pourquoi la coopération franco-allemande correspond au désir d'avoir une industrie. Au-delà de la mise en œuvre d'un centre de données, il y a les composantes de ce centre, sous tous ses aspects, à prendre en compte avec les composants physiques et le logiciel.

M. Jean-Luc Moliner. – Nous nous sommes tournés plutôt vers des solutions *open source* plutôt que d'utiliser des logiciels venant des États-Unis d'Amérique.

Yves Le Mouël. – À la fin de l'année dernière, nous avons réalisé une étude montrant un certain nombre de choses et, parmi ses recommandations, figure la nécessité d'un véritable *building* numérique au niveau européen. L'un de ses piliers serait la confiance numérique et, dans le cadre de cette confiance numérique, trois types de propositions seraient possibles : l'une qui serait de **réaliser un projet d'identité numérique fondée sur la carte *SIM*** avec une impulsion forte des États et de l'Europe.

Face à cela, des acteurs comme *Google* ou *Apple* ont une vision sans carte *SIM* de toute cette problématique.

La deuxième proposition, c'est de **mettre en place et promouvoir un label européen de stockage de données**.

La troisième proposition est celle de **la certification des logiciels et des équipements critiques diffusés en Europe**. Il faut que cette sécurité existe plus profondément dans les outils qu'on utilise.

M. Jean-Luc Moliner. – Aujourd'hui, on sait réaliser des logiciels très sûrs, par exemple dans l'aéronautique. Cela a un coût. À l'inverse, le marché grand public est plutôt tiré vers le bas, vers ceux qui proposent les prix les moins élevés.

Le coût de l'expertise d'un matériel est également **très élevé**. En tant qu'opérateur effectuant ce genre d'évaluation, il faut préciser que cela est extrêmement coûteux en raison du temps que cela demande. **Parfois, cela coûte moins cher de fabriquer soi-même plutôt que d'expertiser la sécurité** car si l'on veut vraiment aller au fond des choses, cette expertise dure des mois et il faut mettre une dizaine de personnes sur le sujet. Les évaluations, les tests que nous faisons ne sont pas exhaustifs. Nous faisons le maximum de ce que l'on peut faire dans des délais et à des coûts raisonnables.

Il y a aussi l'agence européenne, l'*ENISA*, qui est l'ANSSI au niveau européen, mais elle ne fait pas ce type d'évaluation ; elle émet uniquement des propositions. Son rôle est utile mais elle n'est pas financée pour faire des évaluations.

À propos des centres de stockage de données, leur visite n'est pas passionnante – il s'agit de rangées d'ordinateurs et il y fait froid – même si cela est assez impressionnant.

Une des grosses questions posées par ces centres de stockage est leur refroidissement. Nous avons choisi une stratégie de *free cooling* de rafraîchissement de l'air tout simplement par de l'air qui, en Normandie, a une température la plus stable possible. L'air chaud évacué part dans l'atmosphère. Cela a un coût. Le plus impressionnant à voir, ce sont les installations techniques autour des centres.

Yves Le Mouël. – Quant aux noms de domaine, aujourd'hui, **c'est l'*ICANN* qui gère à la fois les noms de domaine et les adresses des utilisateurs**. Le président de l'*ICANN* était à Paris récemment et sa vision peut faire plaisir car une évolution est en cours. Ce président, issu de plusieurs cultures, possède une vision très internationale qui semble aller dans le bon sens pour une internationalisation de la gouvernance de l'*ICANN* permettant à toutes les parties prenantes de s'exprimer, pour **couper le lien avec le gouvernement nord-américain** même s'il ne l'exerce pas, paraît-il. Il serait en tout cas intéressant de le couper formellement tout

en n'introduisant pas la possibilité que d'autres grandes puissances puissent elles-mêmes exercer une mainmise sur l'Internet.

Il serait également catastrophique de sectionner l'Internet en un Internet chinois, un Internet occidental, etc. Il faut préserver l'universalité de l'Internet tout en préservant une gouvernance qui assure la participation de tous. Cet objectif semble en bonne voie de réalisation. Le président de l'*ICANN* compte organiser cette association, actuelle structure de droit californien, pour en faire **une fondation** ayant son siège à Genève qui représenterait par conséquent plus facilement cette vision multinationale, internationale, de la gestion de la gouvernance de l'Internet.

L'*ICANN* gère la couche basse de l'Internet avec les noms de domaine et les adresses et tout le monde a une autre problématique qui s'ajoute à celle-là qui est la problématique globale de la sécurité et des usages qui sont faits de l'Internet. La vision que, aujourd'hui, essaie de populariser l'*ICANN*, c'est d'**aller vers une gouvernance mondiale de l'Internet qui ne soit pas l'ONU,** qui ne soit pas non plus sous l'emprise des seuls États mais regroupe l'ensemble des parties prenantes bien représentées pour gérer les noms de domaine et avoir une forme de gestion sur les couches plus hautes de l'Internet.

La croisade que mène le président de l'*ICANN*, à condition qu'elle se concrétise, va dans le sens d'un meilleur équilibre entre toutes les parties prenantes D'où son voyage en Europe pour rencontrer le maximum d'interlocuteurs, pour drainer dans cette gouvernance des entreprises européennes et françaises en particulier. Il est venu nous voir pour que les entreprises françaises participent davantage afin qu'il n'y ait plus seulement, autour de la table, des ingénieurs américains.

Une des raisons pour lesquelles les Anglo-Saxons ont la mainmise sur cette organisation, c'est que les Européens se sont présentés en ordre dispersé ou étaient absents.

PRÉSIDENCE DE LA RÉPUBLIQUE

M. Thiébaut Meyer, responsable de la sécurité des systèmes d'information

27 février 2014

La prise de conscience des risques de l'insécurité informatique s'est accrue depuis les incidents à l'Élysée et l'affaire Snowden.

Face aux attaques, il convient d'abord d'**analyser la menace**, en établissant contre qui était dirigée l'attaque, d'**analyser les risques** puis d'envisager des **mesures appropriées**.

L'adversaire peut-être un État disposant de moyens et de temps et désirant infliger des dégâts bien supérieurs à ceux de la défiguration d'un site *web*.

Lorsque l'attaque vise des opérateurs d'importance vitale (OIV), les attaquants se feront les plus discrets possible pour parvenir à résider un maximum de temps dans les sites attaqués. La discrétion est une question de moyens et il sera donc particulièrement important de repérer de simples traces d'un attaquant même si, de manière générale, la sécurité n'est jamais absolue.

Une fois la présence d'un attaquant détectée, il reste à déterminer son identité et cela est d'autant plus compliqué que l'attaque est souvent menée à partir de multiples postes informatiques situés dans divers pays du monde. Même si tout laisse des traces dans les réseaux, la multiplicité des rebonds complique la recherche de l'identité de l'attaquant.

En ce domaine, la coopération internationale n'est pas toujours évidente car elle requiert du temps alors que les traces d'attaques informatiques sont parfois très volatiles.

Tous les pays pratiquent de la même manière ; les Chinois comme les Américains dont l'ampleur de la surveillance systématique, notamment des courriels privés, n'avait pas été perçue jusqu'à récemment.

En France, un premier pas a été accompli avec la récente loi de programmation militaire qui va inciter les opérateurs d'importance vitale à effectuer un certain travail de cartographie, de recensement pour savoir où sont les données sensibles, qui y a accès, comment se protéger, comment faire remonter les incidents.

Derrière cela, il y a d'importants enjeux de sécurité nationale à défendre, des enjeux économiques également, par exemple dans l'aéronautique, le ferroviaire, le nucléaire, etc.

Plusieurs points sont importants : d'abord **sensibiliser les personnes pour qu'elles aient conscience de l'importance du patrimoine des entreprises, de la présence de données sensibles dans leurs actifs et de la nécessité de les protéger**. La direction centrale du renseignement intérieur (DCRI) effectue un travail de sensibilisation de tout ce qui est relatif aux ressources, au patrimoine scientifique.

Il faut également **mettre en place des contre-mesures de protection**, c'est-à-dire des mesures de sécurité. Il peut s'agir de filtrages de flux, de détections d'intrusions mais également d'un travail du côté des systèmes d'information pour maîtriser ces systèmes et leur sécurité.

Des questions doivent être posées : quels sont les flux de données importantes ? Qui a accès aux données ? Comment sont gérés l'arrivée et le départ des collaborateurs ? Comment la sous-traitance est-elle gérée ? Comment les venues de stagiaires, de coopérants étrangers sont-t-elles encadrées ? Bien voir comment circulent les données dans l'entreprise, qui a accès à ces données et comment les protéger.

Il y a un autre niveau de questions à poser, en termes de strates : sur quels supports se trouvent les données ? Où sont les serveurs ? Quels sont les logiciels installés dessus ? Sont-ils qualifiés ? A-t-on confiance dans les matériels, dans les logiciels, dans les équipements en général destinés à assurer la sécurité ? **La maîtrise du système d'information est primordiale.**

Des recommandations portées par l'ANSSI à propos des mesures de sécurité, notamment le guide intitulé **« *Les quarante règles d'hygiène* »,** indiquent la base à respecter pour un système d'information protégé des attaques les plus courantes et comment réagir. Ce niveau est parfaitement atteignable.

Il y a également une politique de sécurité des systèmes d'information de l'État qui, actuellement, est en phase de finalisation – elle doit être à la signature du Premier ministre – qui reprend également les grands principes de sécurité à décliner ensuite selon les différents ministères et entités concernés.

À propos des mesures à mettre en place pour la sécurité de l'information, il faut rappeler que celles-ci ont des coûts en achat de matériels spécifiques, achat d'équipements, de licences et, également, des coûts en ressources car il faut mettre en œuvre ces systèmes. Les projets informatiques doivent être dotés de budgets conséquents.

Il y a également des problèmes de délais surtout quand on a pensé un peu tard à la sécurité. D'ailleurs, les projets ont tendance à s'étaler dans le

temps. Et, quand les projets sont livrés, ces mesures deviennent des contraintes pour les utilisateurs.

La politique de sécurité des systèmes d'information de l'État (PSSIE) impose l'utilisation des moyens d'authentification forte (dont la carte à puce) dans le cas de données sensibles, ce qui est plus sûr qu'un simple mot de passe. Il faut ensuite gérer tous les cas usuels et quotidiens de perte de la carte, ne pas l'oublier, penser à la récupérer, etc. Cette vraie contrainte doit être intégrée avec son coût initial et ses contraintes quotidiennes d'absence, de perte et de procédures à mettre en œuvre, notamment pour retrouver sa carte d'accès lorsqu'elle a été perdue.

De même, les mesures de sécurité informatique vont contraindre les utilisateurs à une certaine ergonomie et alourdir les projets.

Ensuite, on peut définir les risques, les objectifs de sécurité et penser aux mesures associées très en amont dans les projets pour faciliter la mise en place du processus de sécurisation mais **il est impossible de faire une sécurité transparente qui ne coûterait rien et ne serait pas perçue par l'utilisateur**.

Un arbitrage est donc à rendre au niveau des autorités entre le niveau de sécurité souhaité et les ressources à y allouer qu'il s'agisse de personnels ou de budgets compte tenu du niveau de service à rendre aux utilisateurs.

À la Présidence de la République, l'organigramme est à peu près le même que dans les ministères, à savoir que la sécurité du système d'information est rattachée à l'organe qui s'occupe de sécurité au sens large. À la présidence, c'est le commandement militaire qui intègre la sécurité des systèmes d'information dans tous ses aspects : sécurité des personnels, sécurité physique des locaux, etc., c'est une des composantes de la sécurité. C'est un découpage que l'on voit ailleurs dans les ministères avec le haut fonctionnaire de défense et de sécurité (HFDS), le haut fonctionnaire de défense adjoint, auxquels est rattaché un fonctionnaire de la sécurité des systèmes d'information.

Il est vrai que, au quotidien, je travaille avec les équipes informatiques. Le problème est que la sécurité physique et la sécurité de l'information sont très imbriquées : par exemple, lorsqu'un ordinateur commande une climatisation ou un générateur électrique qui commande lui-même une ouverture de porte ou autre chose.

Pour que le fonctionnaire en charge de la sécurité de l'information puisse être efficace, cela dépend moins de sa position dans l'organigramme que du service qu'il rend à l'autorité ou à l'institution ; pour sa part, la Direction des systèmes d'information (DSI) rend un service quotidien à travers des services de messagerie, de gestion documentaire ou d'application métier quel qu'il soit. Il est vrai que le responsable de la sécurité des systèmes d'information est un petit peu l'empêcheur de tourner en rond qui

vient régulièrement aiguillonner la DSI sur les aspects de sécurité. Les objectifs poursuivis par chacun sont parfois un peu antagonistes car la DSI travaille à budget constant avec des ressources contraintes pour rendre un service, parfois d'importance vitale, et, d'un autre côté, il y a le service en charge de la sécurité qui veut que le service soit rendu en respectant certaines règles.

De toute façon, un dialogue est nécessaire entre les deux pour que cela se passe bien. Plus qu'un rapport hiérarchique, même si les directeurs des systèmes d'informations sont à des postes élevés dans les organigrammes, c'est plutôt par rapport aux autorités et aux services rendus que les situations s'apprécient. Il y a une autorité qui attend un service de la direction informatique qui, elle-même, est contrainte par une gestion budgétaire de ses ressources et qui, parfois, a tendance à mettre de côté les aspects de sécurité pour justement arriver à atteindre l'objectif qu'elle s'est fixé.

Il est important de sensibiliser les autorités, de leur expliquer les menaces sans les exagérer mais sans, non plus, les édulcorer. Ensuite, le choix leur revient mais il faut qu'elles soient capables de l'effectuer en connaissance de cause.

Pour cela, il y a une démarche d'homologation qui est en train de se mettre en place – qui existe déjà dans certains ministères mais qui va être mise en œuvre à la présidence – qui est une formalisation, pour toutes les étapes d'un projet, de la sécurité des systèmes d'information. En amont, **on va faire une analyse des risques qui pèsent sur un projet**. Le but étant d'aboutir, à la fin de l'étude, lorsqu'on a mis en place des mesures pour contrer ces risques, à identifier les risques résiduels puisqu'il y en aura toujours. Ce peut être le comportement d'un utilisateur ; ce peut être des risques qu'on n'a pas su couvrir, que la technologie ne permet pas de couvrir, à cause de problèmes budgétaires ou autres. Mais qu'au moins l'autorité qui va mettre le réseau ou l'application en service soit consciente des risques qui existent encore.

Les pare-feu restent une brique essentielle de la sécurité : tous les flux sont interrompus sauf ceux qui sont spécifiquement autorisés. Dans les réseaux, il y a plusieurs flux d'informations qui circulent. Même si ce n'est pas l'alpha et l'oméga de toute la sécurité.

Aujourd'hui, ce n'est pas cette brique-là qui pose le plus de problème car c'est une technologie bien maîtrisée et, de plus, **il existe en France des produits de confiance qualifiés par l'ANSSI et fabriqués par des acteurs français**. Cette technologie a vocation à perdurer.

Ce qui a évolué ces derniers temps, c'est la vision de la sécurité ; elle n'est plus périmétrique avec un intérieur et un extérieur de l'entité à protéger. À la frontière, il y avait des pare-feu qui bloquaient les flux passants. On a évolué par rapport à ce schéma, notamment avec tous les

besoins de mobilité. Aujourd'hui, on a du mal à faire comprendre à une autorité qu'une fois sortie de l'institution, elle n'a plus d'accès à l'Intranet, à sa messagerie ou à ses fichiers. Or, les gens bougent et, même depuis chez eux, ils veulent encore avoir accès à leur messagerie professionnelle. C'est pour cela que, aujourd'hui, c'est plus diffus en termes de périmètre.

Les données de l'entreprise ne vont plus être physiquement uniquement sur les terminaux situés dans ses locaux mais seront diffusés sur des terminaux dont il faudra avoir la maîtrise et qui seront disséminés partout.

On ne peut pas interdire toute communication avec des services de courriel, *Google, Yahoo* ou autres, mais il est possible d'interdire la redirection systématique des courriels. Toutefois, si un salarié s'écrit un courriel à lui-même dans sa messagerie, une fois par jour, il n'y a pas moyen de l'en empêcher. En revanche, il faut le sensibiliser aux risques qu'il fait courir à l'institution. Cette sensibilisation commence à se mettre en place.

Si l'on revient à l'affaire Snowden, on a vu l'ampleur de l'agressivité des services étrangers, ce qui a donné matière à sensibiliser les gens aux différentes menaces. Il y a quelques semaines, j'ai effectué une présentation à tous les conseillers de la Présidence de la République. Je me suis contenté de leur montrer ce qu'on trouve partout sur Internet. Par exemple, on y trouve les stations d'écoute de la *NSA* où l'on voit Paris en première place. Ici, ce sont des photos de l'ambassade américaine en Allemagne : on voit une superstructure sur le bâtiment et, à l'intérieur de cette superstructure, il y a ce type d'équipements qui sont des antennes captant les réseaux hertziens et qui vont récupérer les communications à partir d'un traitement de signal.

L'affaire Snowden a aidé à une prise de conscience notamment par les autorités politiques. Maintenant, c'est dans la presse, dans *Le Monde*, *Spiegel*, le *New York Times*, ce qui rend le discours beaucoup plus facile ; on n'est plus entre personnes autorisées pour parler de réception hertzienne ou d'autres questions techniques. On peut avoir un débat avec les autorités politiques qui ne sont ni techniciennes ni d'anciens ingénieurs des télécoms.

On n'arrivera pas à avoir sur les produits de sécurité une ergonomie équivalente à celle des produits grands publics. Le téléphone *Teorem* de la société *Thales* peut être utilisé pour des conversations jusqu'au niveau « secret défense ». Il existe aussi une version pour la mobilité, offrant un chiffrement sûr par rapport à l'extérieur comme à l'intérieur, allant jusqu'au niveau « confidentiel défense ».

Il est parfois difficile de convaincre l'interlocuteur que le produit est suffisamment bien fait pour qu'il n'y ait aucune interception des conversations.

En revanche, ce téléphone ressemble aux téléphones portables de la fin des années 1990 ; il n'est pas tactile ; ce n'est pas ce qu'on a l'habitude d'avoir entre les mains depuis sept ou huit ans.

Ces téléphones sont fabriqués en petites séries qui coûtent cher. Il existe aussi des solutions qui permettent d'équiper des *smartphones* à un niveau de diffusion restreinte qui offrent un canal sécurisé entre ces téléphones et le réseau de l'administration.

Les téléphones actuels sont de petits ordinateurs moins sécurisés que ceux qu'on a l'habitude d'avoir à la maison ou au bureau. Moins sécurisés parce que les éditeurs veulent être les premiers sur le marché ils sont conçus d'abord pour leur ergonomie. **Ils ne sont donc pas ou peu sécurisés.** On trouve sur Internet, pour quelques centaines d'euros, des logiciels qui permettent d'installer sur les ordinateurs des dispositifs permettant d'avoir des copies de vos messages, d'activer des micros à distance, de géolocaliser les déplacements d'une personne. Ces téléphones sont devenus des sources d'information extraordinaires. En plus, l'utilisateur en prend soin, le garde toujours avec lui et pense à le recharger. Lorsque l'on voulait espionner dans les années 1970, il fallait penser à alimenter le micro, changer la pile, la récupérer, **maintenant, la victime s'occupe de tout**.

Peu à peu les gens en prennent conscience. Depuis le mois de novembre 2013, à l'entrée des conseils des ministres britanniques, les ministres déposent leurs *smartphones*.

Dans certaines administrations, c'est ce que l'on demande. Par exemple, au SGDSN, vous déposez votre téléphone à l'entrée dans un petit coffre. Les gens prennent peu à peu conscience de cette nécessité.

La difficulté qui demeure dans les entreprises, dans les administrations, c'est que les utilisateurs aiment bien avoir leur téléphone personnel sur lequel ils aimeraient bien récupérer les données de l'entreprise ou leurs fichiers personnels, ce qui pose de vrais problèmes en matière de sécurité car on n'est pas capable d'assurer la sécurité d'un téléphone qu'on ne maîtrise pas totalement. À l'inverse, si on maîtrise le téléphone, on ne va pas pouvoir laisser l'utilisateur installer ce qu'il veut dessus et l'utiliser comme un équipement personnel.

Il est important d'arriver à bien sensibiliser les autorités et les collaborateurs pour distinguer le monde personnel du monde professionnel. Mais **c'est une utopie de croire que les collaborateurs pourraient installer les données de l'entreprise sur leurs téléphones personnels et qu'elles y seraient en sécurité**.

Thales a un produit, *Teopad*, qui permet d'isoler certaines applications de l'entreprise, néanmoins vous resterez toujours sur un socle grand public avec des couches sous-jacentes de votre téléphone dans lesquelles vous ne pourrez pas avoir confiance. Mélanger sur le même objet deux degrés de confidentialité, cela paraît compliqué.

Il y a une quinzaine de jours, une diplomate américaine en Ukraine a parlé avec l'ambassadeur américain à Kiev, en termes peu diplomatiques, de l'Union européenne. La conversation a eu lieu sur un téléphone tout-venant

et s'est retrouvée sur Internet. Aujourd'hui, on n'a pas de certitude mais on a de fortes suspicions sur les services russes qui ont écouté la conversation et se sont empressés de la mettre à disposition de tout le monde.

Cela illustre le fait que **l'autorité doit être sensibilisée à la sécurité informatique et en accepter les contraintes**.

À cet égard, il existe une différence culturelle entre la France et les États-Unis d'Amérique où les services de sécurité peuvent imposer au président nouvellement élu de renoncer à l'utilisation de son téléphone personnel.

Maintenant, le téléphone *Teorem* est largement déployé dans les administrations centrales, dans les cabinets, dans les administrations territoriales, dans les rectorats et dans toutes les préfectures.

TOTAL

M. Patrick Hereng, directeur des systèmes d'information et télécommunications

6 mars 2014

Pour s'inscrire dans un système de protection contre les risques numériques, *Total* a commencé à dresser une cartographie des risques des systèmes d'information qui sera mise à jour régulièrement pour formaliser lesdits risques. *Total* considère qu'il existe vingt-neuf risques rattachés à neuf enjeux métiers.

En 2013, un comparatif sécurité a été réalisé avec d'autres entreprises pétrolières – *BP, Chevron, Repsol, Statoil, Total, Petrobras, ENI, Aramco, Shell. Total* se situe à peu près dans la moyenne de ce groupe et il a été décidé de lancer un plan d'évolution de la sécurisation du système d'information qui a été validé mi-2013. Il représente environ soixante-dix projets à réaliser sur trois ans, avec une relance éventuelle de cette action dans trois ans pour l'ensemble du groupe. Ce plan est évalué à 80 millions d'euros.

Ce plan de sécurité repose sur quatre piliers. Le premier est **la sécurisation du système d'information de gestion** en passant par les infrastructures des services partagés, essentiellement les télécommunications pour les mille sites de *Total* dans le monde reliés à des entités du groupe. Ce plan de sécurisation des infrastructures et des services partagés est en cours, il nécessite un certain nombre de projets et va prendre trois ans.

Le second pilier est **la sécurité de l'information industrielle**, aujourd'hui en chantier car un certain nombre d'actions sont encore à mener. Les systèmes de commande, appelés *SCADA* dans la terminologie des informaticiens, sont de plus en plus, à la base, construits avec des composants informatiques traditionnels. Ainsi, *Transmission Control Internet Protocol* (*TCP/IP*) des logiciels de *Microsoft* ou de *Linux* sont utilisés dans les *SCADA*. **Ces systèmes sont** donc **de plus en plus vulnérables**. La sécurisation des systèmes d'information industrielle a donc été décidée sur tous les sites de *Total*, que ce soient les plates-formes, les raffineries, les dépôts, pour compléter efficacement le dispositif actuel.

La sécurité des applications constitue le troisième pilier**.** L**e système d'information de métier** bénéficie de la mise en place de dispositifs de gestion d'identité, d'habilitations adaptées aux applications.

Le dernier pilier est la **sensibilisation des utilisateurs** pour changer leurs comportements.

Ces dispositifs dépendent de l'efficacité de la gouvernance des systèmes d'information, en particulier de la gestion de crise et de la réactivité en cas d'incidents de cybersécurité. La pratique d'exercices réguliers permet de pallier les failles. La gouvernance des systèmes d'information évolue en fonction de ce plan de sécurité des systèmes d'information. **Les risques sont continuellement contrôlés et mesurés**, ce qui aboutit à l'établissement d'une réelle cartographie.

Les trois priorités des systèmes d'information du groupe sont la sécurité, l'évolution de l'entreprise numérique et l'optimisation des coûts des systèmes d'information. Relever les barrières de protection pour résister aux futures attaques devient une nécessité.

Total est particulièrement sensibilisé aux risques de cybersécurité depuis la fusion en 2000 entre *Total*, *Elf* et *Petrofina*. Cette problématique n'est pas nouvelle mais elle a pris de l'ampleur suite à l'attaque subie par *Saudi Aramco* en 2012. Cette attaque ciblée, par un virus créé à dessein, indétectable par les antivirus, a entraîné la destruction de 30 000 postes de travail. Sur les disques durs attaqués ne demeurait que l'image du drapeau américain. L'origine et l'identité des attaquants restent indéterminées à ce jour. Ils avaient pour objectif de bloquer la production de *Saudi Aramco* qui représente 12 % de la production mondiale.

Il a fallu un certain temps à cette société pour se remettre d'aplomb en dépit d'une réaction rapide et du fait qu'il existe chez elle une coupure complète entre le système d'information de gestion et le système de production : aucun flux ne part du système d'information de gestion vers le système industriel, les flux ne progressent qu'en sens inverse. Mais il a bien failli y avoir des conséquences. En trois semaines environ, le disque dur de 30 000 postes a été remplacé pour relancer les systèmes.

Cet incident a marqué *Total* et, de manière générale, toute la profession pétrolière. De *user friendly,* ils sont brutalement devenus *security first*. Il existe donc désormais des contraintes pour les utilisateurs. *Total* échange avec d'autres sociétés sur les aspects de sécurité. En effet, pour bien résister, il est nécessaire de **s'appuyer sur un réseau qui transmet l'information, notamment celle sur l'occurrence d'incidents**.

La souveraineté en matière de données numériques se joue des frontières mais elle a du sens par rapport aux fournisseurs de services et d'équipements, en particulier par rapport aux menaces de type étatique. Il est important que la France dispose d'une filière de bon niveau pour fournir à la fois des services dans les nuages qui soient des services qualifiés, « vendus sur étagère », accessibles *via* Internet, à des prix compétitifs. Pour les autres fournisseurs dans le nuage numérique, ou *cloud*, **on ne sait**

où sont stockées les données de tels services. Ce peut être en Europe, aux États-Unis d'Amérique ou ailleurs…

Dans le nuage, il y a plusieurs types de services : infrastructures à la demande (*IaaS*), logiciels à la demande (*SaaS*), ou plates-formes à la demande (*PaaS*). Ces services peuvent se situer dans des nuages publics ou dans une infrastructure spécifique construite par un opérateur, c'est-à-dire un nuage privé.

Total considère que **les données à stocker dans le nuage public ne peuvent être que des données peu confidentielles**, sauf, si dans le cadre du plan sécurité, des données ont bénéficié de moyens de chiffrement complémentaires leur permettant d'y être stockées. Aujourd'hui, le recours aux nuages publics est modéré et est assortie d'un dispositif particulier en matière de sécurité. En effet, *Total* a établi un régime de classification des données en quatre catégories : jusqu'au niveau 2, il est possible d'utiliser le nuage mais, au-delà de 2, pour des raisons de sécurité, il est interdit de recourir au nuage.

Quand on utilise le nuage, une analyse spécifique de risque associé est effectuée en fonction de la classification des données et des types d'applications souhaitées. Aujourd'hui, le SaaS (*Software as a Service*), configuration dans laquelle le logiciel est installé dans le nuage est le service le plus utilisé par *Total* qui a les moyens de se construire lui-même les infrastructures et les plates-formes. C'est l'applicatif qui pousse à aller dans le nuage ; certaines applications ne se trouvent que dans le nuage public et nulle part ailleurs. Si vous ne voulez pas l'utiliser, vous ne pourrez profiter de l'application.

Sous la pression des entreprises, certains éditeurs peuvent mettre des applications à disposition dans un nuage privé mais l'industrie informatique, au vu du poids des investissements effectués, incite à l'utilisation d'un nuage où elles mettent des applications, que ce soit dans le nuage public ou dans le nuage privé. ***Total* est aujourd'hui réservé face aux nuages** et considère surtout le degré de confidentialité des données. Encore une fois, pour éviter les risques, il faut utiliser des moyens de chiffrement.

En raison du peu de confiance accordée au stockage de données dans les nuages, à part pour un certain nombre d'applications dans le *SaaS* dont la sécurité n'est pas à craindre, *Total* possède ses propres centres de stockage de données (*data centers*). Ces centres sont, en fait, loués mais sont considérés comme appartenant à *Total*.

Total est en phase avec les préconisations de l'ANSSI et de la CNIL, surtout avec les **règles d'hygiène informatique** prises en compte dans le référentiel de sécurité de *Total* qui porte sur l'ensemble du périmètre du groupe. Les règles de ce référentiel doivent être respectées et donnent lieu à des **audits réguliers des règles informatiques** préconisées par l'action mise en œuvre. Il faut **mieux gérer les droits d'accès, les droits d'administration,**

les mots de passe pour être capable de les changer rapidement, pour éviter que les pirates trouvent facilement ce type d'informations.

Pour les choix de matériel et de fournisseurs, *Total* s'appuie sur les référencements de l'ANSSI lorsqu'ils existent. L'interaction avec l'ANSSI est fréquente. *Total* est pleinement en phase aussi avec les préconisations sur la sécurisation des systèmes industriels. En général, les gens sont peu sensibilisés à la problématique de sécurité et croient qu'il n'y a pas de problème alors que, en commençant à travailler avec les spécialistes de la sécurité, ils prennent conscience de l'existence et de l'acuité de ces problèmes.

En ce qui concerne la CNIL, la directive européenne de 1995 a repris la loi française informatique et libertés ; les déclarations exigibles sont effectuées pour encadrer les échanges de données personnelles. Suite aux recommandations de la CNIL, des *Binding Corporate Rules (BCR)*, règles qui définissent la politique de *Total* en matière de sécurité, ont été établies et viennent d'être validées par les régulateurs européens. La protection des données personnelles est appliquée à l'ensemble du système de gestion.

Ce que dit la CNIL est repris dans quasiment tous les pays du monde même si la réglementation des États n'est pas forcément homogène**.** La protection de données personnelles est une préoccupation importante à avoir car, lorsqu'il y a un problème de sécurité, c'est l'image de marque de l'entreprise qui peut être atteinte. Cela n'est bon ni pour l'entreprise ni pour ses clients. Aujourd'hui, les préoccupations émises par la CNIL sont de bon sens.

Le référentiel de sécurité s'applique également aux filiales et aux sous-traitants auxquels un plan d'assurance sécurité est imposé. Les activités de *Total* en tant qu'opérateur d'importance vitale ne représentent qu'une petite partie (raffineries, quelques dépôts, les *pipes lines*, etc.) de ses activités mais le plan global de sécurité est appliqué à l'ensemble des activités.

Jusqu'à présent, ***Total* n'a pas subi d'attaque massive mais est régulièrement attaqué par des virus ou des chevaux de Troie**. C'est pourquoi, il était important de lancer très vite le centre opérationnel de sécurité, dispositif permettant d'avoir une analyse précise de ce qui se passe dans le réseau. Ce dispositif est en partie sous-traité à *Thales*. Tout ce qui laisse une trace sur le réseau peut être retrouvé car stocké et donc ensuite analysé. C'est ainsi qu'une attaque par des chevaux de Troie sur l'activité « gaz » de *Total* a été détectée ; ils n'avaient pas encore été activés mais quelques postes avaient déjà été affectés. Ils ont été nettoyés avant d'avoir servi à envoyer de l'information. Des **attaques en déni de service** ont touché certains sites Internet de *Total* qui ont été bloqués pendant quelques heures mais il n'y a pas eu d'attaque massive pour l'instant. Plutôt que de savoir si elle aura lieu, il s'agit plutôt de se demander quand elle surviendra. C'est la raison pour laquelle *Total* veille quotidiennement à ses barrières de sécurité.

La protection des données en qualité d'opérateur d'importance vitale suppose d'imposer aux sous-traitants d'élaborer un plan de sécurité, contrôlé régulièrement, reprenant les règles et les préconisations décidées.

Les utilisateurs doivent être informés et également sensibilisés. Par comparaison, il ne suffit pas d'apprendre que la cigarette est mauvaise pour la santé pour que les comportements changent de ce seul fait. Les actions de sensibilisation vont être intensifiées notamment face au *phishing* - campagne par courriel permettant d'activer des *malwares*. Il est possible de sensibiliser en faisant du faux *phishing*, c'est-à-dire en s'envoyant des courriels pour voir qui va répondre et, ensuite, préciser aux personnes qui ont répondu qu'il ne faut pas répondre à ce genre de message. Ces attaques sont souvent bien conçues. Ainsi, *Saudi Aramco* a commencé à être attaqué, à se faire pirater du fait d'un *phishing* qui renvoyait à un site Internet auquel les employés communiquaient leur mot de passe croyant s'adresser aux informaticiens internes. Il y a toujours des personnes qui réagissent car ces attaques sont mieux en mieux réalisées.

Par ailleurs, dans les avions, dans les trains, empruntés par beaucoup de personnels de *Total*, il leur est conseillé d'utiliser un écran qui limite le champ visuel et de faire attention à ne pas être lu par le voisin. De plus, beaucoup d'informations confidentielles peuvent être volées en cas de perte ou de vol d'un *PC*. Il faut aussi sensibiliser à cela. Aujourd'hui, par exemple, il est facile d'utiliser *Dropbox*, c'est pratique mais ce n'est pas du tout sûr ; il faut expliquer le risque qu'il y a à utiliser ce genre de solution. *Total* construit actuellement une solution équivalente mais sécurisée. Un dispositif de sécurisation peut être efficace mais des comportements inconséquents sont susceptibles de ruiner ce dispositif.

La séparation entre la vie privée et la vie d'entreprise est de plus en plus floue du fait d'outils qui permettent d'accéder aux divers systèmes quel que soit le lieu ou le moment. Ainsi, l'accès aux données de l'entreprise peut s'effectuer au moyen d'un téléphone privé mais cette utilisation est déconseillée en raison des risques de sécurité associés. Il est très difficile de contrôler ce qu'il y a sur le téléphone de la personne. De fait, *Total* donne des **téléphones professionnels** que les employés peuvent utiliser accessoirement à des fins personnelles : ce qui permet d'appliquer la politique de sécurité de l'entreprise. La politique sur le problème des dispositifs à domicile (*home devices*) est également appliquée pour les prestataires. Il est parfois demandé aux prestataires de venir avec leur *PC* et un accès virtuel leur est accordé. Leur accès aux données se trouve, de fait, limité.

Dans la politique de *Total*, **sur les postes de travail, tout chargement de logiciel non professionnel est interdit**. Les droits d'administration sont réservés. Le changement de logiciel spécifique doit être autorisé.

Total a des échanges réguliers avec d'autres entreprises françaises (*Michelin*, *Areva*, *Safran*, *Société Générale*, etc.) à travers diverses structures

(le CLUSIF, le CIGREF, etc.) et beaucoup d'échanges aussi avec quelques autres entreprises du secteur pétrolier pour être en phase avec le marché.

Les antivirus sont nécessaires mais absolument pas suffisants. Des mesures complémentaires doivent être prises face aux menaces actuelles, d'où **la nécessité de mettre en place un centre de sécurité opérationnel** d'autant que les antivirus ne sont pas tous capables d'arrêter tous les virus qui existent. Même si certains virus sont connus, ils mutent. Il n'est pas aisé de les identifier.

Les fournisseurs d'antivirus ne connaissent pas forcément l'ensemble des virus. Et il faut donc favoriser une sorte de biodiversité d'antivirus pour ne pas utiliser une seule solution antivirus pour traiter un problème.

Aux États-Unis d'Amérique, la législation oblige les éditeurs à déclarer les failles de leurs produits dont profitent souvent les pirates. Si, par exemple, *Microsoft* déclare une faille, elle risque alors d'être exploitée par des pirates car, entre le moment où la faille est déclarée et l'élaboration d'une solution de parade, une attaque peut être menée. L'antivirus ne peut être actif que lorsque le virus est connu mais si le pirate crée un virus pour profiter d'une faille, il y a un moment où ce virus a une capacité de nuisance.

S'il y a des failles dans des logiciels applicatifs comme *Internet Explorer*, **il faut mettre à jour les logiciels pour pouvoir résister aux attaques**. En effet, les antivirus ne dispensent pas d'apporter des correctifs au logiciel. Le temps de déploiement des solutions sur l'ensemble du périmètre doit être réduit. Sur ses sites, dans cent trente pays, le programme utilisé par *Total* prend encore trop de temps. Il faudrait cependant pouvoir procéder à une modification en moins de vingt-quatre heures, comme le fait maintenant *Saudi Aramco*.

Le système de supervision de sécurité est fondamental. Les sondes sont essentielles pour permettre d'apprécier en temps réel ce qui se passe sur le réseau. En plus des antivirus, il est nécessaire d'utiliser des pare-feu qui permettent de bloquer un certain nombre d'attaques ou d'accès. Il est à noter que les pare-feu de nouvelles générations peuvent filtrer les couches applicatives et pas uniquement les couches de base.

Il y a régulièrement des attaques sous forme de **chevaux de Troie**.

Les effectifs pour parer aux attaques sont organisés en deux niveaux. D'une part, **une filière de responsables des systèmes d'information** déployée au niveau groupe, au niveau branche, au niveau local qui a pour mission d'appliquer le référentiel de sécurité. Cela représente 250 personnes au niveau du groupe. Par ailleurs, **une filière opérationnelle**, rattachée aux équipes de production informatique, met en œuvre et exploite les outils de sécurité. Elle est alors intégrée dans les opérations et il est donc difficile de dénombrer exactement les personnes qui travaillent spécifiquement à la sécurité.

En cas de crise, des **cellules de crise** sont activées au sein du groupe et, en cas d'événement de grande ampleur, une **équipe d'intervention rapide** est réservée, en permanence, chez *Thales*. Dans la gestion des crises informatiques, la réactivité est un élément extrêmement important de la solution. Ainsi, *Saudi Aramco* aurait pu bloquer l'attaque si elle avait coupé Internet plus vite ; cela s'est joué à cinq heures près. En effet, il **faut réagir en quelques heures face à une attaque** pour limiter les impacts.

Les personnes en charge du référentiel ont pour mission de traiter la problématique de sécurité qui suppose d'abord **d'être organisé face à la crise** en mettant en place un dispositif de crise informatique et de vérifier son efficacité à l'aide d'exercices réguliers.

Les solutions de sécurisation s'intègrent dans le cadre juridique européen ou international mais dans certains pays, comme la Russie, le Pakistan ou la Chine, et pour certains équipements, des autorisations d'exportation sont nécessaires. Certains matériels ne peuvent être implantés dans certains pays, du fait de l'opposition des Américains.

Si la réglementation sur les données personnelles existe, les dispositions d'application de la loi de programmation militaire sont attendues pour mettre en conformité le plan actuel, fondé sur de la prospective, avec les dispositions applicables.

Le fait que les noms de domaines soient attribués par une association américaine ne pose pas de problème particulier à *Total*. Les domaines intéressants ont été réservés : le *Total.com*, le *.total*.

Pour améliorer la sécurité des entreprises face au numérique, à l'image de *Total*, il convient de dresser une cartographie des risques, de mettre en place les outils de protection (le centre opérationnel de sécurité, les équipements de protection, etc.), de protéger les installations industrielles, de renforcer la sécurité des applications, de sensibiliser les utilisateurs, de se préparer en termes de gestion de crise et de posséder une cartographie des risques actifs, régulièrement réévaluée, qui permette de gérer les risques.

Il faut également développer des possibilités d'**utiliser le nuage de manière sécurisée** – pour la mobilité en particulier – afin de pouvoir rester compétitif. Il n'est pas possible de renoncer totalement à utiliser le nuage. Un dispositif est en cours de conception dénommé *cloud broker* (fournisseur de nuage) qui va permettre de faire de l'authentification, de crypter les données. Le niveau de sécurité sera alors plus important.

Le nombre d'objets connectés augmente sans cesse et il en est prévu 50 milliards en 2020. Aujourd'hui, chez *Total*, il y a des dispositifs de surveillance installés dans des turbines sur les plates-formes pétrolières ; ces capteurs mesurent en continu de nombreux paramètres – la température, la vitesse de rotation – et ces informations sont analysées à partir de technologies de *big data* pour déterminer des débuts de pannes ; cela évite

d'être victime d'une rupture de turbines obligeant à arrêter la production d'une plate-forme.

GENDARMERIE NATIONALE - DIVISION DE LUTTE CONTRE LA CYBERCRIMINALITÉ – SERVICE TECHNIQUE DE RECHERCHES JUDICIAIRES ET DE DOCUMENTATION

Colonel Éric Freyssinet, coordinateur du plateau d'investigation Cybercriminalité & Analyses Numériques (PI CyAN) - Pôle judiciaire de la gendarmerie nationale

6 mars 2014

Je travaille depuis une quinzaine d'années dans le domaine de la sécurité numérique, à savoir en début de carrière sur le traitement de la preuve numérique et ensuite à la Direction générale de la Gendarmerie nationale sur les projets de la lutte contre la cybercriminalité. Depuis trois ans, je suis à la tête de la division de la sécurité numérique contre la cybercriminalité, qui fait partie du service de technique de recherches judiciaires et de documentation – service qui assure le traitement de l'information judiciaire et fait partie du pôle judiciaire de la Gendarmerie nationale. En 2005, une division de lutte contre la cybercriminalité a été créée ; elle résulte de l'évolution de la cellule de veille sur Internet créée en 1998.

L'activité de cette division comprend des missions de police judiciaire au plan national, avec deux axes d'action. Le premier est la veille à vocation judiciaire, de façon proactive, sur Internet afin de détecter les infractions. Contrairement aux collègues de terrain, la division choisit les infractions sur lesquelles elle travaille, qui comprennent des enjeux techniques et juridiques. Détecter des infractions sur Internet, cela suppose de collecter des informations, de développer de nouvelles méthodes d'investigation. C'est un métier qui évolue en fonction du type d'infractions. Quelques plaintes sont également reçues notamment des entreprises du commerce électronique ou de services en lien avec le ministère de la défense, victimes d'attaques contre leur site *web* par exemple. La Gendarmerie nationale est toujours ancrée au sein du ministère de la défense pour certaines de ses missions. C'est le service de police qui est le plus proche de la défense et qui essaie de répondre aux attentes de celle-ci.

Le second axe est tourné vers le terrain. Il suit l'activité des enquêteurs spécialisés de la gendarmerie. Au sein de la division de lutte contre la cybercriminalité, il y a un guichet unique téléphonie et Internet pour faciliter les relations entre les enquêteurs et les opérateurs quand il

apparaît des difficultés en matière de réponses aux réquisitions ; par exemple, pour obtenir des informations dans le cadre d'une garde à vue.

Une autre équipe, composée de vingt-huit personnes, est chargée de développer de nouvelles applications, de nouveaux services pour aider les enquêteurs spécialisés, leur rendre plus accessible l'information dont dispose la Gendarmerie nationale

Le laboratoire de preuves numérique (département informatique et électronique de l'Institut de recherches criminelles de la Gendarmerie nationale), avec lequel travaille la division en étroite coopération, et situé également à Rosny-sous-Bois, comprend une vingtaine d'experts, ingénieurs et techniciens en charge de la preuve numérique au niveau central.

Le service technique de recherches judiciaires et de documentation a un rôle de coordination, d'apport de nouveaux outils aux enquêteurs, de réponse aux besoins de certaines victimes de nouvelles attaques, infractions, escroqueries, etc.

En matière de souveraineté numérique, la gendarmerie conseille aux entreprises de commencer par maîtriser leur patrimoine informationnel. C'est-à-dire sérier les différents types d'informations, distinguer les données sensibles et importantes pour l'entreprise, comme les résultats des recherches et développements, les objectifs et tout ce qui peut être essentiel et confidentiel. C'est à partir de là que les contraintes de stockage et de sécurité sont définies. Il ne faut d'ailleurs pas tout stocker au même endroit mais maîtriser les données en fonction des risques par rapport à des critères économiques ou autres. Des choix de stockage s'imposent.

Quant à l'informatique dans des nuages, cela dépasse la problématique du stockage mais inclut la mise à disposition de services, comme de capacités de calcul informatique distribuées, à des coûts accessibles et disponibles en quelques minutes. Ces capacités de calcul ou de stockage plus importantes sont utiles aux entreprises ou à l'État lorsqu'ils souhaitent externaliser certaines fonctions. Par exemple, en cas de perquisition par un enquêteur sur le terrain, les copies d'un téléphone mobile ou celle d'un disque dur pourraient être mises à disposition à Rosny-sous-Bois, à Nanterre ou Écully, sans qu'il y ait transfert physique du téléphone ou du disque dur. Le support pourrait être copié et adressé à des experts à distance avec un double bénéficie : efficacité et économie.

Le stockage dans les nuages est souple. Pour l'administration, cette capacité devrait être gérée par un nombre raisonnable de personnes. Une structure commune pourrait être envisagée avec différents secteurs de sécurité ; elle mettrait à disposition des capacités excédant celles possibles de mettre en œuvre isolément ou de manière plus sûre. C'est la même démarche pour l'entreprise ou pour le particulier. La possibilité d'avoir recours à un serveur d'information a toujours existé mais la disponibilité et la souplesse sont fournies aujourd'hui par les nuages.

La confiance accordée au stockage de ces données dépend d'abord de la confiance accordée à l'entreprise qui gère le nuage et des dispositions prises par elle pour le sécuriser. De plus, il est possible d'ajouter du chiffrement sur un stockage dans un espace partagé. Il y a quelques années, une entreprise spécialisée dans l'archivage de documents sécurisés, située vers Lausanne, a été victime d'un incendie et l'ensemble des données stockées a été détruit. Cela pourrait arriver aussi à des serveurs informatiques confiés à une société n'ayant pas prévu de multiplier la localisation des données et de baliser la sécurité sous tous ses aspects. Sans aller jusqu'à évoquer la notion de souveraineté, il y a beaucoup d'enjeux techniques auxquels il faut penser.

À propos de l'articulation des missions entre l'Agence nationale de la sécurité des systèmes d'information (ANSSI), agence de l'État, et la Commission nationale de l'informatique et des libertés (CNIL), autorité administrative indépendante, il est à noter que l'ANSSI a évolué récemment à partir de la Direction de la sécurité des systèmes d'information (DSSI) et n'est donc pas partie de rien en 2009 même s'il y a eu depuis une montée en puissance. Quant à la CNIL, elle ne cesse d'évoluer depuis 1978.

La CNIL protège l'usager, le citoyen, tandis que l'ANSSI protège les opérateurs d'importance vitale et les administrations. Ces deux types d'acteurs se complètent.

La question de leur coordination se pose cependant, par exemple, pour la notification des incidents techniques. Quel est le bon acteur pour traiter un type d'incidents comme celui survenu à *Orange* ? Les opérateurs d'importance vitale traitent des données concernant le citoyen et relèvent de l'ANSSI mais les 800 000 identifiants concernés par l'incident survenu à l'opérateur *Orange* sont de la responsabilité de la CNIL. Fallait-il communiquer rapidement sur cet incident ? Quand il y a des compétences concurrentes, la coordination et le dialogue sont indispensables. C'est le cas entre l'ANSSI et la CNIL qui ont des actions complémentaires. Toutefois, chronologiquement, ce n'est pas évident à réaliser car la CNIL doit être prévenue très rapidement. La sécurisation des données est dans son champ de compétences.

Une enquête judiciaire est en cours sur l'incident qui a concerné *Orange*. Même si les conséquences n'ont pas été importantes, cela a posé un problème de confiance au consommateur, à l'usager. Le fait de devoir communiquer autour de ces incidents est positif. *Orange* s'interroge sur la manière de communiquer avec ses usagers et, pour l'avenir, *Orange* est sous le regard de tout le monde. Les mesures correctives mises en place sont donc scrutées avec intérêt. **Le secret sur les incidents ne permet pas de progresser**.

À propos de l'anticipation des évolutions techniques par la CNIL, il est à noter que, depuis 2003, a été mise en place **une association dénommée *Signal Spam* qui traite des signalements émanant d'internautes à propos de**

courriers électroniques non sollicités. Cette association travaille en partenariat avec les acteurs du courrier électronique, les opérateurs, l'administration et la CNIL. Grâce aux informations collectées auprès des victimes, la CNIL est à même de connaître les types de messages non sollicités et les mauvaises utilisations faites des listes d'adresses électroniques. *Signal Spam* transmet tous les mois un relevé de ces incidents à la CNIL. Dans ce cadre, un dialogue avec les professionnels du courrier électronique est instauré permettant à la CNIL d'avoir un regard extérieur, de participer aux débats et d'apporter son analyse.

Cet espace de dialogue neutre, externe, permanent, a permis à la CNIL d'émettre un avis sur la façon de traiter les jeux concours. En fait, ces jeux servant surtout à obtenir les coordonnées de personnes, la CNIL a rappelé les règles qu'elle préconisait dans ce domaine. Ces règles ont été établies en dialoguant avec les acteurs et en observant les pratiques. *Signal Spam* permet ce dialogue à partir d'informations concrètes ; c'est le type même de travaux qu'il est important de développer avec la CNIL. La CNIL s'est plutôt bien adaptée aux évolutions technologiques. Comme la gendarmerie, elle compte maintenant des agents qui conduisent des investigations numériques dans les réseaux des entreprises ou des administrations.

À noter que des parlementaires sont commissaires au sein de la CNIL. Celle-ci ne va pas émettre des recommandations sur les bonnes pratiques à conseiller aux entreprises sans les avoir écoutées d'abord. Il en va de même pour la gendarmerie qui d'abord est attentive aux contraintes s'imposant aux divers acteurs avant de leur adresser des recommandations ou des directives. Au niveau européen, le groupe de l'article 29 est beaucoup moins à l'écoute des difficultés des opérateurs quant à la conservation des données par exemple. **Il n'y a aucune écoute des services de police et de la justice au niveau européen alors que c'est tout le contraire au niveau français**.

En matière de données à caractère personnel au sens de la loi informatique et libertés, c'est le responsable du traitement qui est tenu de garantir la sécurité de son système d'information et cette responsabilité s'étend à ses sous-traitants. Il s'agit là d'une garantie légale.

Récemment, l'article 22 de la loi de programmation militaire (LPM) a introduit des dispositions semblables s'imposant aux opérateurs d'importance vitale pour la sécurité de leurs données et leurs infrastructures.

Dans le cadre de ces nouvelles dispositions, les opérateurs d'importance vitale sont impatients de voir avec l'ANSSI les mesures qui vont leur être imposées pour sécuriser leurs systèmes d'information. Légalement, ces dispositions existent, techniquement, elles vont être d'autant mieux mises en œuvre qu'une prise de conscience par les responsables des entreprises interviendra ; de même dans l'administration. Toutefois, des investissements sont requis par ces objectifs en dépit des difficultés

économiques actuelles. De plus, des produits de confiance existent-ils déjà pour atteindre ces objectifs ?

S'il n'y a pas trop d'inquiétudes à avoir pour les opérateurs d'importance vitale, il est à craindre que les entreprises ou les collectivités locales, qui représentent environ 99 % des acteurs, soit ne feront rien soit achèteront des produits outre-Atlantique pour sécuriser leurs systèmes, ce qui n'est pas forcément le moyen de remplacer le recrutement d'un bon spécialiste.

La sensibilisation des responsables à ces problématiques est également une question essentielle. Au vu d'exemples concrets ou d'études menées auprès de responsables, notamment d'hôpitaux et plus généralement d'entreprises, il apparaît que cette sensibilisation est encore insuffisante.

Par exemple, l'analyse du Club de la Sécurité de l'Information Français, le CLUSIF, à propos d'un sondage auprès de responsables, révèle que ces derniers n'ont pas toujours conscience qu'investir dans la sécurité des systèmes d'information est fondamental. À titre d'exemple, les collectivités locales (départements, communes, etc.) n'ont pas forcément mis en place tous les outils qui permettraient de réagir à un incident. Lorsqu'un site *web* est attaqué, elles ne connaissent pas toujours immédiatement le nom de son développeur, ni les clés d'accès ni les mots de passe ni la manière d'obtenir les journaux. Or, il y a souvent des incidents de ce type.

Quant à l'usage indifférencié des outils informatiques professionnels ou privés, il importe d'abord d'être conscient du caractère sensible de l'information et de l'existence de telles technologies. Les employés viennent au travail avec des téléphones mobiles ou des clés *USB* personnels.

Quand un courriel professionnel doit être adressé à quelqu'un à l'autre bout du monde, la réflexion doit porter sur la méthode à utiliser pour son envoi. Même si les moyens classiques ne doivent pas forcément être écartés, il faut sensibiliser les informateurs manipulant des informations très sensibles. Mieux faut téléphoner qu'adresser un courriel. Cela laissera moins de traces et cela sera plus facile à contrôler. Mieux vaut sensibiliser les utilisateurs que d'avoir peur des technologies elles-mêmes.

Le dispositif de formation à la sécurité numérique de la Gendarmerie nationale évolue en permanence. Il y a 260 enquêteurs en technologie numérique qui suivent une formation donnant lieu à la délivrance d'une licence professionnelle délivrée par l'Université de technologie de Troyes. Une vingtaine d'enquêteurs ont ainsi été formés dans le cadre de la promotion 2013. Depuis 2005, en complément, plus de 1 000 correspondants locaux en technologie numérique (C-NTECH), basés dans les communautés de brigade, ont été formés à ce jour. Ils jouent un rôle de relais auprès des victimes et prennent les plaintes pour les infractions numériques (escroqueries, carte bancaire, etc.) et doivent savoir mener des enquêtes simples. Actuellement, une formation en ligne pour les premiers

intervenants a été développée dans le cadre d'un projet européen, en partenariat avec la police nationale française. Elle permet à tous les enquêteurs d'avoir accès à une formation de base sur ces questions-là.

En ce qui concerne la cybercriminalité et plus spécifiquement dans le cadre du traitement de données à caractère personnel au quotidien, des formations régulières sont dispensées aux gendarmes sur l'importance du contrôle d'accès aux bases d'informations judiciaires.

Quant aux solutions mises en œuvre dans d'autres États en matière de sécurité numérique, plutôt que de s'en inspirer, la Gendarmerie nationale constate que la France est plutôt bien positionnée voire souvent en avance comme pour la loi de 1978 ou d'autres législations. Que ce soit sous l'angle juridique ou technique, il ne semble pas qu'elle ait des leçons à prendre ailleurs. En revanche, il y a à apprendre d'un événement. Il vaut mieux être informé de la solution apportée par un État à un incident qui peut se propager à d'autres. Il faut donc être très ouvert aux échanges.

La protection assurée par les antivirus. Il faut d'abord que les antivirus détectent un certain nombre d'incidents sur l'ordinateur mais **ils ne sont pas capables de détecter les activités frauduleuses dans les réseaux eux-mêmes**. C'est important d'avoir une capacité de détection dans les réseaux. C'est ce que l'ANSSI a mis en place, avec succès, à l'aide de sondes dans les administrations. Les entreprises développent également des systèmes de ce type. L'antivirus n'est qu'une brique d'information dans l'ensemble très vaste que constitue le réseau. Trop souvent, aujourd'hui, des incidents sont issus de l'antivirus et non des activités suspectes sur les réseaux. Des progrès sont à réaliser. Une fois qu'un virus est installé dans le réseau, il peut contourner les antivirus. Donc, la solution n'est pas systématiquement dans l'installation d'un antivirus. La **formation des utilisateurs aux incidents dus aux antivirus** doit permettre une réaction adaptée aux problèmes techniques.

Nombre d'incidents quotidiens surviennent mais ce ne sont pas forcément des attaques. Des attaques très sérieuses, de grande ampleur, il y en a toutes les semaines, pas forcément toujours sur la même cible. Elles peuvent être assez graves. En ce moment, des attaques en déni de service surviennent pour rendre inaccessibles les systèmes d'information. De nouvelles techniques ont été développées récemment en utilisant des rebonds sur des serveurs de noms de domaine. Il en a été détecté de très efficaces et qui ne ciblaient pas forcément toujours la même victime. Il est donc **important d'échanger des informations sur tous ces incidents**. Aujourd'hui, il y a beaucoup trop de secret autour des incidents périodiques et, souvent, celui qui va vivre ces incidents ignorera si un acteur analogue a subi les mêmes, alors que, par exemple, de plus en plus, dans le domaine de la banque, une grande banque recherchera si une autre banque a subi le même type d'incident. Cela se fait beaucoup moins dans d'autres secteurs. Les directeurs informatiques des régions, des départements, des grandes

administrations gagneraient à communiquer plus souvent sur ce retour d'expérience.

Quant au cadre juridique européen et international, la gendarmerie est attentive à l'évolution de la **directive sur la protection des données à caractère personnel**. Cela a été malheureusement repoussé. La France est très dépendante de ce qui se passe dans d'autres pays car les données des Français sont souvent stockées à l'étranger, même si c'est en Europe.

Sur le plan de l'enquête judiciaire, pour réagir à des incidents, la gendarmerie est vraiment en difficulté car il n'existe pas d'outils internationaux importants de coopération efficaces. La situation n'a pas évolué depuis la Convention du Conseil de l'Europe sur la cybercriminalité de 2001. Il n'y a pas d'outils permettant de faire progresser la coopération avec les Russes, les Chinois, les Indiens ou d'autres, ce qui peut faire naître certaines inquiétudes. Il faudrait faire évoluer le droit sur cette coopération.

À propos des noms de domaine attribués par l'association de droits privés américaine *ICANN*, cette question comporte plusieurs aspects. En France, pour le « .fr » et les noms de domaine similaires, c'est la loi française qui s'applique. Même si ce système est américain, il autorise les particularités nationales.

Dans le « .fr », il y a des noms de domaine enregistrés aux Bahamas mais au profit de résidents chinois qui vendent des contrefaçons. Cela pose un problème car, normalement, les noms de domaine en « .fr » doivent être réservés à des résidents européens.

Déjà, s'il y avait davantage de contrôles ou de moyens en France pour contrôler l'office chargé de gérer ces noms de domaine, une meilleure sécurité serait possible. D'autant que lorsqu'une éventuelle victime voit un nom de domaine en « .fr », elle a confiance. Il convient donc d'être plus attentif. À l'international, cela est encore plus complexe.

Au-delà de l'attribution de noms de domaine par une association étrangère, il conviendrait **d'instaurer un dialogue entre un grand nombre d'acteurs aux intérêts économiques divergents ou aux intérêts collectifs divers**. Les dialogues avec les professionnels sont également utiles.

L'exemple de partenariat public-privé *Signal Spam* a déjà été évoqué. Il existe également un Centre expert contre la cybercriminalité français (CECyF) qui a été lancé le 21 janvier 2014, à Lille au Forum international sur la cybersécurité (FIC). Ce centre est une association de la loi 1901 qui rassemble les acteurs de l'État, des établissements d'enseignement et de recherche et des entreprises privées. Son but est de développer de façon partenariale des projets en matière de formation, de recherche et de développement et de prévention. Cela doit permettre d'avancer car l'ensemble des acteurs concernés est mobilisé pour des actions communes, par exemple la réaction à avoir lors d'un incident informatique, d'une attaque.

Les techniques utilisées dans les entreprises ou les organisations victimes et les personnes qui les conseillent sont les mêmes que celles utilisées par les enquêteurs en réponse à un incident : la criminalistique en anglais. Il faut pouvoir se former collectivement à ces outils, développer des outils communs. Or, aujourd'hui, **il n'y a aucun outil commercial français reconnu dans ce domaine**. On trouve des outils américains, israéliens, suédois. Pour l'analyse de disques durs, de téléphones mobiles, il n'y a aucun grand acteur français, seulement des toutes petites entreprises qui développent des outils et qu'il convient de soutenir.

Enfin, demeure l'importante question de savoir, à propos des collectivités locales, des petites et moyennes entreprises et des particuliers, vers qui ils doivent se tourner en cas d'incident. Aujourd'hui, rien n'est défini. Ils se tournent donc vers des amis, vers un service après-vente des matériels mais ils ne trouvent pas forcément de réponses quant à la sécurité.

Il serait souhaitable de développer des acteurs de proximité, des réparateurs en réponse à des incidents de sécurité ; ces personnes devant être capables de remettre en état un ordinateur, vérifier les virus qui l'ont affecté, comprendre ce qu'il s'est passé, expliquer à la victime ce qu'elle n'a pas bien fait. Or, aujourd'hui, ce genre de personne se forme sur le tas ou même n'existe pas. Ce type de service ou de formation n'existe pas.

De plus, l'information sur ces incidents ne remonte pas. L'ordinateur est remis en fonction mais la perte de données importantes ou confidentielles peut être à déplorer. Il faut donc développer des formations pour remédier à cela et créer cette chaîne incluant des réparateurs.

La France possède des capacités de formation (école d'ingénieurs, etc.) mais les petites entreprises du domaine de la sécurité numérique n'ont pas été bien soutenues et sont peu visibles, s'en plaignent et se font racheter par des géants étrangers. De plus, toute la chaîne sur le terrain jusqu'aux victimes peut créer des activités économiques et c'est là un rôle nécessaire. Peut-être demain, le vote se fera-t-il sur Internet ce qui suppose que les ordinateurs des particuliers soient sûrs ?

La gendarmerie a développé un petit triptyque pour les petites entreprises car 70 % des petites entreprises sont en zone gendarmerie. Sous la forme d'un fascicule sur la cybermenace, ce triptyque est destiné à aider ce type d'entreprises qui utilisent toutes Internet sans pour autant avoir un informaticien à leur disposition. Il existe un « Mois de la sécurité » au niveau européen, en octobre chaque année, mais rien ne se passe en France. Il faudrait davantage de dynamisme. Dans le cas du centre expert CECyF, un maximum d'initiatives locales et nationales seront lancées pour pouvoir faire se rencontrer et dialoguer les personnes qui travaillent dans ce domaine.

DIRECTION GÉNÉRALE DE L'ARMEMENT

M. Éric Bruni, chef du service de la sécurité de défense et des systèmes d'information

6 mars 2014

La Direction générale de l'armement assure la protection du secret de la Défense nationale conformément à l'Instruction interministérielle 1300 même si, à l'intérieur des systèmes, il y a des systèmes à protéger selon les préconisations de la CNIL.

Devant la nécessité de protéger les acteurs du secteur de l'armement face au risque numérique, la DGA, qui a la tutelle de l'industrie de l'armement, surveille, informe et forme l'ensemble des industriels travaillant pour l'armement en collaboration avec d'autres entités du ministère de la défense.

Cela concerne la majeure partie des industriels habilitée à traiter du secret de la défense nationale comme certains autres aux activités non classifiées. Se développe aussi, depuis quelques années, la protection du potentiel scientifique et technique de la Nation qui a été élargi à l'ensemble des laboratoires de recherche des universités ou autres, ou des écoles militaires de la défense. S'ajoute à cela le corpus réglementaire lié aux activités d'importance vitale qui résulte des directives nationales de sécurité (DNS).

Un volet très important est la déclinaison des réglementations en interne et chez les industriels avec des éléments décrivant les modalités de mises en œuvre pour cette protection. Un autre volet majeur est l'habilitation des entités travaillant pour la DGA comprenant un aspect relatif aux contrôles des infrastructures et en particulier les infrastructures informatiques.

Une autre action importante de la DGA porte sur le développement de technologies et, parmi les différents domaines d'interventions techniques, figure la cybersécurité pour laquelle sont développés des moyens de chiffrement en étroite collaboration avec l'ANSSI qui est un des acteurs majeurs du domaine.

En parallèle, un suivi régulier des industriels et des entités internes au ministère de la défense est mis en place au moyen d'inspections régulières réalisées par la DPSD et grâce à des audits de la DGA commandés par

exemple auprès de l'ANSSI, pour regarder en détails les réseaux utilisés par les industriels.

L'activité de sensibilisation et de formation est aussi très essentielle car il s'agit d'insuffler une culture de protection, certes plus présente au sein du ministère de la défense que dans d'autres activités de l'État pour combattre des comportements laxistes dans l'utilisation des moyens informatiques. Des séances régulières de sensibilisation permettent de faire prendre conscience du risque.

De plus, quelqu'un qui trouve une clé *USB* est très tenté de la connecter à son ordinateur pour voir ce qu'il y a dedans, ne serait-ce que pour le restituer à son propriétaire. D'autres peuvent être tentés de recharger leur téléphone portable ou leur *smartphone* sur leur poste de travail or, le téléphone portable étant un *modem* qui permet de dialoguer sur Internet, il constitue une voie d'accès pour un virus. Seuls les vieux téléphones ne craignent pas grand-chose.

Le centre de cyberdéfense de la DGA fait très régulièrement la démonstration de ce genre de prise de contrôle à distance d'un *smartphone*. C'est pour cela que, à la DGA, il est interdit, dès lors que sont évoquées des informations confidentielles, d'apporter des portables ; les téléphones sont laissés à l'extérieur de la salle.

Tous les industriels de l'armement sont concernés à des niveaux différents ; un certain nombre est érigé en opérateurs d'importance vitale, à savoir les plus gros et ceux qui interviennent sur des domaines très particuliers. Il n'y a que quelques opérateurs d'importance vitale mais un bon millier d'entreprises qui traitent du secret de la défense nationale et d'autres acteurs qui sont regardés de moins près puisque l'information qu'ils détiennent est moins critique.

En matière de souveraineté numérique, il y a encore une trentaine d'années, la défense poussait le monde civil en matière de nouvelles technologies. **Aujourd'hui, on ne sait plus développer une chaîne totalement souveraine pour fabriquer des ordinateurs ou des réseaux. Quelques équipements sont développés spécialement pour la défense nationale, en particulier le chiffrement**, totalement maîtrisé en national, presque étatique et sur lequel on fait reposer les principales architectures.

Les autres équipements sont issus du commerce et l'ANSSI et la DGA peuvent évaluer le risque pris en recourant à ces moyens. Les affaires de « portes de derrière » ou *back doors* présentes dans les logiciels de certains équipements inquiètent et font réfléchir. La presse a évoqué l'hypothèse que, dans des produits *Microsoft*, se trouvaient des moyens d'entrer pour la *NSA* malgré les protections apportées à ces produits. Il existe forcément des relations privilégiées entre un fabricant national, fournisseur de moyens réseaux par exemple et l'État où il se situe.

Si la souveraineté numérique est limitée, le cryptage est un domaine bénéficiant de beaucoup d'effort en France. Il est fondé sur des algorithmes mathématiques réputés sûrs, le temps pour les casser se compte en dizaine d'années, ce qui peut être encore insuffisant quand les informations à protéger doivent l'être sur des durées encore supérieures. Il en va différemment dans un sommet de chefs d'État ou même dans la transmission d'un ordre tactique sur un terrain d'opération.

En ce qui concerne le stockage de données dans des nuages numériques (*cloud*) les seuls éléments externalisés dans le nuage grand public sont des sites de communication institutionnelle dont les informations sont totalement publiques. En revanche, l'information du ministère de la défense, même non classifiée, n'est pas stockée à l'extérieur mais dans l'équivalent un nuage interne.

L'État réfléchit à un certain nombre d'actions pour **développer des nuages maîtrisés avec des fournisseurs français**. Pour la protection de l'information, il faut mettre en place une infrastructure qui la permette.

La confiance à accorder au stockage dans le nuage public est très limitée pour différentes raisons. Déjà, certaines réglementations étrangères sur la protection des données sont différentes de la législation française et **la confidentialité n'est pas assurée**. Quant à **l'intégrité des données**, **comment savoir** si l'information récupérée n'a pas été perturbée, volontairement ou non ? En termes de **disponibilité**, **de gros doutes** sont possibles. Quelques événements de fermeture temporaire de services ont existé chez *Google* ou chez d'autres. Ces aspects font naître le plus d'inquiétude notamment en cas de conflit.

La protection de l'information, la SSI, s'appuie sur ces trois critères de confidentialité, d'intégrité et de disponibilité. C'est au vu des exigences dans ces trois domaines qu'une stratégie est choisie. En effet, dans certains cas, il ne sert à rien d'avoir des informations très bien protégées si on ne peut y accéder.

La stratégie actuelle de la DGA, et plus globalement du ministère de la défense, est de **développer en interne des capacités de stockage délocalisées avec des fermes de serveurs et des baies de stockage** au sein du ministère de la défense que chacun peut exploiter pour ses travaux.

Outre le stockage des données, il existe le recours à des fonctions informatiques très évoluées, très intégrées, comme les fameux progiciels de gestion *ERP* tels que *SAP* ou autres qui peuvent intégrer, au sein d'une importante base de données, toutes les informations financières ou techniques d'une société alors qu'elles impliquent des exigences de protection variables. Par exemple, si la facturation peut parfois être orientée vers l'extérieur, d'autres activités doivent davantage être sécurisées. Tout cela, dans le seul et même système unifié fourni par un prestataire extérieur, peut conduire à se poser des questions en matière de protection de

certaines informations. Quelqu'un qui pénétrerait ce système aurait accès à toute l'information. Certes, ces progiciels mettent en place des chiffrements, toutefois la confiance en ces moyens ne peut être que variable.

L'externalisation et le nuage ne peuvent donc être envisagés qu'avec beaucoup de précautions pour les informations du ministère comme pour celle des industriels mêmes s'ils ont tendance à externaliser davantage.

S'agissant de l'articulation entre les approches prônées par l'ANSSI et la CNIL en matière de moyens de protection, la CNIL propose le même genre de démarche et de solutions que ce qui est développé et évalué avec l'ANSSI qui est le principal interlocuteur de la DGA.

Les moyens de l'ANSSI sont en croissance permanente et forte pour répondre à l'enjeu national. Du côté du ministère de la défense, les effectifs sont aussi en forte croissance dans les domaines technologiques et dans le domaine surveillance.

Une entité du ministère de la défense assure la surveillance et l'intervention sur les réseaux en cas de problème détecté, comme la simple introduction d'une clé *USB* sur un système qui a été mis sur Internet et qui peut ramener un virus à des cas plus complexes.

La DGA se fonde sur les analyses effectuées par l'ANSSI, sachant que ces analyses sont menées conjointement avec le ministère de la défense dans beaucoup de domaines, notamment pour les nouveaux types de risques qui apparaissent et les nouvelles solutions que l'on peut choisir.

La protection des données des opérateurs d'importance vitale passe d'abord par leur responsabilisation. Le code pénal les rend responsables de la protection de leur information. Il a aussi imposé des précautions et des recommandations.

Ces opérateurs sont régulièrement audités. Au nombre d'une trentaine, ils risquent par leur défaillance de mettre en danger le fonctionnement de l'État. L'effondrement de grands groupes mettrait en danger le fonctionnement de l'État. De même, à l'inverse, des industriels de l'armement qui fournissent de petits sous-ensembles ont un impact bien moindre. Mais l'analyse doit être menée entité par entité, système par système, pour déterminer les points de rupture qui doivent être protégés. La démarche est constante, très souvent menée en coopération avec l'opérateur, dans certains cas avec des moyens de rétorsion de la part de l'État. En cas de nécessité, des remises à niveau des réseaux industriels ou du réseau interne sont opérées. Tout cela repose sur **une approche dans la profondeur** car il ne s'agit pas d'ériger une barrière à la périphérie du système.

Aujourd'hui, tout le monde est parfaitement au courant des risques numériques. Mais les personnes ont un ressenti différent devant leur ordinateur ou leur téléphone familiers, alors **qu'il convient de se poser la**

question de la sécurité à chaque utilisation. Pour beaucoup de personnes, recharger son téléphone portable ne semble pas constituer un risque alors que cela peut être risqué. Le niveau d'information des acteurs et des industriels en général, de l'individu en particulier est très variable. Certains n'ont aucune connaissance informatique, il est alors très difficile de les sensibiliser. **Le guide d'hygiène informatique, édité par l'ANSSI, définit des grandes lignes assez simples pour se protéger**.

Quant à l'usage indifférencié des outils privés et des outils professionnels, au ministère de la défense et dans beaucoup d'entreprises, le fait d'apporter ses équipements personnels pour travailler est interdit, de même que tout transfert d'information.

Lorsque l'information circule par Internet, si elle est sensible, elle est chiffrée par des moyens agréés par l'ANSSI et, en l'occurrence, des moyens de chiffrement développés au sein de la DGA.

À la DGA, la nécessaire séparation entre le privé et le professionnel est rappelée très régulièrement.

À l'inverse, il est accepté une certaine utilisation personnelle des moyens professionnels comme le fait de recevoir des courriels privés sur le poste de travail, dans une certaine mesure et avec des restrictions. Il est possible d'aller effectuer des recherches sur Internet mais cela est encadré notamment par un engagement de reconnaissance de responsabilité signé par chaque agent précisant les droits et les limites de celui-ci. Aujourd'hui, interdire totalement ces pratiques ne fonctionnerait que pour quelques personnes peu connectées mais pour les jeunes ce serait illusoire sous peine d'avoir des difficultés à recruter.

À la DGA, la formation numérique constitue une priorité et commence par l'information avec la délimitation du droit de faire ou non. Des séances de sensibilisation régulières sont menées ; chacun en bénéficie tous les trois ans au minimum et, en cas d'erreur commise, de manière plus fréquente afin de lui rappeler les règles de comportement à suivre pour éviter de se voir supprimer son habilitation en raison quelques erreurs et afin de ne pas compromettre son parcours professionnel ultérieur.

Il existe une formation à l'utilisation des outils que l'on déploie, une formation aux techniques de protection de sécurisation ; il s'agit d'un vrai métier correspondant à une formation en commun avec l'ANSSI. Enfin, il y a la sensibilisation et l'information générale de tous les agents de la DGA.

Il peut arriver à la DGA de s'inspirer de solutions de protection promues dans d'autres États, de même que l'ANSSI discute avec ses homologues, ce qui permet d'ailleurs d'être informé d'attaques d'abord détectées par un pays étranger. Cela permet de gagner du temps. Le niveau de coopération technique et opérationnelle est fort mais on n'aura recours à un technicien opérationnel de communication de l'OTAN que pour des communications avec cette organisation.

Le fameux **téléphone *Teorem* chiffré** est utilisé au sein de l'administration. Auparavant, il fallait éteindre le téléphone et enlever la batterie. Mais éteindre le téléphone ne sert pas à grand-chose et on ne peut plus enlever la batterie, c'est pour cela qu'il vaut mieux déposer tous les moyens de transmission à l'accueil.

Il existe aujourd'hui des *smartphones* adaptés pour répondre aux besoins notamment pour y intégrer des moyens de chiffrement. Naturellement, la sécurité n'est assurée que si le téléphone sécurisé ne communique qu'avec un autre téléphone de même type. Mais tout dépend du niveau de protection souhaité. En effet, s'il ne s'agit que d'une information sensible, économique, et non pas de défense, il existe des téléphones du commerce qui possèdent des niveaux de protection raisonnables. Cela permet de se protéger d'un tiers mais non de celui qui a vendu l'équipement.

Le téléphone *Teorem* ou le réseau *Rimbaud* sont certes un peu contraignants mais sont utilisés en cas de réel besoin et cela fonctionne plutôt bien, le code étant relativement simple et la communication établie en une minute, ce qui n'est pas excessif pour un professionnel pour pouvoir parler librement ; ce qui est un bénéfice important, surtout s'il s'agit de parler par exemple aux ambassades. Toute autre solution est bien plus contraignante, comme la valise diplomatique, etc.

Il n'est jamais question de sécurisation totale car ce serait faux et dangereux de laisser croire que l'environnement est parfaitement sécurisé d'autant qu'il faut entretenir un certain sentiment d'insécurité, de la vigilance en permanence. De plus, mieux que de se cantonner aux antivirus, il faut procéder à une **approche en profondeur avec des barrières** à l'entrée des réseaux, des **murs** (*firewall*) qui filtrent certaines informations avec des antivirus et des **moyens de supervision** pour constater si quelque chose d'anormal se produit, comme lorsqu'un ordinateur consulte trop souvent un autre ordinateur ou un serveur ; il est alors possible de savoir ce qui se passe. Des **outils de chiffrage**, des **protections**, des **filtres** sont mis en place à différents endroits au vu des besoins pour améliorer le niveau de sécurité jusqu'à un seuil acceptable.

Il est évidemment très difficile de se protéger contre des virus inconnus dont la première apparition est, par définition, inattendue. La comparaison avec le virus, terme de médecine, est illustrative.

Tout le monde est attaqué. Les industriels sont souvent attaqués, davantage pour des raisons économiques que pour des raisons de défense. **Le ministère de la défense est attaqué très régulièrement mais possède des moyens de sécurisation adaptés**. Il n'y a pas eu de grosses attaques subtilisant de l'information mais plutôt des attaques d'effacements, de perturbations d'un site *web* pour changer les pages d'accueil. Récemment, des messages djihadistes sont parvenus à être affichés sur le site du ministère de la défense, des virus génériques ont pu être décelés mais il ne

s'agit pas d'attaques ciblées. Il y a une équipe permanente de l'État-major des armées qui intervient en cas de problème pour protéger les réseaux du ministère de la défense. Ces moyens sont consommateurs de ressources financières et humaines car il faut parfois réarchitecturer toute l'informatique avec des équipes assez conséquentes chez les industriels et au sein de la DGA.

Le principal axe de coopération rassemble la DGA, la DPSD, l'état-major des armées, l'ANSSI, la plupart des industriels pour rehausser le niveau avec les ressources disponibles.

Le cadre d'intervention de la DGA découle du code pénal qui traite de la protection du potentiel scientifique et technique, de la protection du secret de la Défense nationale, d'un certain nombre d'instructions interministérielles édités par le SGDSN.

Le cadre juridique européen est davantage lié aux aspects relevant de la CNIL. Quant au volet sécurité et défense, il est autonome.

Le fait que les noms de domaine soient attribués par une association américaine de droit privé n'entraîne pas de contraintes ayant des conséquences sur la sécurité informatique. Ce qui est ennuyeux, c'est lorsque les sites sont hébergés chez les industriels, notamment américains

Les recommandations en vue d'améliorer la sécurité numérique se fondent sur des études de la DGA pour améliorer des moyens, des équipements mais, en général, les recommandations découlent davantage de l'expérience dont l'échange de celle-ci entre les divers acteurs.

Il serait souhaitable que les décideurs en matière de sécurité informatique ne soient pas au cinquième niveau hiérarchique mais disposent d'un accès assez direct au patron. La sécurité informatique est très souvent vue comme un coût financier ou une perturbation de l'activité de l'entreprise le temps de reconfigurer les réseaux. Il est important que le responsable informatique ait accès au dirigeant de l'entreprise.

Il existe aussi un volet sensibilisation-formation tout à fait essentiel pour qu'une action de sécurisation soit efficace. La connaissance de ce que l'on veut protéger est importante, il faut donc identifier l'information à protéger. Cela nécessite de connaître ses systèmes, ce qui est ambitieux dans un ministère comptant 330 000 postes de travail et donc un nombre très important de systèmes, de sous-systèmes, de systèmes isolés ; il est nécessaire de les connaître pour bien les protéger. L'approche doit être globale et en profondeur. **Une protection d'une partie du système ne peut suffire si le reste ne l'est pas au même niveau**. Quant au niveau des ressources nécessaires, il peut sembler problématique.

DIRECTION DE LA PROTECTION ET DE LA SÉCURITÉ DE LA DÉFENSE (DPSD)

M. Philippe Le Bouil, lieutenant-colonel, chef de bureau

6 mars 2014

La DPSD est le service de renseignement du ministère de la défense qui lui permet d'affirmer son rôle d'autorité d'habilitation des personnels et de protection des biens, des personnels et des installations de la défense au sens large ; de même en ce qui concerne la détention d'information, pour l'industrie de défense et les industriels ayant des contrats avec le ministère de la défense.

Avant 1981, c'était la sécurité militaire qui s'occupait principalement du risque d'espionnage au sein des forces armées ; elle était le contre-espionnage des forces armées. Il y a donc eu transformation en service de protection des personnels contre les tentatives d'ingérence des services de renseignements étrangers, du crime organisé, du terrorisme international dans la sphère concernant le ministère de la défense et les industries de défense. Pour le reste des organismes ou personnels (enseignement supérieur et recherche, sécurité intérieure, agriculture, santé, etc.), cela relève de la Direction centrale du renseignement intérieur (DCRI).

La DPSD compte 1 100 personnes et a en charge la protection des installations et du personnel de la DGA, de l'État-major, des forces françaises, également à l'extérieur du territoire avec la protection des risques en particulier en Corse ou dans les DOM-TOM, incluant l'intérêt particulier d'autodétermination dans le Pacifique, cette mission incluant l'appréciation du niveau de risque auquel sont exposés les industriels et le personnel du ministère.

Le général Bosser, qui est à la tête de la DPSD, a été auditionné récemment par la commission des affaires étrangères, de la défense et des forces armées du Sénat.

La DPSD conduit trois types d'action ; d'abord des prestations adaptées (contrôles, inspections), ensuite du conseil et, enfin, de la sensibilisation.

La DPSD procède à des contrôles, des inspections au profit du cabinet du ministre de la défense notamment sur l'industrie ; la mission de conseil et de sensibilisation est de plus en plus prenante et appréciée des

partenaires industriels avec la **création de plates-formes de démonstration et de réalisation d'attaques informatiques**, notamment à partir du *smartphone* pour faire prendre conscience à des comités exécutifs, des comités directeurs, des chefs de projet, de la réalité du risque numérique. Dans ce champ d'action, la DPSD intervient dans un domaine différent de celui du contrôle régalien traditionnel de la protection du secret qui ne comprend pas ce volet risque numérique qui touche l'ensemble des citoyens.

L'organisation de la DPSD a été modifiée en fonction de l'évolution du risque numérique avec la création d'un poste d'officier supérieur de contre ingérence-cyberdéfense pour mener des actions dans le domaine du numérique cyberdéfense ou cybersécurité. Un officier de liaison de la DPSD existe aussi au sein de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), comme pour la DCRI et la DGSE depuis 2012.

Face à l'émergence et au toilettage de nouveaux textes réglementaires en vigueur, tout le volet cybersécurité a entraîné la signature de protocoles entre des acteurs du domaine, l'officier général en change de la cyberdéfense au sein de l'État-major des armées, l'amiral Coustillière, et notamment l'ANSSI.

Le rôle des différents acteurs en cas d'intervention, notamment dans l'industrie découle du code de la défense qui décrit bien l'action des armées, avec le rôle particulier de la DPSD dont découle le pouvoir de contrôler au sein des industries de défense en fonction d'exigences contractuelles.

Il existe aussi une action d'information particulière systématique des hautes autorités dans le cas d'attaques informatiques. Le vecteur du réseau interministériel sécurisé, *Isis*, est utilisé pour compléter l'information par des notes de renseignements classifiées « défense », adressées à la fois au SGDSN et à l'ANSSI, et nécessite que l'autorité de contre-ingérence au sein de la DPSD, à savoir l'officier général Noguier, correspondant pour la sécurité, soit informé de tous les incidents de sécurité. La direction générale pour l'armement est toujours en copie comme l'officier général cyberdéfense.

L'action de la DPSD a évolué pour prendre en compte le risque numérique.

La notion de souveraineté numérique a un sens, un peu comme la souveraineté énergétique, même si toute la chaîne n'est pas maîtrisée ; des plates-formes matérielles de stockage n'étant pas, par exemple, forcément maîtrisées de manière souveraine.

Les révélations récentes de M. Edward Snowden sur **le plan d'opération d'ensemble de la *NSA*** pour récupérer et exploiter les données des citoyens et des étrangers non américains sur tout le globe confirme la pertinence de cette notion de souveraineté numérique. Il y a eu aussi des révélations concernant **le piégeage des infrastructures de télécoms**, notamment par les Chinois. Il s'agit là aussi d'un signal fort. L'ANSSI aide le

ministère de la défense à promouvoir la notion de souveraineté nationale en matière numérique.

La définition de l'informatique dans les nuages par la DPSD rejoint la définition classique : **plus qu'une révolution technologique et économique, c'est une révolution entre les individus et l'outil numérique, et entre les individus eux-mêmes, qui vise à s'affranchir du matériel et à se consacrer à la satisfaction de besoins qui évoluent constamment**.

Cette offre d'informatique dans les nuages reflète la volonté de ne plus posséder de parcs informatiques permettant de domestiquer les besoins y compris lorsqu'ils sont évolutifs, avec de petites pointes d'activité en cours de journée, dans une semaine ou dans une année. Par exemple, les plates-formes de vente sur Internet, quand il y a des pics de charge d'activité, ont un besoin de nomadisme qui émerge et qui pousse certains opérateurs du numérique à offrir des services dématérialisés**. Le besoin est satisfait au détriment de certaines exigences de sécurité.**

C'est un peu comme l'évolution des modes de transports au cours du siècle dernier : il fallait posséder un vélo pour aller au bureau, une voiture pour aller chercher ses courses, une autre de grand tourisme, un avion ou un bateau à titre privé pour partir en vacances. Aujourd'hui, il existe des services payants où le droit d'usage est vendu (*Vélib'*, *Autolib'*, transports en commun, etc.). On n'est plus obligé de posséder de véhicules pour pouvoir satisfaire un besoin physique. Il en est de même de l'informatique dans les nuages.

Quant à la confiance, la différence est en termes de risque car l'informatique conserve les données qu'elle va transporter mais on ne sait pas où est situé le matériel ni qui va traiter, stocker ou diffuser des données. **La notion de confidentialité est perdue**.

Or, **en matière de sécurité informatique, on parle de trois familles de besoins de sécurité : la disponibilité, la sécurité et la confidentialité. L'informatique dans les nuages permet de satisfaire la disponibilité, l'intégrité, dans une grande mesure pour certains services grands publics, mais la confidentialité est totalement exclue.**

L'informatique dans les nuages repose sur une architecture mondialisée. En ce sens, l'initiative de nuage souverain français, *Cloudwatt*, par exemple, a été prise par des industriels français sur le territoire national. Il s'agit-là d'une bonne initiative de nature à garantir la confidentialité. Cela semble répondre aux besoins mais cette firme est également confrontée à la logique économique qui pousse les gens à aller dans l'informatique dans les nuages. Les budgets traditionnellement consacrés à la satisfaction du besoin de parc informatique du citoyen sont grevés d'autant.

Pour des raisons de besoins de nomadisme ou d'accès aux messageries, chacun est tributaire de l'opérateur auquel il confie ses données. Le nuage souverain devrait répondre à cette attente. En principe,

les consortiums d'opérateurs ont pris en compte cet objectif de souveraineté. *Bull, Dassault Systèmes, Orange Business Services, Thales* ont compris qu'il y avait **un besoin de redondance nationale**.

Il y a actuellement une inflation des données. Les organisations, les administrations et les industriels eux-mêmes ont tendance à tout conserver, à numériser de plus en plus, à archiver. De plus, il existe une tendance naturelle à conserver et à augmenter la taille des pièces jointes. Le moindre document est chargé d'images d'animation qui pèsent lourd ; en outre, par défaut, par facilité, il est transmis à une quinzaine de destinataires.

Les opérateurs sont là pour organiser la redondance en cas de défaut d'un *data center*, l'existence de capacités de calcul à fournir à un moment donné, par exemple des besoins très forts au moment de la paye, vers le 20 ou 25 du mois. Après, il y a une baisse de charge ; les *data centers* répondent à ce besoin notamment avec des études de prospective montrant l'inflation du nombre de données mais ils consomment beaucoup d'énergie. À noter qu'il existe des plans pour construire de tels centres en Scandinavie pour résoudre à la fois le problème de leur refroidissement et celui du chauffage des habitations.

C'est un des enjeux de *Google* et d'*Amazon* de rendre leur facture énergétique la moins polluante possible. Cependant, **la consommation d'énergie et la pollution de ces *data centers* sera un des problèmes majeurs des prochaines années**.

À noter des différences d'appréciations : l'opérateur qui va vendre un service disponible va dire qu'il est sécurisé tandis que le service de renseignements, lui, se focalisera sur la perte de traçabilité du stockage des données, ce qui aiguise l'appétit de certains.

L'ANSSI et la CNIL ont des périmètres très différents. La CNIL protège l'individu tandis que l'ANSSI protège les organisations, les opérateurs d'importance vitale et les administrations**. Il manque aujourd'hui la protection des données stratégiques.**

La protection de données à caractère personnel est indispensable. Il s'agit de protéger les libertés individuelles, ce qui conduit la CNIL à diminuer la durée de détention des données à caractère personnel. Mais, également, il existe une volonté de **protéger les données plus longtemps pour conduire des investigations quand des attaques numériques seront découvertes ultérieurement. La CNIL souhaite une durée de protection de trente jours à six mois maximum tandis que l'ANSSI et la DPSD préféreraient une quinzaine d'années**.

En effet, en ce qui concerne les attaques sous forme de vol de données, il faut savoir qu'**un vol de données nécessite, en moyenne, trois cents jours pour être découvert,** soit de quelques jours à plusieurs années, selon les cas. Une durée de conservation trop brève affaiblirait la confiance dans le réseau informatique et rendrait très difficile la quantification des

pertes. Si l'on suivait les préconisations de la CNIL à la lettre, il ne resterait donc que trente jours ou quelques semaines pour mener des investigations. Il y a là, encore une fois, une différence de point de vue entre la CNIL et l'ANSSI car la CNIL et l'ANSSI n'ont pas du tout les mêmes centres d'intérêts ou de périmètres.

Aux yeux de la DPSD, les moyens de ces deux acteurs sont insuffisants notamment en matière de capacité de contrôle. C'est ainsi qu'un ancien agent de la DPSD, actuellement à la CNIL, mène un très intéressant travail de veille sur la dérive des nouveaux usages et des nouvelles technologies. Comme les moteurs de recherche et les plates-formes stockent un certain nombre de données à caractère personnel, l'adéquation est recherchée entre la demande et l'offre pour éviter l'intrusion dans la sphère privée.

Les guides publiés par l'ANSSI sont destinés à acculturer les industriels à la sécurité numérique. La DPSD a besoin de la production de la CNIL. Des initiatives prises en ce sens sont toujours relayées par la DPSD.

Les guides de l'ANSSI participent à la bonne évolution de la sécurité des industriels. Par rapport à la CNIL, **l'ANSSI a l'avantage de se concentrer sur le curatif**, notamment face à des attaques ciblées de grande ampleur. Cela doit être relayé. Mais pour en profiter, cela suppose d'avoir du personnel formé.

Pour la protection des opérateurs d'importance vitale, il existe les **directives nationales de sécurités (DNS)** qui sont fondamentales car, dans le paysage de l'industrie de défense, elles opèrent des distinctions par secteur d'activité. Ceux du secteur défense respectaient déjà des exigences de sécurité mais **les textes anciens minimisaient le risque économique et l'importance de la sécurité des systèmes d'information**.

La DPSD participe avec l'ANSSI et ses partenaires sectoriels à un **travail de refonte des directives nationales** pour y intégrer des paragraphes, des chapitres plus contraignants, plus adaptés en matière de menaces numériques. Par exemple, le risque de sabotage, d'attentat terroriste est très bien pris en compte par ces directives nationales ; l'opérateur traite ce risque en ayant une protection physique adaptée de son site industriel mais, pour la sécurité numérique, il apparaît parfois un flou qui peut donner lieu à des dérives de l'informatique en nuages, d'infogérance ou de sous-traitance non maîtrisées.

Ces directives avancent secteur par secteur ; c'est un travail d'autant plus délicat qu'existe la volonté de soumettre l'évolution des textes à un groupe représentatif d'opérateurs d'importance vitale pour qu'ils critiquent le texte, cela prend donc du temps. Le but serait d'aboutir à un texte qui permette vraiment de traiter le risque et non un texte régalien supplémentaire qui serait inapplicable.

Cela rejoint l'évolution de la loi de programmation militaire. Cette bonne initiative a, du point de vue de l'industriel, un impact en termes de coût, de budget qui ne doit pas paupériser l'industrie de défense. Ces exigences supplémentaires passent par le **cloisonnement maîtrisé des réseaux informatiques internes** qui participent à cette production industrielle dont l'absence grèverait la souveraineté nationale. Il faut des cloisonnements plus forts, des capacités informatiques strictes et de détection d'incident soit en interne soit à l'extérieur.

Par exemple, un petit opérateur d'importance vitale, comme *Lacroix tous Artifices*, qui produit des détonateurs qui sont vitaux pour les forces françaises, n'a pas du tout les moyens d'avoir une protection informatique tandis que *Dassault, Thales*, *DCNS*, groupes de portée mondiale possèdent des ressources d'expertise en interne dans le domaine numérique et informatique. La directive nationale de sécurité s'appliquant quelle que soit la taille de l'entité, il convient d'introduire des nuances dans son texte.

L'opérateur d'importance vitale s'appuie sur l'écosystème industriel et la sous-traitance, sur ses partenaires industriels. **Les exigences résultant de la directive nationale de sécurité devraient se propager à tout le secteur** mais il est très difficile de tracer la frontière entre l'importance vitale et la production de sous-ensembles à double usage ou qui n'ont pas le caractère de Défense nationale très affirmé. Selon le retour d'expérience, l'exigence réglementaire commune en matière de sécurité, contrôlable par la DPSD, peut se traduire chez l'opérateur, vis-à-vis du sous-traitant, par une exigence contractuelle. Le contrôle permettra de voir si l'opérateur exerce le contrôle idoine. À ce titre, **les normes internationales de type *ISO* sont d'un grand secours**. De plus en plus, des grands intégrateurs industriels exigent de leurs sous-traitants le respect des **normes *ISO* 27 000 ou *ISO* 31 000**, ce qui **couvre le risque numérique et la gestion du risque**. De bout en bout de la chaîne de production industrielle, il est possible de mesurer le respect des exigences de sécurité.

Les notions actuelles d'entreprise étendue, d'entreprise numérique, de mélange entre le professionnel et l'individuel, ne favorisent pas du tout le respect de la sécurité.

La sanctuarisation des sites industriels des chaînes de production, comme celles de l'industrie lourde du XIX^{e} et du XX^{e} siècle, n'est plus possible. Il s'agit maintenant de sous-traitance et de la valeur d'un patrimoine informationnel complètement dématérialisé et donc difficile à protéger. Cette protection éveille un écho favorable chez **les opérateurs d'importance vitale qui ont bien compris que c'était de leur patrimoine et de leur survie** qu'il s'agissait dans le contexte espionnage économique ; les attaques conduisant au pillage des ressources de la recherche et du développement.

Les divers acteurs ne sont pas toujours à même de se protéger du risque numérique, tout dépend de leur taille. Certains sont encore en train

de découvrir qu'il existe des risques liés à la numérisation. Dans le même temps, ils sont contraints de se doter d'outils structurants (progiciels de gestion, outils numériques, etc.), de prendre le virage du numérique.

L'usage indifférencié d'outils informatiques mélangeant données de la vie privée et données professionnelles fait courir des risques spécifiques. C'est la rançon du succès de ces outils numériques qui facilitent le travail mais, si l'on veut qu'ils soient adoptés par tous les acteurs, il faut que chacun y trouve un intérêt et puisse s'en servir quotidiennement. Cela rejoint la protection de la vie privée et les problématiques couvertes par la CNIL. **Les initiatives de la CNIL participent aussi à la diffusion de comportements maîtrisés, à titre personnel ou professionnel. L'évolution des usages, avec les paiements sans contact ou les données à caractère personnel de santé sur l'ordinateur personnel ou professionnel, vont faire converger les besoins de sécurisation**.

Les sensibilisations effectuées par la DPSD au moyen des plates-formes de sensibilisation trouvent un écho dès que chacun comprend que cela atteint aussi sa vie privée.

La DPSD accorde une **priorité à la formation au numérique** mais il est difficile avec 1 100 personnes de prendre ce virage rapidement. Des formations d'adaptation interne sont dispensées mais pâtissent de la **pénurie de ressources humaines** dans les directions centrales parisiennes, victimes du succès de la cybersécurité, ou à l'État-major des armées. Il n'y a pas assez de jeunes, ou même d'anciens, formés et motivés. **La sécurité informatique, c'est une tournure d'esprit ; il existe pour le développement de celle-ci un bon vivier en France**. La particularité des services de renseignements est d'avoir un personnel donné par les armées, notamment des militaires. Les besoins des services de la DPSD ne sont pas toujours honorés ou encore les personnels formés sont parfois récupérés par les armées. Ce droit de tirage sur les armées est intéressant mais, dans le contexte actuel, chacun souhaite conserver ses experts.

Quant à s'inspirer de l'amélioration des techniques de sécurisation des données mises en œuvre dans d'autres États, la DPSD ne se sent pas obligée d'adopter les solutions déjà adoptées ailleurs. Elle donne la priorité au respect de l'arsenal réglementaire déjà existant. **Des ressources nationales de qualité existent pour la cryptographie** sans besoin de s'inspirer d'exemples étrangers.

La question de la confiance dans les outils numériques rejoint la problématique de la souveraineté. **Aujourd'hui, les fabricants de matériel informatique, vendent de plus en plus des ensembles ou des sous-ensembles, des serveurs d'ordinateurs qui ne sont pas nationaux. Il y a un risque dans ces matériels. Il faut accepter ce risque et le traiter**.

Les grands acteurs du développement logiciel, des systèmes d'exploitation sur lesquels repose toute la confiance dans les outils

numériques, que ce soit *Apple*, *Android* ou *Microsoft*, sont américains et ne sont pas de confiance. Il y a donc un risque.

Les solutions de sécurisation reposent sur les capacités d'investigation des paquets Internet, sur des ressources en national mais il existe les mêmes difficultés que pour les autres acteurs à faire adopter ces outils qui portent atteinte aux libertés individuelles.

Comme les antivirus ne couvrent pas tous les risques du numérique, la protection assurée par les antivirus doit être complétée par l'importante défense en profondeur. Il s'agit de **l'empilement de briques de sécurité** qui permet d'accorder un certain niveau de sécurité aux outils et aux usages que l'on en fait. L'outil informatique comprend des mises à jour de sécurité des briques matérielles et logicielles car **les composants ne sont pas développés de façon suffisamment sécurisée et comportent des failles de sécurité**. Tout un écosystème vit de la détection, de la production et de la vente de ces failles de sécurité.

Le développement de certains comportements à risque peut affaiblir le meilleur outil informatique et le meilleur antivirus. Par exemple, lors de la navigation sur des sites non sécurisés ou comportant des pages ou des liens piégés, le comportement est essentiel.

Or **il manque aujourd'hui un volet que veulent couvrir les directives nationales de sécurité : c'est la préparation à la gestion des crises, la détection, la mise en œuvre de procédures de secours, de continuité d'activité**. Aujourd'hui, ce risque est très peu pris en compte et pas de manière mûre.

Les opérateurs du secteur bancaire ou de l'assurance disposent déjà d'un arsenal normatif qui permet de contraindre les opérateurs à la prise en compte de cette problématique de la continuité de l'activité en cas de la crise majeure, voire la production de comptes rendus d'exercices de gestion des crises et de secours.

Dans la défense, si le contrat ne spécifie pas des exigences fortes, en cas de crise ou de guerre, l'industriel n'est pas tenu d'avoir un outil résiliant, redondant, du moment qu'il respecte le rythme de livraison industrielle forcément ralenti par le contexte économique.

La prise en compte de briques de sécurité doit être complétée par un volet opérationnel et un comportement ; tout cela suppose un accompagnement. **Il faut passer d'une culture du coffre-fort numérique et de la confiance dans l'outil à une culture de la gestion du risque. On ne peut plus faire confiance à l'outil numérique**. L'apprentissage du numérique par les jeunes passe par cette affirmation nouvelle qu'**il ne faut pas faire confiance à l'outil** alors que, pour l'automobile et les transactions bancaires, une confiance aveugle est faite aux dispositifs de sécurité.

À propos des attaques subies par les divers acteurs du secteur de la défense, un certain nombre d'entre elles a été publié. Le secteur de la

défense, l'aéronautique, le spatial, le nucléaire l'informatique et les télécommunications sont des secteurs de convoitise pour les industries étrangères, d'où beaucoup de tentatives d'intrusions informatiques contre ces secteurs.

Les effectifs et les moyens pour y parer, ce sont d'abord ceux mis par les industriels à partir de leur perception des risques encourus pour leur cœur de métier. Comme l'a déjà fait l'armement terrestre, **l'informatique est souvent complètement externalisée par les entreprises ainsi que la supervision de sécurité**. Un dialogue avec ces opérateurs est entamé pour qu'ils sachent **conserver une visibilité de ce qui se passe en termes d'événements de sécurité, de signaux faibles**, qui leur permettraient de déclencher les investigations en faisant du préventif et du curatif.

Pour faire face aux attaques informatiques menées à des fins d'espionnage, la DPSD a mis en place un personnel au plus près des régions, un maillage territorial. L'ensemble des 1 100 personnes ne se situe pas à Malakoff ; les autres sont présentes dans le maillage territorial ; il y a des experts zonaux au plus près du terrain pour sensibiliser les personnels à des réalités qu'ils ne mesurent pas forcément. Un renforcement des effectifs des personnels au plus proche des régions, des industriels, est souhaitable pour prodiguer des conseils de manière décentralisée. D'autres personnels procèdent à des contrôles.

Un effort en vue du **renforcement des effectifs** est en cours à partir de transferts des postes et des efforts du général Bosser pour stabiliser les effectifs de la DPSD tout en renforçant le volet d'expertise notamment dans le domaine numérique. **Seulement une trentaine d'experts**, sur les 1 100 personnes en direction centrale ou en région, **se consacrent au traitement des incidents informatiques** et ont participé, en lien avec l'ANSSI, à certaines interventions liées à la défense. La DPSD est capable d'accompagner et de faciliter le travail de l'ANSSI en caractérisant un peu le paysage industriel dans lequel leurs inspecteurs évoluent.

Les solutions de sécurisation face aux risques du numérique sont celles prônées par l'ANSSI dont les bonnes pratiques sont **en accord avec le cadre juridique européen**.

Davantage de réserves peuvent être exprimées sur le cadre juridique international devant l'espionnage numérique industriel. Cela se heurte à la juridiction de certains pays, notamment à l'occasion de la **rétention des outils informatiques aux frontières**. La DPSD participe à l'évaluation de ce risque car les ingénieurs français, quand ils vont répondre à des appels d'offres à l'étranger, avec leurs ordinateurs remplis de données stratégiques sous le bras, voient parfois leurs appareils retenus à la frontière des États-Unis d'Amérique, d'Israël, de certains pays du Golfe ou de la Chine, très friands de rétention numérique aux dépens des ingénieurs français. **Des parades réglementaires et légales, comme le chiffrement de disques,**

doivent être trouvées pour conserver la maîtrise des données tant que les contrats en négociation ne sont pas signés.

À souligner aussi les risques liés aux audits intrusifs en raison du respect de certaines réglementations comme celles de l'aéronautique américaine (réglementation *ITAR, International Traffic in Arms Regulations*). **Une réponse juridique adaptée est à trouver** face à des acteurs qui se présentent avec un arsenal de règlements à respecter qui leur donne le droit de se faire présenter un certain nombre de résultats d'investigations numériques. Cela suppose aussi un **important changement de culture**. Il n'existe pas aujourd'hui de réponse stricte et adaptée à un audit légitime de *Microsoft* ou de *SAP* pour vérifier l'absence de licence pirate. Mais, pour permettre que ce genre d'audit se réalise dans le respect de toutes les lois, il faut l'accompagner.

La gestion des noms de domaine par l'*ICANN*, structure américaine, pose un problème puisque cette société, de droit américain, donne des facilités d'accès aux sites *web via* les moteurs de recherche.

Mais ce n'est qu'une brique dans la sécurité d'Internet. Cela fait partie de la neutralité de l'Internet car **le moteur de recherche a autant d'importance que le nom de domaine**. Si *Google* accorde des préférences à certains domaines, c'est aussi important que l'attribution de certains noms de domaine. **Il suffirait d'avoir une sorte de moteur *Google* souverain français pour pallier les risques et les vulnérabilités de l'attribution des noms de domaine par une société américaine.** Au total, **le fait que les noms de domaines, les moteurs de recherche et les géants de l'Internet soient concentrés dans des sociétés de droit américain et situés dans la même zone géographique fait courir un certain nombre de risques et pose un problème d'accès à l'information**. Cela peut se traiter par des outils alternatifs.

Pour améliorer la sécurité des acteurs de la défense face au risque numérique, la DPSD recommande surtout la lecture d'études publiques qui modifient la perception des risques : les rapports des éditeurs de sécurité, par exemple, le rapport *Mandiant* qui cible une unité de l'armée populaire de libération chinoise comme ayant mené des attaques ciblées contre des sites industriels, des administrations européennes, mondiales depuis quelques années ou encore des rapports de cabinets de sécurité, comme le cabinet américain *Kaspersky*. **Un certain nombre d'études publiques pousse à augmenter la vigilance face au risque numérique.**

La loi de programmation militaire et la révision des DNS sont des leviers d'action, au moins pour une vingtaine d'opérateurs d'importance vitale du secteur de la défense parmi les 2 000 sociétés appartenant à l'écosystème de l'industrie de défense française. Les DNS et la LPM permettront, à terme, de traduire les exigences de sécurité qui devraient bénéficier à l'ensemble de la sécurité de défense.

Les initiatives de nuages souverains, l'émergence d'une offre de prestataires de services de sécurité français de type *Cassidian*, *Thales*, détectant et supervisant pour ceux dont ce n'est pas le métier, constitueront autant de sociétés à conseiller aux industriels à travers un appel à la concurrence. Aujourd'hui, ce secteur souffre du nombre restreint d'acteurs et de prestataires de services de confiance nationaux.

CLUB DES DIRECTEURS DE SÉCURITÉ DES ENTREPRISES (CDSE)

M. Alain Juillet, président

19 mars 2014

Tout d'abord trois constats peuvent être faits. En premier lieu, en France, les entreprises ont d'abord souhaité protéger leur capital physique et leur capital matériel mais, avec le rapport Jouyet-Levy est arrivé le concept de capital immatériel. On s'est rendu compte qu'il fallait **protéger ce type de capital** car c'est là que se trouvent les parties les plus intéressantes de l'entreprise et celles sur lesquelles pèsent le plus de risques : les brevets, les savoir-faire, la recherche, les formules. Aujourd'hui, tout le monde est conscient que **la défense du capital immatériel devient un problème majeur.** D'autant plus que, avec l'évolution du numérique, il est de plus en plus facile de pénétrer les entreprises.

Sur ce point, je fais mienne la phrase de M. Patrick Pailloux, ancien directeur général de l'ANSSI, disant : *« quand je vois un responsable de la sécurité informatique d'une entreprise, un DSI, m'affirmer qu'il n'y a pas eu d'intrusion chez lui, je me dis que c'est soit un menteur soit un incompétent »*. Tout le monde se fait attaquer et tout le monde sait qu'une partie des attaques réussit. C'est le premier constat.

Le deuxième constat, c'est la prise de conscience qu'il faut impérativement protéger ce capital immatériel mais que, les intrusions réussies étant en croissance rapide, la protection technique n'est plus la solution suffisante. On débouche alors sur la pratique du secret des affaires sur lequel des travaux sont actuellement en cours. Il ne faut pas le confondre avec la conception militaire du secret qui amène à mettre des tampons allant de la diffusion restreinte au secret défense pour empêcher l'accès et sécuriser l'information. **Dans l'entreprise, il serait trop onéreux de tout défendre, ce qui amène à faire des choix en définissant ce qui est vital pour la survie et l'avenir. Il faut identifier ce que l'on doit réellement protéger par tous les moyens utilisables.** En se livrant à cet excellent exercice, on s'aperçoit que, **la partie du patrimoine immatériel à sécuriser totalement est relativement restreinte.**

Troisième constat : lorsque l'on veut protéger le cœur de l'entreprise, la justice française est très laxiste, non pas du fait d'un relâchement, mais

parce que **la loi n'a pas prévu la situation du numérique.** Les lois, très bien faites pour d'autres domaines, sont mal adaptées au domaine du numérique.

Par exemple, lors d'une attaque numérique, le *hacker* professionnel pilote son action de n'importe quel pays du monde, sauf s'il s'agit d'un petit *hacker*. Il prend le contrôle d'ordinateurs relais qui vont lui servir pour en asservir d'autres qui, eux-mêmes, seront le support pour récupérer des informations chez vous. Quand vous voudrez vous défendre en justice, on vous objectera que les ordinateurs utilisés étaient situés dans des pays étrangers, soumis à une législation différente de la nôtre et que l'on n'est pas sûr de l'origine réelle de l'action. L'internationalisation des pratiques pose un vrai problème.

À l'étranger, **les États-Unis d'Amérique sont d'autant plus rigoureux et efficaces qu'ils disposent du droit de suite ; ils considèrent leurs lois comme supranationales.**

Dans ce cadre, si un soupçon d'illégalité vient à peser sur une entreprise française, en vertu de la loi *Discovery,* qui s'applique en France, le juge américain pourra demander qu'on lui communique toutes les pièces du dossier sans qu'il y ait une instruction ouverte dans notre pays. Certes, il est possible de refuser car, heureusement, il existe une loi en Europe et en France interdisant de transférer des secrets d'une entreprise. Mais les Américains précisent alors à l'entreprise visée qu'elle aura des problèmes d'entrée aux États-Unis et qu'elle risque de ne plus jamais pouvoir y conclure d'affaires. Devant cette éventualité, les entreprises françaises communiquent les dossiers...

Il existe donc un déséquilibre dans le combat entre nations puisque, d'un côté, il y a ceux qui peuvent aller partout chercher de l'information et exercer des pressions et, de l'autre, nous qui ne pouvons pas.

Les Chinois ont des lois extrêmement contraignantes chez eux et surveillent tout. Les États-Unis d'Amérique font de même tout en prétendant le contraire. Il ne faut pas oublier les Russes qui ne sont pas mauvais du tout, même s'ils n'ont pas la capacité de développer des technologies aussi pointues que les Américains ou les Chinois.

Il existe un autre grand problème face auquel on est complètement démuni : l'identité numérique. Dans une entreprise comme dans une administration, il y a de l'information qui circule partout vers l'extérieur avec Internet, ou à l'intérieur avec l'Intranet entre les salariés, les cadres, etc. Lors de ces multiples échanges avec l'administration, des collègues, des concurrents, ou des clients, le **problème majeur réside dans l'identification de la personne avec qui on échange.** Même si celle-ci est soumise à une authentification par son adresse *IP*, cela ne permet pas de savoir qui est véritablement en face.

Un premier exemple de cela a été fourni, il y a deux ans, par ce qu'on a appelé les attaques à la nigériane qui ont touché une bonne partie

des entreprises du CAC 40. Le vendredi soir, le directeur financier d'une de ces sociétés recevait un courriel interne de son président, reconnaissable aux formules utilisées habituellement par lui, pour ordonner impérativement le virement immédiat de quelques millions d'euros à tel compte dans tel endroit, et précisant que cette opération entrait dans le cadre d'une négociation en cours cette fin de semaine d'où la nécessité d'envoyer un acompte pour conclure, à payer dès réception du courriel. Étant tenu par le secret, je ne vous dirai pas le nom et le nombre des entreprises françaises tombées dans ce piège : ce n'étaient pas les plus petites.

Comme des messages de son chef parvenaient tous les jours au directeur financier, il se contentait de joindre l'assistante du président qui lui confirmait que le président était absent puisqu'il était en train de conduire une négociation. Ce qui validait le contexte du courriel. L'argent était alors viré sur un compte qui, dans la seconde, était vidé par le récepteur. Quand, le lundi matin, le directeur financier informait son président qu'il avait versé la somme demandée selon ses instructions, celui-ci s'étranglait, voulait connaître les détails de l'histoire et déclenchait l'alerte mais trop tardivement pour bloquer le processus.

La police ne pouvait que constater l'escroquerie faite à l'entreprise le vendredi ou le samedi. La DGSI et l'ANSSI n'avaient plus qu'à lancer une enquête administrative et technique. Alors que la seule réaction valable aurait dû être d'alerter *Tracfin* qui est la seule entité capable de remonter très rapidement un circuit financier en France et à l'étranger. Ce service a les moyens de repérer le trajet suivi par le virement et de le bloquer en cours de route puisqu'il s'agissait d'une opération de vol et de blanchiment. Mais *Tracfin* ne peut agir en l'absence de décision de justice.

Il faut savoir que la préparation de telles attaques par des organisations criminelles peut prendre des mois compte tenu de l'importance de l'enjeu, d'autant qu'elles doivent présenter toutes les apparences de la réalité.

Dans ce même registre, j'ai été le témoin direct d'un appel téléphonique dans le bureau d'un président d'un groupe français : il s'agissait de l'appel du directeur de cabinet d'un président africain qui lui rappelait les circonstances de leur dernière rencontre et l'informait de la création d'une fondation en France pour laquelle il souhaitait obtenir de la société une participation de 200 000 €. Le président a argumenté quelques minutes puis a fini par accepter en prenant bonne note de la banque, située en France, à laquelle cet argent devait parvenir avant la visite prochaine du président africain. Comme le président de la société se déclarait sûr d'avoir réellement parlé au directeur de cabinet, qui avait laissé un numéro de téléphone, je lui ai conseillé de rappeler ce numéro en Afrique où le directeur de cabinet lui a confirmé que c'était bien lui qui venait d'appeler. J'ai alors cherché les numéros de téléphone officiels de la présidence de la République de ce pays africain et constaté que le numéro donné n'existait pas.

Donc le système actuel n'est pas en mesure de lutter efficacement contre la fraude numérique alors qu'avec Internet de telles attaques se multiplient. **Le problème majeur est celui de l'authentification de l'interlocuteur.** Cela concerne aussi l'administration. Par exemple, quand le fisc notifie un redressement à un particulier, il y a des personnes qui vont vérifier s'il s'agit réellement du fisc mais d'autres non. L'origine de la messagerie électronique semble faire foi.

Le problème de l'authentification de celui qui vous parle, qui vous appelle ou de celui à qui vous voulez parler ou avec lequel vous souhaitez échanger, est un problème majeur. Aujourd'hui, face à cela, **nous sommes totalement sous-équipés.** Pourtant, il y a de petites sociétés, françaises ou étrangères, qui ont mis au point des systèmes d'authentification performants. Au niveau national, il va falloir rechercher un système qui donne satisfaction à tout le monde et le mettre en place en l'imposant progressivement en commençant par l'administration.

Pour les déclarations fiscales aujourd'hui, les formalités débutent par un certificat d'identification, suivi de l'entrée de plusieurs codes. Les services des impôts sont bien les seuls à prendre de telles précautions. Cela étant, si les services des impôts se font prendre, ils ne le diront jamais.

Dans les entreprises, il faut déjà mettre en place un système d'authentification interne pour vérifier si ce sont bien les employés, les clients et les sous-traitants de l'entreprise avec lesquels on entre en contact.

Les grandes entreprises sont également au cœur du problème avec des sous-traitants qui gravitent autour d'elles. Leurs systèmes de sécurité sont connectés avec celui de l'entreprise principale avec laquelle ils ont des échanges permanents, donc des interconnexions. Si ces sous-traitants n'ont pas mis en place des systèmes de sécurité sérieux, **ils vont constituer des lieux de passage pour les *hackers* cherchant à entrer dans le système principal.** Ce problème existe aussi pour toutes les petites PME et PMI qui travaillent dans l'orbite des grandes entreprises.

Le troisième volet concerne l'organisation. Le numérique bouleverse complètement le mode de gouvernance des entreprises. Il existe des outils professionnels utilisés hors du bureau pour travailler en se connectant à l'ordinateur central. Dans la pratique, rien ne dit qu'à travers ces outils, c'est réellement votre collaborateur qui est en ligne et échange avec votre serveur.

Enfin, les dirigeants découvrent que le système pyramidal traditionnel en place dans les entreprises des pays européens va être remplacé par un système en râteau. Auparavant, un individu ne pouvait pas gérer efficacement plus de cinq à sept personnes simultanément et en direct. L'apport du numérique change la donne en permettant d'encadrer directement beaucoup plus de personnes mais avec pour conséquence l'obligation de déléguer plus et de devoir prendre des décisions plus rapidement.

Avec le numérique, celui qui détient des quantités d'informations prétraitées ou traitées par des logiciels spécialisés peut élargir considérablement le nombre de gens qu'il traite en même temps. D'où l'idée de **supprimer les échelons hiérarchiques pour travailler en réseau ou en râteau**. Cela constitue un changement fondamental dans la gouvernance et l'organisation des structures que les écoles de commerce vont devoir enseigner à leurs étudiants. En haut, nous aurons des généralistes capables d'opérer la synthèse et, en dessous, des experts très pointus mais qui n'auront pas la connaissance de l'ensemble du système.

Dans cet environnement-là, il est vital que le numérique soit sécurisé. Dans un système en râteau dans lequel une vingtaine de personnes, ou de fonctions, sont gérées simultanément, la moindre défaillance bloque l'ensemble de la structure.

Dans le système hiérarchique, il y avait des filtres. Les arbitrages étaient rendus par les échelons supérieurs. À l'inverse, dans le système en râteau, l'information arrive de partout. Il sera demandé aux dirigeants une capacité de synthèse très large et également d'évaluation pour prendre des décisions en fonction des parts de risque acceptables. Il y a toujours une partie subjective dans le risque sur laquelle l'expert, qui travaille sur la partie objective, ne pourra pas prendre de décision. C'est pourquoi cette tâche incombera aux dirigeants. En conséquence, **il est particulièrement important de recevoir une information non polluée et sûre.**

Le besoin d'État se fait sentir pour que l'entreprise ait une politique globale. Alors que les Américains et les Chinois mènent une politique globale dans le numérique, nous prenons du retard. Même si un accord avec la ministre, en charge du numérique, Mme Fleur Pellerin, est intervenu récemment, dans notre pays, **rien n'est fait pour développer une politique du numérique, à moyen et long terme.** Un exemple : en 2002, la Commission européenne s'est réunie à Lisbonne. Ils savaient que les États-Unis d'Amérique investissaient 3 % du budget fédéral depuis 1985 et avaient lu les déclarations de 1996 du président du *National Intelligence Economic Council,* qui affirmait que pendant les quinze premières années du XXIe siècle, la compétition mondiale serait gagnée par **les meilleurs sur le plan du développement du numérique.** Les chefs d'État européens ont donc décidé que 2 % du budget général seraient consacrés aux technologies de l'information.

Cette attitude **vertueuse n'a pas vraiment été suivie d'effet puisque, loin des chiffres annoncés, la dépense européenne n'a jamais** dépassé 0,7 %.

Depuis 2002, il s'est donc créé un écart important entre ceux qui ont agi et ceux qui n'ont rien fait. Certains ont surinvesti tandis que d'autres sous-investissaient.

La France pourra-t-elle rattraper l'important retard accumulé ? Même si la France est bonne, voire très bonne dans le domaine du numérique, tout dépend du suivi d'une politique cohérente. Compte tenu des moyens à mettre en œuvre, on peut se demander s'il ne serait pas possible de travailler sur ces questions avec l'Allemagne.

Le dernier point que je souhaiterais évoquer c'est qu'**aujourd'hui, les outils numériques que nous utilisons sont des outils nord-américains à 99,9** %. Dans le futur, tout indique que les Chinois, notamment avec *Huawei,* vont également produire de tels outils. Cela contrebalancera-t-il les Américains ? Dans un cas comme dans l'autre, ce qui se vend est « plombé », par les uns ou les autres. Il a été révélé que ***Google, Yahoo, Facebook,*** **faisaient des copies de tout à la demande des services américains mais il n'y a pas que cela. La quasi-totalité des logiciels sont construits avec une porte d'entrée dérobée pour le fabricant ou l'administration de son pays.**

Dans le futur, avec l'arrivée de l'Internet 3.0, **tous les objets seront équipés de puces qui permettront de les repérer grâce à des signaux émis en permanence ou activés dans certaines conditions.** On le voit avec les avions et le matériel militaire mais c'est valable pour toutes les activités et produits. Déjà chez les grands fournisseurs d'automobiles, les modèles haut de gamme envoient en continu à peu près cinquante données vers le fabricant, allant de l'usure des freins à des valeurs de motorisation.

Le *GPS* est entré dans notre vie grâce à ses possibilités de géolocalisation. Si le fabricant, comme cela s'est fait sur zone pendant la première guerre d'Irak, fait passer la précision de 10 m à 100 m, il se créera, dans Paris, le plus gros embouteillage jamais vu. Heureusement, la concurrence entre les trois systèmes existants – l'américain, le chinois et le russe – réduit ce risque mais ne l'élimine pas.

Les objets connectés causeront des problèmes énormes car les quantités d'informations fournies par eux seront stockées et utilisées. Par qui et pour quoi faire ?

Actuellement, les quatre acteurs majeurs sont les États, les entreprises, les particuliers et les entreprises criminelles – même si on n'en parle jamais. Chaque catégorie défend ses propres intérêts et s'adapte à l'évolution. Aujourd'hui, il faut être stupide pour **attaquer un distributeur de monnaie, braquer une banque et courir le risque d'une quinzaine d'années de prison, alors que voler un ordinateur dans un laboratoire de recherche ou une société puis vendre des informations au concurrent permet de toucher beaucoup d'argent et, en cas de sanction, de ne risquer que quelques jours de prison avec sursis.**

Les organisations criminelles ont compris le parti qu'elles pouvaient tirer de cette situation. La drogue leur rapporte beaucoup d'argent acquis à haut risque mais, avec le numérique et la vente de médicaments trafiqués sur

Internet, le risque est nul. Il y a une sorte d'omerta sur ces affaires-là qui constituent pourtant la réalité de tous les jours.

Actuellement, pour se protéger efficacement, la meilleure solution est le cryptage. C'est d'autant plus intéressant que **la France possède de très bonnes compétences dans ce domaine grâce à notre école de mathématiques.** Nous sommes parmi les meilleurs au monde à en juger par la collection de médailles *Fields* obtenue par notre pays alors qu'il s'agit de la plus haute distinction mondiale dans cette spécialité. Nous devrions en faire une priorité nationale car, au lieu de s'éparpiller, la France doit choisir des domaines dans lesquels elle est vraiment bonne pour y devenir encore meilleure.

On peut rajouter au cryptage **le segment des tunnels numériques, ces liaisons informatiques entre deux destinataires impossibles à intercepter** car transitant dans une sorte de tunnel numérique inviolable. Là aussi, nous sommes en pointe et avons donc la capacité de nous défendre face aux interceptions américaines, chinoises ou autres.

OPEN-ROOT

M. Louis Pouzin, président

19 mars 2014

La question de l'identité numérique est un vrai sujet. Actuellement, se déroule à Genève un jeu de dupes entre l'*ICANN* et ses interlocuteurs pour fixer de nouvelles règles d'attribution des noms de domaines.

Il est à noter que les numéros de l'Internet sont considérés comme peu pratiques car un même numéro d'ordinateur peut être utilisé pour des milliers de services. L'usager ne connaît pas ce numéro.

Ce système a été inventé dans les années 1980 et mis en service en 1983. **C'est à partir de la création des noms de domaine que le *web* est devenu populaire.**

Au départ, des numéros flanqués de l'extension *Top Level Domain (TLD),* ou domaine de premier niveau, ont été attribués, les pays étant identifiés selon la structure « .fr » ; les autres noms sont attribués à des sociétés ou à des classes de service. La société qui gère le *TLD* tient un registre.

Les utilisateurs ne se servent que des deux premiers niveaux tandis que les autres niveaux sont gérés par des registreurs, comme *VeriSign*, sorte de grossiste, qui attribue les « .net » et les « .org ». Il s'agit-là de marchés captifs, d'exclusivités.

Puis les Américains ont pensé à faire de l'argent avec l'*ICANN*, les noms de domaine étant inscrits dans un registre et l'*ICANN* fixant les tarifs.

Pour utiliser les noms de domaine, un serveur de noms est interrogé qui renvoie à un numéro et ce service est mis en place gracieusement par *Google* qui récupère des infos en rendant ledit service.

L'*ICANN* ne paie pas d'impôts et se trouve en situation de conflit d'intérêts car elle se trouve aux deux bouts du processus : le monopole de l'*ICANN* s'exerce sur les registres à l'occasion de la délivrance d'un nom unique au sein d'un régime clientéliste d'où elle tire un revenu.

À noter que **l'Union européenne est de connivence avec les Américains dans cette organisation**, *VeriSign* ayant obtenu un contrat d'exclusivité pour gérer des noms de domaine de l'Union européenne.

Maintenant, l'*ICANN* propose de gérer l'Internet des objets.

Les codes **qui leur seront attribués –** il s'agit là de codes autres que les **codes-barres** mêmes si les codes-barres en font parti**e – sont discutés pendant des années**. Le code attribué comprend environ quatre-vingt-dix caractères incluant notamment le prix, les conditions de vente etc.).

D'abord proposés gratuitement, les codes deviendront payants et le piège se refermera.

Gencod, devenu *GS1* et situé à Issy-les-Moulineaux, emploie environ cinquante personnes ; c'est une fédération indépendante de tout État. Aucune exclusivité ne lui est attribuée mais elle exerce une dominance.

Les Américains et les Japonais obligeront les Européens à se soumettre à ce système.

En réalité, c'est l'*ISO* qui devrait héberger la normalisation mais c'est *GS1* qui le fait.

Dans ce domaine, il est important d'éviter les monopoles, surtout américains.

L'essentiel est de changer de système, sauf que, aujourd'hui, il y a à peu près 130 millions de codes de deuxième niveau qui sont gérés par les Américains ; **tous les codes génériques sont gérés par des Américains ou des filiales** ; les codes pays, c'est à peu près autant, c'est-à-dire qu'il y a au total 300 millions de codes légaux ; alors que seulement un quart de l'humanité est connecté. Dans cinq ou six ans, il n'y aura pas 130 millions de codes mais peut-être trois milliards et ils ne seront pas nécessairement en *ASCII*, ils seront dans une sorte de langue arabe, indienne, etc. Cela signifie que **le système actuel est complètement inapproprié à cette croissance.**

Déjà, à l'heure actuelle, le simple fait d'utiliser des accents, du cyrillique, de l'arabe, se fait au prix d'acrobaties techniques. Tous les noms qui ne sont pas en caractères latins, sans accents, sont traduits par une succession de caractères et ne veulent plus rien dire du tout. En plus, cela crée un nombre considérable de confusions possibles notamment avec le cyrillique. Le cyrillique a beaucoup de caractères qui n'ont pas le même code. On peut faire croire aux gens qu'ils sont connectés à une certaine société qui existe à Paris alors qu'ils le sont en réalité à une autre en cyrillique. Il existe trente-six moyens de créer la confusion dans l'esprit du lecteur car le système fondé sur le codage pourrait l'être aussi sur l'œil, sur ce que voient les gens.

Le poison, le cancer du système, c'est le monopole parce que cela permet d'imposer des contraintes qui sont inutiles et coûteuses. Le fait que l'*ICANN* ne permet pas d'avoir des homonymes n'est pas du tout adapté aux besoins des utilisateurs.

Aucune flexibilité régionale ou de type de métiers n'existe. Ils enregistrent des noms qui sont protégés légalement. Cela ne veut pas dire

qu'il n'y a pas des pirates qui s'en servent mais ça laisse la possibilité à des utilisateurs, à la société dont on a volé le nom, d'attaquer en justice le voleur. C'est assez fallacieux parce que **si un Chinois vous copie, l'*ICANN* ne fera strictement rien pour régler la question. Il n'y a aucune protection juridique sérieuse dans le cadre de l'*ICANN*.**

La *World Intellectual Property Organization* (*WIPO)*, en français l'Office international de la propriété intellectuelle, offre une protection avec une gamme de prix qui dépend du métier. Par exemple *Montblanc* ce peut être les stylos, des accessoires de bureau, des yaourts, ça peut vouloir dire plein de choses.

Il y a une quarantaine de classes de produits. Il peut y avoir aussi des homonymes à protéger selon la classe de produits à laquelle ils appartiennent.

Deuxième type de souplesse, un nom peut être réservé à une partie du monde. Il peut ne pas être utilisable dans certains pays mais seulement dans d'autres. Il y a donc des zones géographiques protégées. On peut avoir le même nom pour le même produit dans différents pays. Je ne sais pas si, par exemple, *Avis* est protégé ; je sais que, au Brésil, il y a un *Avis* qui n'est pas du tout celui qu'on connaît en France. Je ne sais même pas s'il est protégé. Le *WIPO* a une capacité beaucoup plus fine pour satisfaire les clients, plus adaptée aux besoins car il permet à la fois de protéger des similitudes et des variétés par zone géographique.

La protection par le *WIPO* peut coûter éventuellement quelques centaines d'euros par an, bien moins que dans <u>le système de l'*ICANN*</u> pour la protection du *PLD* (*Penthouse-Level Domains)*. Par exemple, pour avoir leur nom, *Sony*, *L'Oréal, Toshiba, Canon,* etc., ont dû commencer par payer 175 000 $ mais seulement pour obtenir les cinq cents pages qui constituent la demande. Il faut pour cela disposer d'une armée d'avocats et de juristes qui vont alors défendre le dossier. Entre le moment du dépôt et le moment où c'est finalement accepté, après des discussions avec les avocats, cela peut coûter environ 300 000 $ en plus. Sans compter 50 000 $ par an ensuite.

La plupart du temps, les directions des entreprises ne s'occupent pas de cela ; c'est géré par des gens qui sont plutôt du niveau de la communication alors qu'il s'agit d'informatique. Quand c'est *Rolex* ou *L'Oréal*, c'est différent. La plupart du temps, personne ne s'en occupe vraiment. Cela passe plutôt par les webmestres dont la culture est peut-être bonne sur le plan technique mais qui ne les conduit pas à prendre des risques dans la société. Ils n'ont donc pas le niveau nécessaire pour prendre une décision de ce type.

Il s'est passé cinq années avant que les noms de domaine soient vendus de manière cohérente par l'*ICANN* alors qu'ils pensaient le faire dès l'année 2008. Ils ne connaissaient pas le métier des noms de domaine dans lequel ils débarquaient. Comment gérer la marque dans leur système

technique ? Ils pensaient que c'était simple. En réalité, ils sont attaqués par plein de sociétés. Ils ont même commis l'erreur de mettre sur le marché des noms dont ils avaient déjà eu la gestion autrefois, ce qui leur a valu d'être attaqués par beaucoup de sociétés.

Éventuellement, ils peuvent arriver à convaincre. Aujourd'hui, **la plupart des gens ne comprennent pas à quoi servent les noms de domaine** ; ils ne comprennent pas pourquoi les noms de domaine sont précédés de trois w – ce qui ne sert d'ailleurs à rien. Ces w sont juste un symbole qui montre que l'on est sur le *Net* alors qu'on peut très bien y être sans cela. Cela ne sert à rien techniquement. Quant à http, c'est pareil, c'est juste un protocole. Le nom de domaine, c'est ce qui suit.

La plupart des gens n'ont jamais essayé de comprendre pourquoi il y a plusieurs noms qui se suivent, pourquoi il y a des points, etc.

L'annuaire mondial, c'est l'*ICANN*.

En téléphonie, les numéros que vous utilisez ne sont pas des numéros physiques de téléphonie, ce sont des noms tout simplement. Le numéro sert simplement à aller voir, dans la base de données de l'annuaire de la société de téléphonie dont vous êtes l'abonné, qui vous êtes. C'est tout à fait l'équivalent des noms sauf qu'il s'agit là de numéros. Il y a au moins 1 500 sociétés agréées qui ont chacune leur annuaire ; il n'y a aucune centralisation. En définitive, ce sont les premiers chiffres du numéro virtuel qui servent à trouver l'opérateur.

Open-root dispose d'un réseau de vingt-cinq serveurs dont un en Allemagne qui gère les noms avec un administrateur allemand. Vous y trouvez des noms et des adresses avec le numéro *IP*. L'obtention d'un nom de domaine par une société *non profit* en structure d'association peut lui coûter 200 € ; il n'y a pas besoin de gérer les arriérés de paiement, l'association paie une fois pour toutes. Pour une société commerciale, le prix est de 20 000 € et non pas 50 000 € par an.

L'*ICANN* fait semblant de ne pas savoir qu'*Open-root* existe. On est attaqué tous les jours par des virus ciblés de type *Denial of Service Attacks (DoS ou DDoS*) dont le principe est d'envoyer, sur les serveurs de noms d'une société à qui l'on veut du mal, des billets de messages à la seconde de manière à ce que le processeur de la machine n'arrive pas à traiter tout et s'effondre. On est attaqué tous les jours par des choses comme cela, ce qui signifie que l'on est ciblé. Depuis quinze jours, on a découvert que les messages ne provenaient pas directement mais passaient par des zombies, c'est-à-dire des ordinateurs infectés. Ce genre d'attaque est difficile à contrer, surtout si l'on n'a pas une très bonne connaissance du fonctionnement du système. Depuis quinze jours, on sait que les attaques venaient de la *NSA* et du *Government Communications Headquarters (GCHQ)*. Comme ces attaques ont été contrées par notre administrateur, c'est maintenant *Google* qui attaque. Habituellement, les attaques sont menées par des sociétés russes ou

sud-américaines pilotées par des Américains ; c'est d'ailleurs une erreur de se livrer à une attaque directe ; peut-être avaient-ils peur de sous-traiter à des *gangsters* comme cela se fait aussi ?

Ils craignent que se répande l'idée qu'on n'a pas besoin d'eux et que, à côté de l'*ICANN*, on peut très bien faire la même chose. Il y a une quarantaine de petites sociétés indépendantes qui gèrent des abonnés. C'est probablement une erreur de la *NSA* d'avoir procédé de la sorte, aidée ou non par *Google*. **Tous les systèmes de réseaux aux États-Unis d'Amérique dépendent de la *NSA*.** Le système actuel est concentrationnaire pour ne pas dire totalitaire.

Quel que soit le protocole, ils peuvent toujours l'implémenter. Ce ne peut être une manière de se défendre. Il faut commencer par ce que l'on sait faire, ce qui peut l'être sans leur accord.

Il faut commencer par mettre du chiffrement.

Aujourd'hui, tout ce qui passe par messagerie est en clair. Si vous voulez monter une opération commerciale ou politique, vendre des avions, par exemple, à des pays du tiers monde, ils connaîtront votre proposition avant même que vous ne l'ayez remise ; ce qui se passe ainsi dans le commerce, se passe également dans la diplomatie. **Dans un système fermé, on peut concevoir de la sécurité avec du chiffrement mais non dans un système ouvert.**

Nous avons ce qu'il faut pour le faire mais jusqu'à présent la manière de s'en servir n'était pas pratique. Aujourd'hui, **ce qu'il faudrait, au lieu du bouton « *Send* », c'est un bouton « *Send* normal » et un autre « *Send* chiffré ».**

Il existe des normes de chiffrement. Actuellement, **dans les techniques de chiffrement, il y a deux clés, celle secrète, de l'expéditeur et celle publique, du récepteur** – et inversement au retour. Personne ne peut décoder le message autrement qu'en ayant votre clé publique destinée précisément à diffuser l'information mais en sachant qu'elle provient de vous. De la même manière, quand ils vous répondent, ils vont vous envoyer un message sur votre clé publique à partir de leur clé secrète, si vous le décodez, cela veut dire que cela vient bien de chez eux.

Il existe des tiers de confiance sur le marché qui vont pouvoir dire exactement à qui appartient cette clé. Pour vous envoyer un message, je vais créer une clé secrète et vais vous envoyer ma clé publique.

Il y a une bonne dizaine d'années, un Américain avait inventé un système appelé *Pretty Good Privacy* (*PGP*) qui est relativement facile d'usage. Certaines personnes s'en servent, c'est encore un peu confidentiel car il faut l'installer dans sa machine. Ce système peut fonctionner sous deux conditions : premièrement, il faut un système qui soit très simple pour les usagers, ce qui reste à inventer et, deuxièmement, il faut éduquer les usagers. Cela pourrait devenir obligatoire ; pour les administrations ou pour

les sociétés qui travaillent pour l'État, pour des sociétés qui ont des contraintes de sécurité commerciale. Il faut à un moment qu'il y ait un entraînement et que cela passe dans les mœurs.

On ne peut rien faire sans être sous surveillance. Vous ne pouvez pas avoir de relations avec d'autres personnes sans que la *NSA* soit au courant. Il faut **donc mettre en place des systèmes indépendants**. Mais, pour l'instant, les gens ne comprennent rien aux noms de domaine, ne savent pas à quoi servent les points ; il n'y a que les professionnels qui savent exactement de quoi il retourne.

Pour que ce soit acceptable, il faut qu'il y ait des sociétés du type d'*Open-root* qui se créent dans tous les pays. Ce n'est pas très difficile à faire. **Le plus difficile est de faire en sorte que cela fonctionne tous les jours, d'où une maintenance importante de jour comme de nuit.** Aujourd'hui, vendre des noms de domaine très cher, c'est de l'arnaque.

Ce qui coûte, c'est de faire fonctionner le système or, précisément, ils ne le paient pas parce que cela est assuré ; par des volontaires.

Les identités ne sont pas forcément des noms de domaine mais cela obéit aux mêmes processus de structuration. Quand c'est personnel, évidemment, cela est plus sensible et c'est plus contrariant si on vous le vole plutôt que si on vous vole un nom de produit.

CONFÉRENCE DES DIRECTEURS DES ÉCOLES FRANÇAISES D'INGÉNIEURS (CDEFI)

M. Christian Lerminiaux, président

M. Jean-Marie Chesneaux, vice-président

M. Reza El Galai, ingénieur projet cybersécurité

19 mars 2014

M. Reza El Galai. – La conférence des directeurs des écoles françaises d'ingénieurs ne fédère que les écoles.

Les écoles françaises d'ingénieurs délivrent deux types de diplômes qui vont former à la sécurité informatique des entreprises : il s'agit de *masters* et de *mastères* spécialisés (MS) suivis après un *master* et qui ne sont pas agréés par l'État puisqu'ils sont accrédités par la conférence des grandes écoles ; il s'agit donc d'une sixième année.

Les thématiques enseignées sont la sécurité des contenus, des réseaux, des télécoms, des systèmes.

La plupart des *masters* traitent des réseaux, des télécoms et des systèmes. Il existe aussi des *masters* de **gestion des risques**, des *masters* propres à la sécurité, des *masters* d'audit qui permettent de trouver des failles de sécurité ; certains *masters* naissent dans des matières assez novatrices comme l'informatique légale, par exemple, les enquêtes numériques. Dans le sud, à Grenoble et à Nice, il y a beaucoup de **formations en cryptologie**.

En revanche, **au niveau ingénieur, il y a très peu d'écoles qui forment en cybersécurité**. Il faut vraiment arriver au niveau de *mastères* spécialisés pour être sensibilisé à la problématique de la cybersécurité La carte des formations en sécurité informatique, dressée par l'ANSSI, montre la répartition géographique de la formation en cybersécurité.

M. Christian Lerminiaux. – Aujourd'hui, il n'existe pas de formation d'ingénieur en cybersécurité. Les *masters* ou *mastères* spécialisés sont des diplômes de niche. L'ingénieur doit avoir un regard plus large. **Il faudrait que tous les ingénieurs aient un minimum de compétences en sécurité informatique quelle que soit leur formation de base.** Cela reste à développer.

M. Jean-Marie Chesneaux. – Deux types de formation coexistent : une formation spécialisée en sécurité et une formation de masse plus généraliste. **Il faut non seulement sensibiliser au risque numérique mais aussi donner une compétence en sécurité en vue d'un comportement responsable, ce qui reste souhaitable pour tous les ingénieurs pour le plus grand bien des entreprises. En réalité, ce sont souvent les erreurs commises dans les entreprises qui permettent aux attaquants de rentrer.**

Tous les aspects sécurité informatique et risque devraient être enseignés aux ingénieurs. Se développe, d'ailleurs, le certificat appelé C2i2mi (Métiers de l'ingénieur), qui est le niveau supérieur du C2i, et que chaque ingénieur devrait avoir. Ça ne ferait pas de chaque ingénieur un expert de la sécurité mais ça formerait des gens responsables face au risque numérique.

Dans un cas, il s'agit d'un enseignement qui forme un petit nombre d'experts extrêmement compétents ; dans l'autre cas, il s'agit d'un enseignement de masse pour sensibiliser à la prévention. **Tout ingénieur, qu'il soit chimiste ou autre, devrait avoir une attitude responsable face à la sécurité informatique.**

M. Christian Lerminiaux. – Ce qu'il faut voir, c'est ce qu'il y a derrière le diplôme aujourd'hui, à une époque qui forme des cadres. **Un quart des diplômés de niveau bac+5 sont des ingénieurs, soit une proportion passée de 15 % à 25 % en dix ans** ; le nombre d'ingénieurs formés est passé de 18 000 à 34 000 par an ; le diplôme d'ingénieur est donc prépondérant à ce niveau.

Derrière la formation d'ingénieur, se trouve un processus de référentiel des compétences en constante évolution. Tous les deux ans, ce référentiel de compétences est revu en fonction des besoins des entreprises ; c'est un processus clé.

L'obtention du C2i2mi au niveau du *master* sera nécessaire pour tous les ingénieurs de niveau bac+5.

M. Reza El Galai. – Le 20 février 2014, le Premier ministre a encouragé l'ANSSI à s'intéresser aux formations à la cybersécurité. L'association des écoles et des universités est indispensable pour promouvoir ces nouvelles formations.

Dans l'immédiat, les bonnes pratiques recommandées par l'ANSSI et la CNIL sur leurs sites permettent d'asseoir la sensibilisation sur les recommandations de guides.

Compte tenu de la rapidité de l'évolution des technologies, l'anticipation des évolutions techniques du numérique ne pourra se faire que par une veille technologique de qualité, éventuellement mutualisée à travers un observatoire des nouvelles technologies.

Par exemple, les objets connectés sont aujourd'hui utilisés comme des *gadgets* sans que l'on pense à leur aspect sécurité. Or, un *hacker* a montré qu'il pouvait s'en prendre à un *pacemaker* en lui infligeant une décharge électrique de 800 volts. La technologie va très vite mais on n'analyse pas les conséquences de cela sur la cybersécurité.

Un observatoire, français ou européen, permettrait de creuser ces questions.

M. Christian Lerminiaux. – L'usage des objets connectés doit être systématiquement associé aux aspects de sécurité. Il serait souhaitable de **mettre en place des normes de sécurité que tout objet connecté devrait respecter**.

M. Jean-Marie Chesneaux. – Aujourd'hui, la veille numérique est particulièrement importante car c'est l'usage qui est mis en avant pour que tout le monde ait accès à tout, partout. Certes, **il ne faut pas bloquer, au nom de la sécurité, le développement de l'usage mais si, du fait d'une sécurité insuffisante, quelqu'un prend la main sur le système, il peut tout contrôler**.

Par exemple, dans le cas d'un hôpital, si le fait d'entrer dans son système informatique avec des visées malveillantes permet de tout y faire, le décalage entre les outils existants et la sécurité qui les accompagne inquiète.

Même **les cartes bleues professionnelles ne sont pas convenablement protégées**. À l'heure actuelle, les banques préfèrent payer pour les erreurs constatées plutôt que de voir leurs clients renoncer à utiliser leurs cartes.

M. Reza El Galai. – La Commission européenne a souhaité financer le développement dans chaque pays d'un centre de formation à la lutte contre la cybersécurité. Depuis janvier 2014, un tel centre de formation existe maintenant en France, le CECyF regroupant notamment la Gendarmerie nationale, *Thales, Orange, Microsoft,* l'Université de Montpellier 1…

Le siège de cette association se trouve au Centre de recherche de l'École d'officiers de la Gendarmerie nationale (CREOGN) qui est dirigée par le général d'armée Marc Watin-Augouard mais il n'y a pas encore de bâtiments proprement affectés au CECyF.

Dans le cadre du projet 2Centre, les besoins en formation liés aux nouveaux métiers de la sécurité ont été recensés comme, par exemple, celui de disposer de personnes qui vont intervenir sur les incidents, d'analystes également en charge de la veille, de testeurs d'intrusion – pour **trouver les failles avant les attaquants** – et, également, d'ingénieurs en charge de la réponse aux incidents, pour les *CERT* – comme il y en a dans les grandes entreprises, comme, par exemple, les banques (la *Société Générale,* la *Banque de France*, ou autres).

L'ANSSI envisage de recruter environ deux cents spécialistes de la sécurité tandis que les effectifs du Centre d'analyse de lutte informatique défensive (CALID) de la DGA, devraient passer de quarante à quatre-vingts personnes très prochainement.

En effet, pourquoi attendre d'être attaqué ? Le centre de la DGA sert justement à repérer les failles avant d'être attaqué et à riposter.

Ces métiers concernent les milieux gouvernementaux, les opérateurs d'importance vitale (OIV) et les entreprises en général, qui en ont également grand besoin, même si l'ampleur des recrutements nécessaires est difficile à quantifier.

M. Jean-Marie Chesneaux. – La France a été un des derniers pays au monde à avoir introduit l'informatique dans l'enseignement secondaire alors qu'**il faudrait que, du collège à la terminale, une formation en informatique puisse être dispensée**.

J'ai fait partie, l'an dernier, de la commission qui réformait le contenu des programmes des classes préparatoires dans lesquels **l'informatique ne figurait pas**. Si vous aviez un vrai corps d'enseignants en informatique, la prise de conscience de l'importance de la sécurité informatique par l'ensemble de la population en serait améliorée.

La durée consacrée à d'autres matières par les programmes actuels devrait être réduite en conséquence.

Longtemps, l'informatique a été considérée comme une discipline applicative des mathématiques.

M. Christian Lerminiaux. – Le problème de l'INRIA, c'est que l'informatique n'est toujours pas rentrée dans les classes préparatoires.

M. Jean-Marie Chesneaux. – **Le corps enseignant n'est pas suffisamment informé des possibilités et des risques du numérique.**

Dans les établissements d'enseignement supérieur, le mélange entre l'usage privé et l'usage professionnel du numérique est une source de faiblesse du système.

Il y a quelques endroits où des laboratoires sont extrêmement protégés parce que c'est leur métier. En revanche, **des laboratoires extrêmement sensibles ne sont pas assez protégés.**

Nous reprenons à notre compte le rapport de l'Académie des sciences qui prône **un *continuum* de l'enseignement du numérique**. Il faut un vrai corps d'enseignants en informatique.

La réforme des classes préparatoires n'a débouché que sur deux heures d'informatique par semaine à compter de septembre 2013… Il faudrait également favoriser un enseignement en informatique de masse en classe de terminale. Avec des enseignements où l'on forme des formateurs.

M. Reza El Galai. – De leur côté, depuis 2011, les gendarmes, « enquêteurs en technologie numérique » ont un bon niveau de formation informatique et se voient délivrer une licence professionnelle.

Avec Europol, c'est-à-dire l'ensemble des polices européennes, il y a eu beaucoup de réunions, de rencontres sur le terrain où ont été évoqués les problèmes de sécurité informatique et de formation. Chaque année, **la Commission européenne met en place trois cours qui vont être dispensés à l'ensemble des forces de l'ordre européennes, sur des thématiques liées à la cybercriminalité (groupe de travail *ECTEG*, *European Cybercrime Training and Education Group*)**.

M. Jean-Marie Chesneaux. – À noter aussi le retard face aux Américains : jusqu'au début des années 1980, l'informatique était quasiment absente des Écoles normales supérieures. En France, la formation est beaucoup plus conceptuelle que celle dont bénéficient les Américains.

M. Reza El Galai. – Beaucoup d'aspects légaux sont également à prendre en compte : par exemple, aux États-Unis d'Amérique, un *hacker* peut être embauché pour s'occuper de sécurité informatique après avoir déjoué une sécurité de son nouvel employeur.

M. Jean-Marie Chesneaux. – **Dans les écoles d'ingénieurs et dans certains départements d'université, les gens ont réussi à bien se protéger avec des architectures efficaces et des passerelles sécurisées – sous scanner en permanence – qui empêchent l'attaquant de mener une attaque en profondeur.**

Cela nécessite que les personnels prennent en compte le fait que, comme l'informatique est organisée en réseau et que tout circule dans l'enseignement supérieur, de vraies mises à jour des systèmes de sécurité sont indispensables.

Pour les établissements d'enseignement, le besoin de sécurité numéro un provient de leur site *web* car, pour y accéder, il suffit de rentrer le nom de l'*URL* puis un code.

Le summum de la protection, c'est tout simplement de ne pas être connecté à l'extérieur. C'est la solution que le CEA-Direction des applications militaires (DAM) adopte pour ses salles les plus stratégiques.

M. Christian Lerminiaux. – C'est la même chose pour une entreprise. **Il faut que tous les organes clés de l'entreprise soient totalement séparés du site *web* avec seulement une passerelle entre les deux.**

M. Jean-Marie Chesneaux. – Certes, une cage de Faraday peut protéger de l'espionnage électronique car on arrive à lire à vingt mètres un écran grâce à des ondes électromagnétiques. Mais, si vous êtes connectés, la cage de Faraday peut être pénétrée.

Il faut tout de même se rappeler qu'on a réduit d'un facteur mille les capacités d'intrusion.

M. Reza El Galai. – La première précaution à prendre consiste à installer des pare-feu : si possible plusieurs et de marques différentes.

ASIP SANTÉ

M. Michel Gagneux, président de l'Agence des systèmes d'information partagés de santé (ASIP Santé)

M. Jean-François Parguet, directeur du pôle technique et sécurité (ASIP Santé)

26 mars 2014

M. Michel Gagneux. – L'Agence des systèmes d'information partagés de santé (ASIP Santé) est une jeune agence créée en 2009 par le Gouvernement sur ma proposition. Elle a pour mission de créer les conditions de développement futur des systèmes d'information de santé sécurisés pour permettre le partage des données de santé qui sont personnelles et particulièrement sensibles.

L'ASIP Santé doit créer les conditions applicables par tous les acteurs de santé, hôpitaux, professionnels de santé, de nature à garantir le **respect de la confidentialité des données individuelles de santé.**

Selon l'orientation stratégique du ministère de la santé, **l'agence est le prescripteur de tous les référentiels qui doivent être respectés par les opérateurs et les acteurs en matière d'interopérabilité et de sécurité des systèmes d'information de santé**, de façon à ce que les données soient partagées, échangées et stockées dans des conditions de sécurité optimale.

La seconde mission de l'ASIP Santé consiste à promouvoir **des services comme le dossier médical personnel (DMP) ou une messagerie sécurisée de santé** (MSS) pour lesquels l'agence est responsable du traitement des données aux termes de la loi relative à l'informatique, aux fichiers et aux libertés.

L'agence propose des dispositifs de gestion de la sécurité interne pour l'ensemble de ses infrastructures, services et produits et vérifie l'impact de tout correctif sur l'ensemble des services.

La vocation première de l'ASIP Santé est de créer un espace de confiance qui soit respecté par tous.

Depuis quatre ans, l'agence est l'un des principaux acteurs de la définition d'une politique générale de sécurité des systèmes d'information de santé qui est appliquée par les éditeurs et industriels, les établissements de santé et les médecins.

Plutôt que de s'attacher au respect de la notion de souveraineté numérique alors qu'il n'y a pas de frontière dans le numérique, l'ASIP Santé concentre ses efforts sur les règles et les procédures à imposer en matière de sécurité.

La procédure d'agrément des hébergeurs de données de santé, définie par le décret de 2006, a mis du temps à se mettre en place. C'est en 2009 que l'ASIP Santé a relancé l'application de ce décret, resté lettre morte, qui permet aux industriels de se mettre aux normes et se conformer à une doctrine.

Il existe un comité d'agrément des hébergeurs de données de santé qui étudie tous les dossiers de candidats à l'hébergement de données de santé. Ainsi, les dossiers sont soumis à une double instruction celle de la CNIL et celle du comité d'agrément de l'ASIP Santé.

Une soixantaine d'agréments ont été délivrés depuis le lancement de cette procédure et il y a eu plus de 40 % de refus d'agrément en 2013.

Cette procédure garantit que tout hébergeur de données de santé en France respecte les règles conformes à la fois à la directive européenne et aux prescriptions de la CNIL.

Les données personnelles peuvent être hébergées à l'étranger uniquement si elles restent sur le territoire de l'Union européenne dans des conditions conformes à une directive européenne transcrite dans le droit français en 2006, modifiant la loi de 1978 relative à l'informatique, aux fichiers et aux libertés.

En outre, la Commission européenne a donné son accord pour que les données personnelles puissent être hébergées dans certains pays, comme le Canada, qui offrent des garanties équivalentes à celles décrites dans sa directive (réglementation « *Safe Harbor* »). Certains autres pays ont passé un accord avec la Commission européenne, comme ce fut le cas en 2001 pour les États-Unis d'Amérique.

Un hébergement des données de santé en dehors des frontières de l'Union européenne, notamment par de grands industriels, est possible s'ils respectent des cahiers des charges contractuels ainsi que des règles internes qui garantissent les bonnes pratiques et l'application des procédures de sécurité prescrites par la commission européenne et la CNIL.

Le stockage des données dans les nuages se fonde sur des technologies de virtualisation qui reposent à la fois sur des infrastructures, sur des plates-formes et sur des applications. Il existe une grande diversité de technologies de virtualisation.

Le stockage dans un nuage peut permettre d'apporter une sécurité à des données atomisées qui nécessitent peu de sécurité et qui ont besoin d'être mutualisées. Mais **plus les données ont besoin de sécurité, ce qui est**

le cas des données de santé, plus le stockage dans un nuage constitue une limite au maintien de l'optimisation des normes de sécurité.

C'est la raison pour laquelle, **l'ASIP Santé n'a pas recours aux nuages pour le stockage des données.** Seules certaines infrastructures techniques sont dans un nuage localisé en France.

Les données personnelles du DMP sont stockées, en France, chez deux hébergeurs sur deux sites distincts ; à Lille et à Marseille pour le dossier médical personnel (DMP) et à Paris et au Mans pour la messagerie sécurisée de santé.

M. Jean-François Parguet. – **Seules les données de certaines des infrastructures techniques de l'ASIP Santé sont stockées dans un nuage en France.** Il s'agit des données du site institutionnel qui présente l'ASIP Santé, des sites de formation ou encore des sites de données techniques partagées avec les industriels et les différents opérateurs de santé. Cela permet de diminuer les coûts et d'obtenir une grande disponibilité des informations de ces sites.

De même, mettre à disposition des 120 000 médecins libéraux un logiciel de gestion stocké dans un nuage peut permettre d'accroître la sécurité dans la mesure où ce logiciel est géré par des spécialistes et mis à jour régulièrement. En sens inverse, le nuage peut amoindrir la sécurité d'un dispositif totalement maîtrisé.

M. Michel Gagneux. – Pour l'identification des patients, l'échange et le partage de données de santé les concernant, la CNIL a recommandé l'utilisation d'un identifiant national de santé spécifique (INS) à la place du numéro d'identification de sécurité sociale (NIR). Cela présentait l'inconvénient majeur d'interdire en pratique à tout le secteur de la recherche d'avoir accès aux banques de données constituées par le secteur de la production de soins qui utilise le NIR. Il aurait fallu construire une passerelle entre l'univers de l'INS, avec le DMP et la messagerie sécurisée de santé, et l'univers des données de l'assurance maladie gouverné par le NIR.

Après de nombreuses années de discussion avec l'ASIP Santé, une délibération de la CNIL vient de modifier sa doctrine et d'accepter de lever l'obligation d'avoir un INS spécifique pour l'échange et le partage des données de santé.

M. Jean-François Parguet. – Les technologies des années 1980 ne permettaient pas de croiser des données alors qu'aujourd'hui, il n'y a plus besoin d'index pour croiser les bases de données. Selon les préconisations du rapport de M. Pierre Truche de 1997, il aurait fallu un identifiant pour chacune des différentes sphères : justice, intérieur, finances, santé, médico-social et médico-administratif. **À l'heure actuelle, l'identifiant n'est plus un gage de sécurité.**

M. Michel Gagneux. – **Aujourd'hui, l'enjeu est non plus dans l'identifiant mais dans le contrôle de l'accès au système.**

Chaque accès aux données d'un patient donne lieu à une traçabilité impétrable. Le patient lui-même peut contrôler tous les accès à son dossier intégralement retracés. De plus, un patient peut demander que tel professionnel de santé ou telle catégorie de professionnels de santé n'aient pas accès à ses données.

Tout médecin qui utilise le système du DMP ou la messagerie sécurisée de santé doit respecter les règles de l'espace de confiance et utiliser une carte à puce qui permet une authentification forte de son accès autorisé par le patient.

Les exigences de sécurité seront beaucoup plus fortes avec le système numérique qu'avec les pratiques actuelles où un dossier médical peut traîner sur un chariot, etc. On saura immédiatement le nom de l'infirmière qui a administré un traitement, sa qualification à dispenser ce traitement. La rigueur dans la préservation de la confidentialité des données sera bien supérieure à celle observée dans l'utilisation des dossiers « papier », des photocopies, etc.

Le DMP est dans une première phase de déploiement ; le dossier du patient électronique, dans les établissements de santé, se développe petit à petit. Un vaste programme d'hôpital numérique a été promu par le Gouvernement depuis trois ans et s'étend peu à peu.

Ce sont des processus très complexes qui supposent une réorganisation des soins. Il s'agit, à l'échelle nationale, d'un projet à l'horizon d'une génération.

Le DMP peut être à la fois utilisé par des professionnels de santé et le patient. **Il n'a pas vocation à recevoir toutes les données de santé d'un patient** mais uniquement les données pertinentes à partager dans un moment donné ou pour une prise en charge ultérieure. Il ne se substitue pas au dossier professionnel de santé constitué par le professionnel.

Le DMP est prêt à être déployé ; des tests ont été faits depuis 2011. C'est un produit qui fonctionne techniquement, qui est ergonomique, fiable et qui peut, s'il est bien utilisé, faire gagner du temps.

D'une manière générale, l'agence est l'opérateur chargé par le ministère de la santé d'établir les textes qui régissent la sécurité des informations de santé. Elle travaille de façon permanente avec l'ensemble des autorités compétentes en matière de sécurité des systèmes d'information et de protection des données.

Le dispositif du DMP, qui respecte les préconisations de l'ANSSI, peut être homologué au titre du référentiel général de sécurité (RGS).

L'ANSSI et la CNIL sont associées étroitement aux travaux portant sur la mise en place de la politique générale de sécurité des systèmes

d'information de santé ; l'ASIP Santé a créé l'identifiant national de santé en étroite collaboration avec le laboratoire de cryptologie appliquée de l'ANSSI.

La CNIL intervient pour délivrer un avis dans le cadre de la procédure d'agrément des hébergeurs de données de santé.

Si le site Internet de l'ASIP santé est susceptible de subir des attaques générales tous les jours, sans pour autant avoir jamais été pénétré depuis 2011 ; **le système de gestion du DMP n'a pas été attaqué, de manière ciblée, et des données de santé n'ont jamais été volées.**

L'hébergement sécurisé des données de santé est confié à des sociétés privées françaises choisies selon une procédure d'appel d'offres mais assorti de **procédures d'agrément particulièrement rigoureuses et coûteuses pour les entreprises.** Cela permet d'avoir un marché de professionnels spécialisés dans l'hébergement de données de santé favorables aux normes de haut niveau garantissant le respect des bonnes pratiques de sécurité et de la réglementation.

Les Anglais ont créé un dossier informatisé du patient relatif à la production de soins qui peut être partagé mais auquel le patient n'a pas accès. Ils n'ont pas mis en place de dossier de coordination de soins partagé qui serait l'équivalent du DMP.

Leur projet est d'ailleurs ralenti parce que, contrairement au choix français, ils n'ont pas mis au point de normes d'interopérabilité qui permettent aux systèmes d'échanger des informations quelles que soient leurs différences d'environnement. Le Royaume-Uni a confié la gestion des données de santé à des industriels différents, en découpant son territoire en plusieurs zones, rendant ainsi impossible le traitement et l'échange des données d'un dossier par un système autre que celui qui l'a conçu.

Le DMP a connu une première phase, de 2004 à 2007, lors de laquelle les politiques ont fixé des objectifs économiques, de généralisation et de quantité irréalisables, selon l'avis de tous les experts. Après un audit interministériel, auquel j'ai participé, aux conclusions assez sévères sur le projet initialement prévu, Mme Roseline Bachelot, ministre de la santé de l'époque, m'a demandé de formuler des propositions qui permettraient de relancer ce projet en définissant des conditions stratégiques à réunir pour sa réussite.

C'est en application des conclusions de ce rapport, qu'a été créée l'ASIP Santé afin de garantir l'interopérabilité et la sécurité dans les échanges et le partage des données de santé.

Un nouveau DMP a été mis en place sous forme expérimentale au début de l'année 2010 et son déploiement aurait pu commencer dès la fin de l'année 2011.

En raison du changement de gouvernement intervenu en 2012, la phase de développement a connu quelques retards mais ce déploiement est

maintenant inscrit dans la stratégie générale de santé et devrait être lancé à grande échelle.

Cela montre qu'il s'avère particulièrement difficile en France de concevoir des projets stratégiques complexes et de les inscrire dans le long terme d'autant plus lorsque l'on touche à de nombreux secteurs, l'organisation du poste de travail du professionnel de santé, la façon dont il va travailler avec l'hôpital, la façon dont le patient et le professionnel de santé vont communiquer, la façon dont l'assurance maladie et les services de l'État vont échanger des données. Dans ce domaine, les défis relèvent moins de la technologie que de la conduite du changement et de la réforme. De plus, la dualité de gouvernance, mal pilotée, entre l'assurance maladie et l'État rend la mise en place du projet du DMP plus difficile.

Sur ce sujet, tous les pays ont été confrontés, en fonction de leurs traits culturels, à de très grandes difficultés. Ce fut le cas pour le Royaume-Uni et le Canada.

Les pays scandinaves ont connu plus de succès en raison de leurs systèmes très intégrés et de petite taille ainsi que de leurs contraintes de climat, de géographie, qui les poussent à passer par la virtualisation.

La France est en panne d'une gouvernance, d'une définition de stratégie en matière de santé numérique et de pilotage de cette stratégie. La diversité des acteurs, leur propension à l'autonomie, la faiblesse du ministère de la santé, qui a perdu beaucoup d'expertise, en créant toutes ces agences sanitaires, posent un problème de gouvernance important.

Le DMP permettrait aux professionnels de santé de travailler de manière coopérative autour d'un même patient et de limiter le nombre d'examens redondants. Sans cet outil, la coordination des soins est difficile.

Aux États-Unis d'Amérique, les sociétés d'assurances ou les cliniques constituent des dossiers pour optimiser leur prise en charge en imposant leur système à leurs assurés.

En France, les professionnels de santé, tout comme les patients, restent très peu conscients de la nécessité de protéger les données de santé, très sensibles, intimes. De bonnes pratiques sont à promouvoir.

En 2008, le système de santé était atomisé, cloisonné, peu sécurisé et peu communiquant.

La communication constituera l'un des grands enjeux du déploiement du DMP. À noter que, dans une même journée, des patients qui pourraient se montrer frileux à l'idée de voir des médecins échanger leurs données de santé, n'hésitent pas à dévoiler, sur *Facebook,* des éléments de leur vie privée bien plus intimes. Ils pourraient aussi être victimes de nouveaux projets comme celui de *Google Health* ou de *Microsoft – Health Vault* - qui avaient essayé de mettre en place des dossiers médicaux mondiaux et virtuels sans se soucier de sécurité ni de confidentialité.

Ces opérateurs ont d'ailleurs renoncé à leur projet pour des raisons de modèle économique mais pas pour des raisons de sécurité.

Lorsque les systèmes de santé informatisés seront mis en place, ils seront beaucoup plus protecteurs des libertés individuelles que l'absence de système actuel.

M. Jean-François Parguet. – **Le DMP offre une traçabilité exhaustive des consultations dans la durée. C'est ce qui permet d'arbitrer le compromis entre la confidentialité et la perte de chances.** Car si l'on prévoit de la sécurité *a priori,* on peut priver le professionnel d'informations et, par conséquent, aboutir à ce que l'on appelle une perte de chances pour le patient.

La traçabilité offre une base simple à cet arbitrage et permettrait de pénaliser les usages fautifs si la pénalisation existait.

M. Michel Gagneux. – L'objectif de l'ASIP Santé a répondu à une nécessité de service public en mettant en place, avec le DMP et avec la messagerie sécurisée de santé, dont le développement va commencer cette année, des outils sécurisés à grande échelle au profit des professionnels de santé comme des patients. Néanmoins, **il s'avère impossible d'aller plus loin dans la façon de sécuriser l'espace de santé en raison du nombre important de professionnels de santé et de la disparité de leurs équipements informatiques.**

La clé du système mis en place pour le DMP et la messagerie sécurisée de santé réside dans l'obligation pour les professionnels de santé et les patients d'entrer dans l'espace de confiance, régi par des normes d'opérabilité, de sécurité et de cryptologie, pour pouvoir échanger des données de santé en toute sécurité quelle que soit la fragilité de l'environnement numérique des utilisateurs.

En revanche, on ne pourra jamais rien contre l'utilisation par un personnel de santé d'un matériel étranger, aux mises à jour de sécurité non effectuées, par exemple.

M. Jean-François Parguet. – La protection par l'antivirus reste illusoire. La guerre de la protection du poste de travail du professionnel de santé est perdue d'avance. **La sécurité doit être concentrée sur le système central.**

Il existe **953 000 cartes de professionnel de santé** (**CPS) qui produisent le milliard de feuilles de soin par an qui servent pour le tiers payant.**

L'ASIP Santé distribue un logiciel d'accès à la carte (« *Middleware* »**) que le professionnel de santé peut installer dans son système. Ce logiciel supporte des versions obsolètes de systèmes d'exploitation, comme *Windows XP*, car il est impossible d'imposer aux**

professionnels le changement du parc de matériel informatique des médecins libéraux.

M. Michel Gagneux. – En matière d'améliorations des conditions de sécurité, nous nous trouvons toujours sur une ligne de crête, une **tension entre facilité d'usage et garantie de la sécurité**.

À titre d'exemple, la messagerie sécurisée de santé destinée aux personnels de santé doit être compatible avec une certaine mobilité et il faut **définir jusqu'à quel point on peut alléger les normes de sécurité,** par exemple, pour allonger le temps d'ouverture des sessions.

Jusqu'à présent, **l'ASIP Santé a maintenu des principes de respect des normes de sécurité assez rigides.** Mais, pour que le système ne soit pas dissuasif à l'usage, il va falloir étudier les modalités d'un assouplissement, notamment pour la saisie du mot passe, qui ne dégrade par la sécurité.

Il paraît difficile d'imposer à un infirmier en tournée la saisie trop fréquente d'un mot passe de huit caractères, composé de lettres, de numéros, de signes de ponctuation, etc. Il sera tenté d'utiliser une messagerie disponible sur Internet comme *Gmail, Orange,* etc.

C'est l'usage, dans les années à venir, qui déterminera le bon compromis à trouver.

En accompagnant les usages et en menant une **politique de pédagogie, de sensibilisation et de communication** permanente, durable et récurrente, en direction des professionnels, des patients et de tous les utilisateurs, il sera possible de construire, petit à petit, une culture de bon usage de l'échange et du partage de la donnée de santé par le numérique avec une bonne sécurité de base.

DIRECTION GÉNÉRALE DE LA COMPÉTITIVITÉ, DE L'INDUSTRIE ET DES SERVICES (DGCIS)

Mme Cécile Dubarry, chef du service des technologies de l'information et de la communication à la Direction générale de la compétitivité, de l'industrie et des services (DGCIS)

26 mars 2014

Le ministère doit contribuer à développer significativement les usages numériques sans négliger pour autant le volet sécurité. Toutes les politiques publiques mises en œuvre par le ministère et plus largement par le Gouvernement en matière de soutien aux entreprises peuvent bénéficier à l'industrie de cybersécurité ; c'est notamment le cas des appels à projets de R&D des investissements d'avenir.

Ainsi, il a été décidé, en liaison avec le Commissariat général à l'investissement (CGI), l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et l'ensemble des administrations concernées, de **consacrer périodiquement des appels à projet à la thématique de la sécurité**. Par ailleurs, le choix a été fait de cibler les appels à projets sur des thématiques identifiées comme prioritaires. Ainsi l'appel à projets « sécurité numérique » des investissements d'avenir, clos en novembre 2013, portait sur des **thématiques très précises (outils de détection d'intrusion, outils de sécurisation des *smartphones)***.

Au-delà des solutions développées pour la protection des informations classifiées de défense, extrêmement robustes mais avec un degré d'ergonomie souvent éloigné de celui des solutions grands publics, il est nécessaire, en lien avec l'ANSSI, de promouvoir la réalisation de solutions de sécurité à destination du grand public ou des entreprises adaptées aux enjeux tout en correspondant ergonomiquement aux attentes des utilisateurs.

Le ministère est également amené à travailler sur certains textes législatifs ou réglementaires ayant un impact en matière de sécurité (dans le cadre de la transposition du paquet télécoms, par exemple) que ce soit en tant que chef de file ou en coopération avec d'autres ministères.

À la suite de la transposition du paquet télécom, l'État disposait de la possibilité d'imposer aux opérateurs télécoms le respect de règles de sécurité. Les dispositions adoptées dans le cadre de **l'article 22 de la loi de programmation militaire ont étendu les prérogatives de l'État en matière**

de capacité à imposer des règles de sécurité, en matière de déclaration d'incident ou de contrôle à tous les opérateurs d'importance vitale, bien au-delà du secteur des télécommunications.

Afin de faciliter la concertation entre les industriels et les grands donneurs d'ordre de la filière sécurité, le Premier ministre a installé, en octobre 2013, le comité de filière sécurité dont le secrétariat est assuré conjointement par la DGCIS et le secrétariat général de la défense et de la sécurité nationale (SGDSN).

Les besoins des grands donneurs d'ordre (sécurité aéroportuaire ou maritime par exemple) ne sont pas toujours très bien connus. De même, ces grands donneurs d'ordre ne connaissent pas forcément les solutions techniques à leur disposition. Il existe donc un réel besoin d'échanges auquel le SGDSN et le ministère répondent en copilotant un certain nombre d'initiatives dans ce domaine.

En matière de sécurité, l'ANSSI est un partenaire incontournable. C'est ainsi que le directeur général de l'ANSSI s'est vu confier la mise en place d'un plan en vue de favoriser le développement des solutions de cybersécurité en France (**plan cybersécurité de la Nouvelle France industrielle**) et de **consolider les acteurs** – souvent plutôt performants mais de taille trop réduite pour aller à l'international.

Par ailleurs, une sensibilisation générale des entreprises au numérique est mise en place en s'appuyant sur les réseaux locaux ; le **programme « transition numérique »** permet à près d'un millier de conseillers sur le terrain de relayer les messages localement pour **proposer sur le terrain des solutions clés en mains incluant des formations**.

De tels programmes sont rendus possibles par la présence sur le terrain de conseillers déjà au contact des entreprises et prêts à se battre pour le développement numérique des entreprises, à qui il est nécessaire de donner les moyens d'accomplissement d'une telle mission.

Une **mission qui permettra d'identifier les secteurs où le numérique peut apporter le plus dans les années à venir** a également été lancée par la ministre en charge du numérique car, dans certains secteurs, l'apport (ou l'impact) du numérique est souvent mésestimé ou analysé trop tardivement.

À titre d'exemple, le site d'*Expedia* a été utilisé par le groupe *Accor*, dans un premier temps pour vendre ses surcapacités hôtelières ; maintenant, 30 % de son chiffre d'affaires est réalisé *via Expedia*. Les évolutions du monde du tourisme, notamment par le numérique, viennent perturber les acteurs en place qui, pour certains, prennent conscience de ces évolutions un peu tardivement. **Ce que l'on veut faire pour ceux qui n'ont pas encore été touchés de plein fouet par le numérique, c'est de créer une dynamique de réflexion et de prise de conscience pour qu'ils subissent un peu moins ces mutations** dont l'ampleur est très variable selon les secteurs.

La pratique actuelle est de plus en plus que les consommateurs entrent dans les magasins, par exemple chez *Darty*, pour regarder voire tester les produits et, ensuite, les achètent sur Internet.

Dans la future loi sur le numérique, qui devrait venir devant le Parlement à l'automne 2014, au plus tôt, il pourrait y avoir un volet sur la **cybercriminalité** ou encore la **protection des données personnelles**.

Le ministre a demandé à l'ANSSI d'**élaborer des normes de sécurité pour les systèmes de comptage intelligents, sujet dont** personne ne s'était saisi jusqu'alors. Aujourd'hui, on s'aperçoit que **les objets connectés peuvent être des portes d'entrée pour les attaquants informatiques** lorsqu'ils ne sont pas forcément sécurisés et, lorsqu'ils sont sécurisés, ils ne sont pas forcément reconfigurables. **Il est important que des failles de sécurité ne puissent pas permettre la prise de contrôle de tels objets par des individus malveillants.**

Une action associative, nommée *Signal Spam*, a été mise en place afin de **permettre à chaque citoyen d'alerter la CNIL ou l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC)** de la réception de *spams*.

Derrière l'expression de souveraineté numérique, se cache notamment la préoccupation de la protection des données personnelles. Le *Safe Harbor* nord-américain permet aux Américains d'avoir accès à des données européennes à condition que certains engagements soient pris. Un point de préoccupation est que c'est le département du commerce américain, qui contrôle le respect de ces engagements alors qu'il est lui-même intéressé au développement de ses entreprises nationales.

Dans de telles conditions, **le *Safe Harbor* risque de ne pas constituer une protection suffisante pour les Européens. L'intégrité et la confidentialité des données ne sont pas garanties.** Certains **acteurs américains ont fait le choix de stocker toutes les données provenant d'Europe ou hors d'Europe mais ce choix** ne permet pas de garantir la protection des données.

L'acceptation de l'application en France du *Safe Harbor* risque par ailleurs de ne pas assurer une protection suffisante des citoyens et **de donner un avantage compétitif aux Nord-Américains qui stockeront les données sur le territoire américain**.

En mars 2014, **ce débat est venu devant le Parlement européen où il a été reconnu qu'il fallait encadrer l'ensemble de ces transferts de données. Mais les Américains se retranchent, en quelque sorte, sur leurs bases arrière en considérant que les normes européennes ne leur sont pas opposables.**

Dans le cadre de l'informatique en nuage, les petites et moyennes entreprises ne sont pas forcément bien armées pour apprécier si les offres de stockage correspondent à leurs besoins et si la sécurité numérique de leurs

données est correctement assurée (notamment pour ce qui concerne les aspects liés à l'interopérabilité et la réversibilité). Un travail est engagé avec l'ANSSI pour **labelliser les offres offrant un niveau de sécurité adéquat**.

Les échanges avec la CNIL sont limités mais la DGE porte une grande attention à son action.

Au sein de l'Union européenne, **le débat se focalise sur la neutralité des opérateurs de télécommunications mais il convient aussi de s'intéresser de près aux questions liées à la loyauté des plates-formes et des moteurs de recherche**.

Récemment l'*ICANN* a décidé d'ouvrir le marché des noms de domaines dits « génériques » **–** *generic Top-Level Domains* (*gTLD*), contre l'avis d'un certain nombre d'États. Aujourd'hui, elle lance **des appels d'offres relatifs aux noms de domaines qui vont être soumis au droit américain**, ce qui est une fragilité pour les entreprises françaises ou européennes. **Au niveau technique, l'*ICANN* dispose d'un contrôle très important sur les noms de domaine, lui donnant la capacité de perturber très significativement voire complètement le fonctionnement de l'Internet, du jour au lendemain.**

Avec l'ouverture du marché des noms de domaines génériques, les entreprises françaises seront obligées de déposer beaucoup de noms de domaines pour protéger leurs marques. Cette ouverture peut dans certains cas contribuer à fragiliser les appellations contrôlées comme dans le cas d'attribution du « .vin » ou du « .wine ».

Certes, au niveau de l'*ICANN*, il existe un *Govermental Advisory Committee* (*GAC*) mais ses préconisations ne sont que peu entendues par l'*ICANN*. Le gouvernement américain a cependant indiqué qu'il allait renoncer à un contrôle sur l'*ICANN*.

Au-delà des entreprises, le ministère considère comme essentiel de **sensibiliser les individus**, même si les recommandations en matière de sécurité ne sont pas nécessairement les mêmes. Il s'agit de **diffuser les bonnes pratiques, une sorte « d'hygiène numérique »**.

MEDEF

M. Pierre Louette, président du comité « *Transformation du numérique* »

Mme Anne-Florence Fagès, directrice de mission « *Économie numérique* » à la direction de la recherche et de l'innovation

27 mars 2014

M. Pierre Louette. – Dans le cadre de vos travaux, **v**ous avez déjà entendu la personne qui est la plus compétente dans ce champ, à savoir M. Jean-Luc Moliner, directeur de la sécurité chez *Orange*, domaine qui m'est rattaché au sein du groupe, et qui est très directement concerné par les très nombreux dangers de l'interconnexion.

Pour préparer la présente audition, nous avons choisi de nous inscrire dans le cadre de réponses au questionnaire que vous nous avez déjà adressé auquel nous ajouterons trois ou quatre messages que nous souhaitons partager avec vous.

Le MEDEF s'inscrit dans la protection des entreprises et entend donner une impulsion à travers une sensibilisation y compris auprès des **93 % des entreprises en France comptant moins de dix salariés ; c'est aussi auprès d'elles qu'il faut agir car elles sont tout aussi exposées que les très grandes entreprises** puisqu'elles sont aussi des fournisseurs et des sous-traitants de très grandes entreprises, des inventeurs de projets et de brevets.

Le comité de transformation numérique du MEDEF que j'anime émet des avis, donne une vision objective et nationale pour produire des éléments d'information nationaux et également va dans les territoires pour en faire remonter les préoccupations partagées. La sécurité concerne tout le monde et la sensibilisation est un sujet auquel le MEDEF s'attache.

Aujourd'hui, pour les entreprises, le principal risque lié au numérique consiste à ne pas y basculer.

Il peut être souligné que 80 % des entreprises françaises déclarées en faillite en 2013 n'étaient pas présentes sur Internet. Elles n'avaient pas développé une présence forte de vente ou une action sur Internet.

Mme Anne-Florence Fagès. – Il semble donc qu'on ne puisse pas développer une économie sans intégrer Internet.

M. Pierre Louette. – Cet enjeu de la transformation numérique concerne en particulier le secteur du voyage mais d'autres secteurs entiers seront affectés en totalité, comme le BTP, avec l'analyse par des spécialistes de la donnée des composants et des matériaux, des lieux d'implantation des

bâtiments ; comme les télécommunications, ils vont croiser des données. Ceux qui ne sont pas dans ces transformations risquent de passer à côté d'un facteur de survie et de croissance. Il est donc essentiel que les entreprises s'intègrent au fonctionnement de la nouvelle économie en faisant de l'Internet un levier de développement tout en sécurisant leur intégration dans le numérique. **La démarche d'entrer dans le numérique est autant vertueuse que risquée si elle ne s'accompagne pas d'un renforcement de la sécurité.**

C'est pour cela que nous nous intéressons beaucoup à la cybersécurité, à l'incitation massive à numériser. Il s'agit d'une « chance dangereuse », porteuse d'autonomie comme de danger, qui provient de **l'exposition à de nouveaux risques contre lesquels les entreprises ne sont pas forcément préparées**.

Dans le cadre des opérations de sensibilisation affichées par le MEDEF, il est expliqué que **le numérique est un facteur de compétitivité et de réduction de coûts pour l'entreprise**.

Deuxième réflexion : la cybersécurité constitue un véritable défi pour le MEDEF alors que confiance et sécurité sont indissociables du numérique. On aborde par là le thème de la confiance.

Récemment, un responsable du *FBI* américain déclarait qu'**il n'y a que deux catégories d'entreprises face à la sécurité informatique : les entreprises qui ont été attaquées et celles qui le seront ; le premier groupe étant le plus nombreux**. *Orange* subit plusieurs attaques par jour à un point ou un autre de ses réseaux très déployés et diversifiés ; tous les jours ces attaques sont tentées et, de temps en temps, certaines aboutissent.

Le côté spectaculaire de certaines des attaques menées risque d'éroder la confiance et de susciter une réticence à livrer ses données qui risque de diminuer la croissance liée au numérique. Les espoirs de croissance du numérique, de création d'entreprises et de croissance en général ne peuvent se concrétiser que si la sécurité et la confiance sont préservées.

Les entreprises visées par les cyberattaques sont souvent des PME qui ont peut-être omis de mettre en œuvre tout ce qu'il convenait pour assurer leur propre sécurité. **Plus de 70 % des entreprises victimes d'attaques en France comptent moins de cinq cents salariés.** Or, comme elles font partie de l'écosystème des grandes entreprises, ce nombre d'attaques ne cesse d'augmenter. Il peut s'agir d'attaques malignes pour chercher de l'information mais, également, d'attaques simplement destructrices, de blocages, avec le phénomène des dénis de services.

Les jeunes générations, très consommatrices d'*Apple* et de *Mac* à domicile, à travers des jeux ou de la création graphique, ont tendance à vouloir apporter leur ordinateur personnel sur le lieu de travail, ce que les entreprises favorisent plutôt mais cela est, en réalité, très compliqué. D'abord favorable à cette pratique, *Orange* est en train de lever sur le pied

sur ce point car cela est trop compliqué à gérer au quotidien puisque les personnes viennent avec leurs virus.

L'introduction de virus dans le système d'information de l'entreprise entraîne une perte de capacité et doit être évitée à tout prix.

Mme Anne-Florence Fagès. –Les entreprises déploient un arsenal de moyens de sécurisation et hésitent à demander à leurs personnels de contrôler et de sécuriser les matériels qu'ils apportent de chez eux. Finalement, ce n'est pas une très bonne idée d'autoriser l'apport d'outils personnels sur le lieu de travail, sans déployer parallèlement les garde-fous et protections nécessaires.

M. Pierre Louette. – On a eu d'abord le sentiment qu'il était bien de leur permettre aux chercheurs, et il y en a beaucoup chez *Orange*, près de six mille au sens large, d'apporter leurs outils personnels mais il a été constaté que c'était cette partie du réseau qui était la plus perméable car offrant un maximum de points d'échanges avec l'extérieur. On a effectué des tests d'intrusion qui ont montré une réelle porosité même si le dernier test a été plus rassurant que les précédents.

Il a aussi été observé que l'on faisait toujours attendre les visiteurs dans des lieux où se trouvent des prises de courant par lesquelles il peut être possible d'accéder au réseau.

Le MEDEF, estimant qu'il faut partager plus, a installé, au sein du comité de transformation numérique, un groupe de travail « confiance et sécurité » mis en œuvre avec la Fédération des entreprises de vente à distance (FEVAD) car elles sont au premier rang de celles qui doivent s'interroger sur la pérennité de leur propre activité si la confiance numérique venait à disparaître. Mais la problématique est partagée par toutes les fédérations du secteur numérique. D'où, pour la formation au numérique, la création d'un autre groupe de travail avec le Syntec-numérique incluant une formation à la sécurité, ce qui ne s'improvise pas.

La troisième réflexion à partager avec vous, c'est que le contexte réglementaire du numérique doit nécessairement s'adapter pour prendre en compte les évolutions technologiques et les failles constatées.

Quant au contenu du projet de loi sur la liberté numérique annoncé par la ministre chargée du numérique, Mme Fleur Pellerin, qui devrait permettre d'adapter la législation nationale à l'évolution internationale des données tout en préservant les libertés fondamentales, il est encore inconnu.

Ce projet devra en tout cas veiller à la protection de la sécurité face à la préservation des libertés fondamentales. Si le projet de loi s'appelle liberté numérique, il doit traiter de ces questions-là. Le MEDEF sera forcément associé à cette construction tout à fait importante**. Il serait temps de prévoir des dispositifs d'information des entreprises sur la sécurité. Il est**

important que les entreprises montrent qu'elles respectent certains modes de prophylaxie informatique.

Une des conditions de la liberté fondamentale de l'usage du numérique est sa sécurité. Il ne sert à rien d'afficher un objectif protecteur si des silos de données sont pillés. Il faut déjà **sélectionner ce que l'on veut soumettre à une bonne protection**.

Cette démarche doit s'insérer dans un développement global partagé par d'autres nations dans lequel **la France ne doit pas prévoir seule des dispositifs trop protecteurs si, au même moment subsistent, dans le cadre européen, des dispositifs permettant aux entreprises étrangères, notamment nord-américaines, d'échapper aux réglementations nationales**. J'évoquerai en particulier, le *Safe Harbor*, dispositif américain qui permet aux Américains d'éviter d'être soumis aux lois nationales ou européennes en invoquant cette réglementation.

J'ai eu l'occasion d'accompagner le président du MEDEF, M. Pierre Gattaz, à Las Vegas, pour une conférence lors de laquelle des entrepreneurs privés américains tenaient un discours de domination technologique mondiale. La question pour eux étant d'imposer la supériorité technologique nord-américaine au monde. C'est une machine puissante qui est à l'œuvre.

Actuellement, **la France est victime d'une fragmentation de l'Europe alors qu'elle doit affronter le marché unique nord-américain**. Cela a des conséquences immédiates en matière de propagation des produits car, quand bien même, dès 1997, *France Telecom* aurait réussi à développer un moteur de recherche aussi efficace que celui de *Google*, ce moteur n'aurait pu être déployé que dans un marché français d'environ cinquante-cinq millions d'habitants et non de quatre cents millions. Cela est toujours le cas aujourd'hui car **nous nous trouvons face à vingt-huit ARCEP (Autorités de régulation des communications électroniques et des postes), vingt-huit autorités de la concurrence, de la consommation car il n'existe pas un marché unique des télécommunications**. L'avantage d'Internet, c'est de ne rencontrer aucune barrière dans sa propagation. En fait, **sur la ligne de départ, chacun a potentiellement une vocation à devenir mondial mais ceux qui émergent sont assez rapidement rachetés par *Google*, *Facebook*, *etc.*** En effet, les opérateurs français ne peuvent se déployer aussi rapidement que les opérateurs américains.

De plus, depuis assez longtemps, les États-Unis d'Amérique ont abandonné la notion de service universel. Certains États, comme la Californie, ont eu la 4G bien avant les Français mais ont encore du mal à faire fonctionner une téléphonie de base. Une forte concentration s'opère sur le marché hyper utile, à savoir celui des grandes villes, tandis que des zones rurales sont un peu à l'abandon avec une distribution d'électricité qui ne fonctionne pas très bien. En France, nous avons une vision universelle de l'accès généralisé. Les Anglais et les Danois partagent cette vision. Mais la

fragmentation nous coûte très cher car elle rend impossible d'avoir un service se répandant très vite.

Le second aspect est l'état de la concurrence. Aux États-Unis, les télécommunications sont parvenues à un certain degré de reconcentration, de concurrence 3.0 – le 1.0 étant le monopole du temps de *Bell* et le 2.0 l'époque de la forte fragmentation. Même s'il reste aujourd'hui de multiples petits opérateurs de téléphonie fixe, dont on ne parle jamais, avec peu de clients. Les autorités de la concurrence sont débordées. De plus, il ne reste plus d'opérateur de téléphonie fixe mobile même s'il y a quatre grands opérateurs aux États-Unis du fait de la reconcentration. En Europe il y a encore cent vingt opérateurs de télécommunications. La Croatie qui vient d'entrer dans l'Union Européenne a elle-même trois ou quatre opérateurs téléphoniques.

La commission européenne vient d'autoriser le passage de quatre opérateurs à trois en Autriche, mais en accompagnant cela de la nécessité de créer seize *MVNO* (*Mobile Virtual Network Operator*), ce qui ne se produira jamais car le marché est dévasté et les prix extrêmement bas. **En France, la politique de la concurrence n'est pas propice à l'émergence de grands acteurs.**

Par ailleurs, l'accès au crédit est très facile aux États-Unis même pour ceux qui ont déjà créé une première entreprise qui a échoué.

En conclusion, il est à observer que tous les moteurs de recherche étaient, en 1997-1998, sur la même ligne de départ mais que, comme le moteur de recherche est auto-améliorant, plus il se propage vite, plus il est consulté et plus il s'améliore, et ainsi de suite, et donc sa domination s'accroît. Actuellement, **en France, 93 % du marché sont détenus par *Google***. Donc **le système devient lui-même producteur de nouveaux monopoles**. Même si nous sommes les tenants de la concurrence la plus forte, ce système de monopole se développe sous nos yeux.

Google est numéro un dans les moteurs de recherche avec des parts de marché monstrueuses. Après, il y a *Yahoo* et *Bing* puis plus grand monde. C'est comme cela dans chaque catégorie où il existe toujours un grand groupe dominant tout le monde et, en fait il s'agit de **systèmes quasi monopolistiques face au système européen où l'on a produit autant de concurrence que possible**. Il est probable que l'on a été trop loin dans la concurrence. La baisse des prix est devenue l'ennemi du développement de l'entreprise et de la croissance.

Pour revenir aux sujets de sécurité et de risques, **il est important qu'existe un sentiment de sécurité numérique même s'il n'est pas partagé par tous**. Par exemple, aux États-Unis, le noyau des personnes inquiètes demeure aux alentours de 3 %, soit au même niveau que dans les années 1970, à l'époque de M. Ralph Nader. **Pour ne pas casser la confiance, il faut**

développer la sécurité. Elle doit être renforcée aussi bien pour les entreprises que pour les individus.

Orange essaie de proposer des solutions de protection mais cela est modeste. En effet, dans le groupe *Orange*, dégageant trente-neuf milliards d'euros de chiffre d'affaires, la vente de données représente moins de dix millions d'euros. Si l'on devait quantifier la valeur que l'on tire de l'installation de sondes dans les réseaux, ce qui permet de mettre en place les capacités de transmission là où c'est nécessaire, l'on constaterait que ces sommes sont importantes mais à usage interne.

***Orange* estime qu'il est nécessaire que l'acceptation des personnes soit recueillie pour que leurs données puissent être vendues mais peu nombreux sont ceux qui l'acceptent volontiers.** Pour *Orange,* il n'est pas question de forcer les gens à voir leurs données vendues.

Pourtant, nombre de données personnelles sont disponibles en ce qui concerne le téléphone : qui téléphone à qui et de quel endroit. Cela pourrait servir la géolocalisation et le géomarketing de nombre d'entreprises.

Orange commercialise un peu les données agrégées, donc anonymisées, mais en aucun cas les données personnelles. Mais *Orange* se voulant un opérateur de confiance, il ne procède pas à la commercialisation des données personnelles de ses clients.

En matière de l'utilisation de données personnelles, la CNIL joue un rôle très important et les opérateurs se soumettent d'eux-mêmes à un certain nombre de restrictions car ils craignent davantage un scandale lié à l'utilisation non autorisée de données plutôt qu'ils n'espèrent profiter de l'exploitation d'un marché au demeurant pas très important.

Par ailleurs, il est très important que lors de l'examen des futurs projets de loi relatifs au numérique, à l'inverse de ce qui s'est passé pour la loi de programmation militaire, ne soit pas alimenté le débat opposant le numérique aux libertés individuelles qui risque de ruiner la confiance dans le numérique. Au lieu de cela, le législateur pourrait montrer que, comme le monde actuel produit forcément un grand nombre de données, il est possible de les gérer de manière encadrée permettant à la fois la vigilance et la sécurité. À partir de l'exploitation de données agrégées, de meilleurs services peuvent être assurés. **Il serait souhaitable de donner à la CNIL des moyens de sanctions renforcés car le niveau actuel des sanctions n'est plus adapté au monde actuel.**

Mme Anne-Florence Fagès. – Les données sont considérées comme le pétrole des années à venir et sont déjà une source de croissance et de création d'emplois. Les entreprises doivent pouvoir sécuriser au maximum les données sans bloquer l'innovation. Il faut à la fois libérer la créativité et l'innovation dans l'entreprise et protéger l'individu.

M. Pierre Louette. – Le MEDEF participe à beaucoup de réunions nationales et européennes ou à des séances de travail avec l'ANSSI dans le cadre de l'écosystème de la sécurité. Il en ressort notamment qu'il souhaitable que toutes les entreprises soient obligées de **notifier les incidents de sécurité dont elles ont été victimes**. Il reste à faciliter cela à l'aide de formulaires électroniques, par exemple, à adapter selon que l'on subit plusieurs attaques par jour ou bien une seule dans l'année. **À chaque fois, les pirates apprennent de leurs attaques tout comme les défenseurs apprennent des attaques des pirates. Ainsi, le système est auto-améliorant**, à l'instar du moteur de recherche de *Google*. Cela doit être accessible aussi bien aux petites entreprises qu'aux grandes.

Mme Anne-Florence Fagès. – Les petites entreprises ont quelquefois tendance à baisser la garde, ne serait-ce qu'en ne procédant pas régulièrement aux mises à jour de leur système d'information.

M. Pierre Louette. – **Les niveaux de protection sont extrêmement hétérogènes en fonction des clients.** Un client a même exigé que ses serveurs soient entourés de grillages au sein des centres de données car il souhaitait une protection physique séparant ses serveurs de ceux d'autres clients, ce qui est un peu étrange car les données circulent entre serveurs et, de plus, elles peuvent même circuler d'une unité à l'autre. Toujours est-il que cette exigence a été acceptée car provenant d'un grand client.

D'autres clients risquent, au contraire, d'accepter des offres de stockage numérique où leurs données seront stockées parmi d'autres sans qu'ils se rendent compte exactement du niveau de protection dont elles bénéficient.

Mme Anne-Florence Fagès. – Les entreprises ont un arbitrage à opérer entre le niveau de protection qui pourra leur être garanti dans leurs usages numériques et le coût financier de cette opération. Une des questions qui est posée au MEDEF est de savoir où le stockage de données sera implanté.

M. Pierre Louette. – Dans l'affaire de la *NSA*, il est impressionnant de constater que la captation massive de données est effectuée sans que l'on sache très bien ce qu'il sera possible de faire d'autant de données. À noter que, dans une phase ultérieure de leurs activités, les analystes de la *NSA* créent souvent des entreprises spécialisées dans l'analyse des données massives dans la Silicon Valley. À partir de ce qui se passe dans le domaine militaire, se prépare l'industrie de demain. Si ce cercle est vertueux pour les Nord-Américains, il ne l'est pas pour les autres. Il s'agit vraiment là d'un système militaro-industriel. La France est cependant loin d'être à la traîne dans ce domaine.

Mme Anne-Florence Fagès. – La France possède une très bonne école de statistiques comme de mathématiques mais il reste à stimuler les créations d'entreprises.

M. Pierre Louette. – En Allemagne, sous l'impulsion de Mme Angela Merkel, meurtrie de ses découvertes relatives à l'action de la *NSA*, un **effort national de cryptage** a été relancé.

L'**inclusion dans la loi de certaines obligations en matière de cryptage** concernant un certain type d'échanges pourrait être une voie à suivre, y compris par l'administration, de même que tout ce qui favoriserait la diffusion de telles mesures. Une initiative franco-allemande dans ce domaine serait très constructive d'autant qu'**il n'existe encore aucun moteur de coopération franco-allemand dans le domaine du numérique**. Cette coopération pourrait donc commencer par le domaine des cryptages plutôt que de voir de nouvelles industries allemandes prospérer seules dans ce secteur.

Par ailleurs, il serait intéressant de **mettre en place, dès la classe de sixième, une initiation au codage**.

Le MEDEF a énormément changé et ce monde d'entrepreneurs s'interroge sur la manière de se protéger en matière numérique. Un grand opérateur de télécoms français a mis en place un tableau de bord, qui devrait être bientôt opérationnel, permettant à chacun de suivre les données qu'il a laissées dans l'entreprise et, également, un système qui permettra d'éviter de noter les mots de passe en recevant un code par téléphone pour accéder à tel ou tel serveur à partir d'une carte *SIM*. Tout cela est mis en place pour faciliter l'accès aux sites, même protégés, sans que cette facilité s'étende aux attaquants.

Enfin, il serait intéressant, lors de la vente d'un téléphone, de mettre à disposition du client un petit **guide permettant d'indiquer la manière dont il convient de protéger ses données**.

DÉLÉGATION INTERMINISTÉRIELLE À L'INTELLIGENCE ÉCONOMIQUE

Mme Claude Revel,
déléguée interministérielle à l'intelligence économique

27 mars 2014

La délégation interministérielle à l'intelligence économique est placée auprès du Premier ministre depuis le décret du 22 août 2013. Précédemment, elle était rattachée au ministre chargé de l'économie et des finances et, encore auparavant, au Secrétariat général de la défense nationale (SGDN).

Le premier haut responsable, nommé en 2004, a été M. Alain Juillet remplacé, en 2009, par M. Olivier Buquen et j'ai été nommée le 29 mai 2013 au moment où délégation a été rattachée au Premier ministre.

De cette évolution découlent quelques conséquences. En ce qui concerne les missions de la délégation, elles sont définies autour de quatre piliers.

Le premier pilier, c'est la veille, l'anticipation et l'alerte des pouvoirs publics et du Gouvernement sur tous les sujets qui ont des enjeux économiques, scientifiques, techniques, industriels, etc. Ce premier pilier consistant à avoir de l'information sur son environnement est essentiel et les autres en découlent.

Le deuxième pilier, c'est la sécurité économique qui consiste en l'immatériel, c'est l'**intelligence économique**. C'est la préservation, la protection des savoir-faire, des recherches, de l'état de la recherche, des données, du capital, de la réputation, toutes ces choses immatérielles qui ont une valeur très grande pour les entreprises.

Le troisième pilier, c'est l'influence, c'est-à-dire d'abord être capable de **saisir les opportunités pour influer sur son environnement**, tout ça étant lié à l'anticipation, notamment le fait de savoir si telle ou telle nouvelle technologie va émerger ou si une autre va disparaître et quels sont les investisseurs concernés. On essaie d'organiser les événements pour qu'ils se passent comme on le souhaite au lieu d'attendre la crise ou que les autres choisissent pour vous.

Le second aspect de l'influence, c'est **l'influence sur les normes et sur les règles internationales**. C'est probablement une des raisons de ma

nomination car j'ai remis, en janvier 2013, un rapport à la ministre, Mme Nicole Bricq, intitulé : « *Développer une influence normative internationale stratégique pour la France* ». En effet, il y a un grand nombre de terrains sur lesquels on pourrait être bien davantage présent dans les organismes internationaux et les organismes normatifs en particulier.

Le quatrième pilier, c'est le pilier pédagogique, à savoir la sensibilisation à travers la formation initiale, la formation supérieure et la formation continue car **la plupart des risques sont d'origine humaine**. La sensibilisation, entendue dans un sens de protection mais aussi dans un sens proactif, est essentielle.

L'intelligence économique repose donc sur trois fondements : savoir, se prémunir et influer sur son environnement.

Pour en terminer avec la présentation générale de la délégation interministérielle à l'intelligence économique, celle-ci dispose désormais de moyens un peu accrus avec la possibilité de mobiliser des correspondants dans les ministères, dans les services déconcentrés de l'État en France et à l'étranger.

Il est même recommandé, dans le décret constitutif, de procéder à des échanges de vues avec le secteur privé, avec les entreprises ; cela est extrêmement important. Il faut échanger avec les entreprises, les organisations non gouvernementales, etc., tout ce qui n'est pas public**.**

Le décret précise également que la délégation doit participer à la politique de rayonnement international de la France ; elle est d'ailleurs associée à toutes les décisions concernant les investissements étrangers en France.

Voilà pour les textes. Mais il n'est pas facile d'agir alors que, en réalité, les pouvoirs de la délégation sont limités compte tenu des luttes de territoires diverses et variées de l'administration.

La délégation travaille déjà sur un certain nombre de sujets qui ont plus ou moins trait à la sécurité numérique mais la manière d'affronter les nouveaux risques numériques n'a pas encore été abordée de manière globale.

Quand on parle du numérique, cela peut se décliner de plusieurs manières, mais, ce qu'il faut arriver à faire, c'est **penser et maîtriser les technologies à l'avance**.

Tous les jours, de nouveaux défis doivent être affrontés compte tenu des innovations des concurrents. Ce qui se fait à l'international est particulièrement important à connaître.

Maîtriser les technologies et les penser dans notre intérêt peut être illustré par l'exemple de ce qui s'est passé aux États-Unis d'Amérique dans les années 1975-1980 à propos des autoroutes de l'information, les *High Ways*. À cette époque, un certain Al Gore disait partout que les autoroutes de

l'information étaient intéressantes et, par la suite, Internet a découlé de cette volonté de penser les autoroutes de l'information des années 2000.

À partir de la constatation que des technologies émergentes allaient dominer le monde, il y a eu la volonté de les maîtriser. Il ne faut pas être en retard. Les Américains sont actuellement à la tête de la gouvernance d'Internet, de grands empires industriels se sont créés car tout cela a été pensé et voulu.

L'information est devenue une matière première à partir de laquelle on peut réaliser ce que l'on veut. Comme toute matière première, elle peut être protégée, vendue, raffinée etc. De plus, les acteurs économiques qui utilisent cette matière première le font de manière totalement dérégulée. Ce qui n'est pas le cas de toutes les matières premières.

La délégation n'a pas un mandat sur la protection du numérique. Mais, comme ce sujet est essentiel, elle en traite notamment à travers la norme, la règle. Car si les défis du numérique sont technologiques, ils sont aussi humains et juridiques.

Il est possible de diminuer les risques à l'aide de règles juridiques.

La délégation à l'intelligence économique a quelques mandats spécifiques concernant le numérique. C'est ainsi que la réunion interministérielle du 12 février 2014, présidée par le directeur de cabinet du Premier ministre, a porté sur la cybersécurité. Dans ce cadre-là, nous avons été chargés d'améliorer la formation des PME à la cybersécurité en établissant un référentiel avec les chambres de commerce et d'industrie et en essayant de le diffuser *via* les chambres de commerce, les préfets et les autorités locales. Il y a eu toute une distribution de tâches effectuée entre les diverses administrations dont les premiers résultats devraient être perçus à la fin de l'année 2014.

J'ai été nommée membre de droit du Comité de la filière industrielle de sécurité (CoFIS), créé le 23 octobre 2013 ; l'idée étant de renforcer les industries françaises de la sécurité à travers une filière, comme cela existe pour d'autres industries. Au sein de ce comité siègent à la fois des acteurs publics et privés. La délégation à l'intelligence économique a pris en charge un sous-groupe sur l'intelligence normative. En effet, les normes sont extrêmement importantes car elles peuvent ouvrir ou fermer un marché. Il faut donc arriver à **fabriquer la norme avant les autres**. Or, **les normes techniques sont obligatoires pour l'interopérabilité des produits qui se vendent dans le monde entier**.

Les normes ne se font plus sous l'égide des pouvoirs publics nationaux ou internationaux mais elles proviennent des industriels, ce sont des normes de fait.

Actuellement, à Paris, se tient une réunion collaborative pour déterminer des normes sur les bandes dessinées, les mangas, les magazines

publiés sous forme numérique pour les rendre adaptables aux appareils mobiles. De nouvelles normes sont toujours nécessaires pour améliorer ces produits. Toutes les nationalités sont autour de la table et ce sont les industriels qui, entre eux, élaborent ces nouvelles normes.

Comme les normes numériques sont quelquefois liées à la sécurité, il pourrait être imaginé que ce soient les États qui les élaborent. Même au sein de l'*ISO*, la représentation des professionnels se fait par États et ces professionnels rendent compte aux États. Les pouvoirs publics sont tout de même derrière même s'ils ne sont pas présents.

À l'inverse, pour les normes de fait, il n'y a plus aucun aspect national. En général, le président de ce type de réunion est nord-américain même quand les négociations se passent en France. L'Américain commence par souligner que les règles de propriété intellectuelle n'ont pas leur place dans ce type d'enceinte où le secret des affaires n'est pas invocable. L'élaboration de la norme, la mise au point de nouvelles manières de faire très techniques devront être ouvertes et, ensuite, chacun pourra faire ce qu'il voudra ; la question demeurant de savoir comment gagner sa vie à partir d'un tel modèle.

Toutes les personnes présentes sont des producteurs qui ont pour ambition de vendre des produits élaborés selon ces nouvelles normes. Le principe est de se dire que les meilleurs au monde ayant élaboré les normes, les autres producteurs suivront.

La structure qui recevait ces jours-ci s'appelait l'ADPF et il est envisagé qu'elle s'unisse un jour avec *W3C* qui est l'organisme privé américain de référence en matière de normes numériques, quelque chose d'analogue à l'*ISO*.

Pour prendre un exemple, la norme de fait *GSM* a été fabriquée à Sophia-Antipolis, sans passer par l'*ISO*, à l'initiative de M. Didier Lombard qui a réuni des chercheurs, l'État étant présent ; des Allemands, des Hollandais, participaient, en plus des Français, à cette élaboration. Cette norme s'est imposée dans le monde et a donné naissance aux empires français qui existent aujourd'hui.

Au sein du CoFIS, si l'on pouvait arriver à fabriquer la norme ce serait formidable, à condition que les industriels et l'État s'y intéressent dans la durée.

Thales s'intéresse beaucoup aux normes de gouvernance, financières et comptables et, aussi, aux normes de responsabilité sociétale des entreprises (RSE), aux normes anticorruption ou aux normes anticoncurrentielles.

Le 19 décembre 2013, un Conseil européen de la défense s'est tenu pour réfléchir à des normes pour de nouveaux produits de défense à présenter avant la fin de l'année 2014.

Pour des sujets stratégiques, il est important de se réunir pour arrêter une position commune.

Quant à l'aspect juridique, la protection du secret des affaires, dont une partie est liée à l'accès numérique, une **proposition de loi** a été présentée, il y a deux ans, puis adoptée par l'Assemblée mais non par le Sénat. Elle a été reprise en tant que projet par mon prédécesseur en 2011 et doit être encore améliorée.

Un projet sur ce point, excédant d'ailleurs le champ du numérique, a été remis au cabinet du Premier ministre à la fin du mois de septembre 2013.

Pour garder le secret des affaires, il faut disposer de machines non reliées au *Net*, à aucun réseau, de cages de Faraday ou d'un brouillage sonore ambiant.

À propos du projet de règlement européen sur la protection des données, mené par la commissaire Mme Viviane Reding, actuellement en cours de négociation, il est freiné par tous les groupes de pression ultralibéraux (*Google* et autres) qui voient d'un très mauvais œil une régulation de l'utilisation des données.

Ce projet est soutenu par le Parlement européen qui, le 12 mars 2014, a émis un vote sur la protection des données qui obligerait les entreprises, lorsqu'elles travaillent sur le territoire européen, à **respecter le droit à l'effacement, le droit à l'oubli et l'obligation d'informer les personnes lorsque leurs données sont utilisées à des fins commerciales**.

Au-delà des données personnelles, qui sont importantes, il faut aussi prendre en compte les données économiques.

À noter qu'une bonne partie de ce qui a scandalisé à travers l'affaire Snowden est légale aux États-Unis d'Amérique **– *Patriot Act* ou autres qui, pour des raisons de sécurité, permettent de passer outre la protection des données**.

Sous l'empire de la directive de 1995, on ne peut fournir toutes les données, c'est pourquoi, l'Union européenne a négocié avec les États-Unis le *Safe Harbor* à travers lequel **il est convenu de traiter les données comme l'exige la directive de 1995… sauf si la sécurité est en jeu**. Il y a environ 4 000 organismes américains avec lesquels ce type de convention a été signé.

Le règlement Reding, en cours d'élaboration, a pour ambition de moderniser la directive de 1995. Il est à espérer que les conventions mentionnées ci-dessus ne pourront prospérer sous l'emprise du nouveau règlement européen.

Il serait souhaitable que les Français soient capables de mettre sur pied une force d'influence pour travailler au cœur de l'élaboration de ce nouveau règlement européen. La capacité d'influence au sein de l'Union européenne reste à mettre au point notamment en plaçant des personnes aux bons endroits.

Sur des sujets stratégiques de ce type, il faut que la position stratégique française soit élaborée et diffusée dans tous les cercles d'influence possibles.

Il faut commencer par rencontrer la personne en charge de l'écriture du texte européen pour expliquer la position française.

De plus, comme pour la protection des données, quand tout le monde est quasiment d'accord, il faut mettre au point une méthode pour éviter que chacun travaille dans son coin.

Un autre lieu juridique où ces aspects vont être traités sera la négociation sur le Traité de partenariat transatlantique avec les États-Unis d'Amérique (*TTIP*), l'accord de libre-échange entre les États-Unis et l'Union européenne.

Les Américains veulent un accord normatif dans tous les domaines dont les marchés publics et la propriété intellectuelle qui concerne directement les affaires de numérique et la protection des données. Cela est extrêmement important.

Mme Nicole Bricq a réuni à plusieurs reprises un comité d'anticipation sur cet accord et, dans ce cadre-là, il y a environ deux mois, le négociateur en chef européen a été reçu ; c'est un français, M. Jean-Luc Demarty mais il n'est pas très profrançais.

Il lui a été demandé si le statut des données faisait partie de cet accord et il a d'abord semblé répondre par la négative mais, en réalité, il parlait de l'exception culturelle. Il a affirmé ensuite que **les informations liées aux produits numériques entraient naturellement dans le cadre de l'accord puisque les produits numériques y entrent** en fonction du statut qui leur a été donné au niveau européen.

Dans ce contexte, **il serait souhaitable d'attendre que le règlement européen soit adopté avant que l'accord de libre-échange ne puisse être négocié car il ne faut pas commencer à négocier avant d'avoir une base européenne qui ne saurait être la directive de 1995 – dépassée**. C'est pour éviter cela que l'élaboration du règlement européen est freinée par tous les groupes de pression pour éviter qu'il puisse servir de protection européenne dans le cadre de la négociation de l'accord transatlantique de libre-échange.

Cette position, est également celle de Mme Viviane Reding.

Il faut donc éviter que les données entrent dans la négociation du traité tant qu'un socle réglementaire européen n'existe pas. Seuls les Allemands sont sur la même ligne que la France – sans doute stimulés par l'écoute du téléphone portable de la chancelière qui a indigné les Allemands.

La souveraineté numérique n'a plus de sens au niveau français mais a un sens au niveau européen où les Français doivent être davantage proactifs. Elle peut également avoir un sens à travers la présence française dans les cercles normatifs internationaux.

Le nuage numérique consiste à stocker des données dans des serveurs externalisés. Il y a eu, le 29 mars 2013, une réunion interministérielle sur l'informatique en nuage et sur les stratégies françaises et européennes demandant aux ministères de se concerter sur le projet de règlement européen, sur la proposition de directive destinée à assurer un niveau élevé de sécurité des réseaux et de l'information dans l'Union européenne et, également, sur le projet d'accord de libre-échange entre l'Union européenne et les États-Unis d'Amérique.

Le côté national peut être réaffirmé à travers la confiance à accorder au numérique à travers la constitution de nuages numériques français car, étant français, ils ont leur siège en France et sont soumis aux lois françaises. Or, la France à un niveau très élevé de protection des données.

Il faut distinguer la loi du lieu où se trouve le serveur de celle du lieu du siège social du propriétaire de ce serveur. *OVH*, qui constitue une très belle réussite, est situé en France. Lorsque l'on a des hébergeurs français, l'État devrait inciter les grands groupes à les utiliser. À cet égard, le Conseil national du numérique a élaboré une note précisant que **l'existence d'instruments nationaux n'est pas hors de portée** puisque les Japonais ont réalisé un nuage japonais et un *Facebook* japonais qui sont préférés par les consommateurs à *Facebook* et aux nuages américains.

Pour *Google* notamment, la principale source de revenus est constituée par les consommateurs européens. C'est pour cela qu'il s'oppose absolument au fait que nous ayons des règlements en Europe.

Les Chinois ont leur propre équivalent pour *Google*.

Il faut une volonté nationale de promouvoir les outils français : des hébergeurs français, des nuages numériques français, dans un cadre français, avec des réseaux français. Une sensibilisation est essentielle pour cela. Cela peut partir des grands groupes dans lesquels il y a des représentants de l'État.

Sinon, **il est impossible d'avoir quelque confiance que ce soit dans le nuage numérique**, y compris dans les nuages français et d'autant moins lorsqu'ils sont gouvernés par des lois non françaises.

Les experts américains ou anglais, les cabinets de conseil ne peuvent être totalement crus car leurs lois permettent aux gouvernements de requérir quand ils veulent des données détenues. Il en va de même en Chine.

Les ingénieurs français, excellents techniquement, doivent être sensibilisés à ces questions de protection française.

Le secrétariat général de la défense et de la sécurité nationale SGDSN a mis en place des zones à régime restrictif (ZRR) de protection concernant certains laboratoires de recherche dans le cadre de la protection du patrimoine scientifique et technique et a demandé qu'il y ait beaucoup

plus de laboratoires sous zone ZRR. Les chercheurs sont vent debout contre cette initiative. En réalité, **il faudrait que les chercheurs eux-mêmes sachent déterminer ce qu'est une information stratégique**.

Il ne faudrait pas que les chercheurs donnent toutes leurs informations sur le réseau : les noms des personnes avec lesquelles ils travaillent, les informations relatives au dernier état de leurs recherches, etc.

Pour les laboratoires dans lesquels la France est très en avance, il faut vraiment prendre en compte ce qu'est l'information stratégique. Il ne faut pas signer des accords de propriété intellectuelle à l'étranger avant d'avoir consulté le service juridique de leur employeur pour vérifier l'accord avant de le signer.

Il n'est pas nécessaire de livrer toutes ses informations pour remporter un appel d'offres.

Pour l'instant, la délégation à l'intelligence économique est un peu entravée dans son action par le manque de moyens. Elle ne dispose que de quatre collaborateurs sur un site, d'autres sur un deuxième et encore deux personnes sur un troisième site. Les systèmes informatiques de ces trois endroits sont incompatibles.

Pour l'instant il n'y a aucune coopération avec la CNIL. Il serait souhaitable de développer une stratégie en commun pour dominer et maîtriser le risque numérique.

En revanche, il y a travail en commun avec l'ANSSI notamment sur les questions internationales, normatives et européennes, sur la pédagogie en matière de cybersécurité. Des **fiches de sécurité économique**, qui seront présentées prochainement, ont été élaborées en commun avec l'ANSSI. Quelques-unes de ces fiches, très simples, portent sur le numérique et donnent des conseils pratiques.

Safran, *Thales*, toutes les grandes entreprises sont sensibles à la protection des données ; le *GIFAS* les rassemble tous sur la même ligne. Mais certains sont concurrents entre eux ce qui complique la coopération.

Les PME ne sont pas assez informées des risques du numérique. Il serait souhaitable aussi de dispenser une formation en intelligence économique auprès des PME.

De même, des **sensibilisations à l'intelligence économique** ont été débutées dans l'enseignement supérieur en septembre 2011 à destination d'une trentaine d'établissements pilotes où **quarante heures d'intelligence économique** doivent être enseignées, tous *cursus* confondus. Soit, seize heures d'intelligence économique au niveau M1 et vingt-quatre heures au niveau M2.

Le test s'achèvera en juin 2014 et donnera lieu à une évaluation.

J'ai moi-même été professeur dans un enseignement pilote où j'ai eu l'occasion d'enseigner cela.

L'ennui, c'est que des personnes s'autoproclament formateurs en intelligence économique allant jusqu'à expliquer comment provoquer une dépression nerveuse chez un chef d'entreprise en s'attaquant au capital de sa société.

Mais, au-delà de la technique, de l'outil, il s'agit d'abord de pratiques humaines.

Les investissements prioritaires dans le domaine de la sécurité numérique pourraient constituer la **promotion de sites français, de nuages français et de produits de sécurité français et travailler sur le droit européen** lié à ces sujets.

Il faudrait simplifier la vie des petites entreprises françaises du secteur du numérique car beaucoup de celles-ci sont confrontées à des problèmes sans nom de formalités excessives… Il faudrait veiller à ce que des simplifications aient réellement lieu.

Il faut appliquer la directive européenne, mais sans faire de zèle – comme le font les Anglais et les Allemands –, ne pas publier des données excessives, protéger les entreprises. Par exemple, en matière de publication des comptes, il est possible de les déposer auprès de l'autorité de tutelle des comptes de toutes les entreprises mais rien n'oblige à les publier. En termes de concurrence, il n'est pas bon de livrer ses données aux concurrents et, en plus, c'est compliqué.

Par ailleurs, il faudrait tenter d'éviter ce qui est appelé « *la vallée de la mort* », c'est-à-dire que les petites entreprises innovantes soient aidées également deux ou trois années après leur création. Par exemple, pour favoriser l'investissement en capital à ce moment-là.

Il advient que l'on trouve davantage d'investisseurs chinois, coréens, russes, américains en France que d'investisseurs français pour prendre ce type de risque.

La délégation à l'intelligence économique n'a jamais subi d'attaque informatique.

Au niveau des ministères, on pourrait imaginer une politique de sécurité informatique forte comprenant une **formation des ministres, des parlementaires et des principaux responsables aux exigences de la sécurité numérique**.

Les encourager, par exemple, à **ne plus employer *gmail.com*** car c'est *Google*. À noter qu'un logiciel peut permettre d'accéder à sa fiche *Google* résultant de votre boîte de messagerie *gmail.com* qui indique tous les sites sur lesquels vous êtes allés, les thèmes de votre recherche et, en plus, tous vos déplacements en France comme à l'étranger.

L'*ICANN* est américaine mais son conseil d'administration est extrêmement large. **Il serait souhaitable qu'elle compte des membres français influents au sein du conseil de cette association**.

ÉCOLE SUPÉRIEURE D'INFORMATIQUE ÉLECTRONIQUE AUTOMATIQUE (ESIEA) OUEST

M. Éric Filiol, directeur du laboratoire de cryptologie et de virologie opérationnelles

2 avril 2014

Les récentes révélations de la presse sur l'affaire Snowden n'ont pas fini de nous réserver quelques surprises même si les spécialistes n'ont pas été vraiment étonnés.

Les premiers programmes d'espionnage *US* – dont *Prism* n'est qu'une suite – ont été mis en place par les Américains dès la fin des années 1940. La technologie des communications et de l'information s'était déjà révélée comme étant vraiment du domaine militaire et nécessitant un contrôle ; dès cette époque, le général De Gaulle avait décidé que ça devait être une affaire strictement nationale, en particulier tout ce qui touchait au chiffrement des communications souveraines (étatiques). Le problème, c'est que, année après année, **la technologie évoluant, elle a envahi nos vies et conduit à une perte quasi totale de souveraineté par des situations de quasi-monopole des États-Unis d'Amérique**.

Certes, l'exception culturelle est importante d'autant que, dans la tentative d'assimilation de tous les pays par un seul, la culture est un enjeu important. Elle fait partie du plan consistant à faire adhérer à des normes et à une culture dominante. Le but ultime est le contrôle des populations assimilées *via* la divulgation permanente de la vie de tous. Face à cela, la France devrait, comme le font les États-Unis d'Amérique, mais en violation des accords internationaux en matière de commerce, considérer que **les questions de sécurité doivent être sorties des accords internationaux et imposer que, dans un certain nombre de domaines, les produits soient purement français ou *a minima* européens (et relevant du droit européen et non plus anglo-saxon).**

Un exemple, emblématique, a été cité par M. Jean-Marie Bockel, à savoir les routeurs qui sont des équipements en réseaux que l'on trouve partout, ce sont des gares de triage de l'information. Ils constituent un matériel critique mais facile à produire car ils ne requièrent pas, à l'inverse des processeurs, d'industrie lourde. Pendant longtemps, il y a eu une fourniture française en matière de routeurs grâce à *Alcatel* ; de ce fait, on était à peu près sûr de savoir ce qui se trouvait, ou non, dans les routeurs. Dans le

contexte du commerce international sous domination nord-américaine, on a envie de **savoir par qui on est espionné** en ayant déjà admis que le seul choix qui nous reste est celui de choisir qui nous espionnera.

Le sénateur Bockel avait, à juste titre, alerté l'opinion sur les routeurs chinois mais les routeurs américains sont tout aussi dangereux. **Pour les infrastructures critiques, il faut revenir à une certaine souveraineté, sinon française, du moins européenne, qui serait de nature à créer des marchés.**

L'esprit français, assez particulier, l'un des plus innovants de la planète, en ce qu'il est un mélange de Descartes et de l'esprit gaulois, fait que les Français sont capables de produire des choses étonnantes. Technologiquement et par voie de conséquence, économiquement et psychologiquement, **la France a vocation à figurer parmi les nations qui comptent mais cela ne sera pas possible si l'on utilise des outils fournis par l'adversaire** dont les Chinois. Comment peut-on construire une cyberdéfense rationnelle et indépendante en faisant le choix du tout *Microsoft* pour nos armées ? La France mériterait mieux que de se borner à choisir par qui elle peut être dominée.

L'évolution technologique a également comme conséquence que, à l'heure actuelle, la désinformation devient de plus en plus compliquée car les organismes de renseignement de pays comme les États-Unis d'Amérique, la Russie, la Chine, leur permettent de dominer beaucoup de choses, notamment dans le domaine mathématique ou informatique, ce qui facilite le repérage d'informations discordantes et rend difficile voire impossible la désinformation.

Autrefois, une image satellite permettait de distinguer un char. Maintenant, avec *Google earth* et une vision inclinée, des détails bien plus précis sont identifiables et on se demande comment cela peut être autorisé par un État comme la France. Quand la *Google car* passe dans les rues pour effectuer des relevés, si quelqu'un a sa porte ouverte, c'est comme si on entrait chez lui ; il s'agit là d'un viol des vies privées. Désormais, pour monter un cambriolage, il suffit de rapprocher l'information de *Facebook* de celle du plan de masse reproduit par *Google*. En informatisant les informations, on amplifie les possibilités de croisement et de renseignement.

Après les attentats du 11 septembre 2001, il a été établi que les États-Unis avaient eu en leur possession toutes les informations mais n'avaient pas été en mesure de les traiter. Par la suite, d'énormes progrès ont été faits avec la capacité de traiter très rapidement un très grand nombre de données (*data mining* appliqué au domaine du *big data*). En effet, il existe de nombreux modèles mathématiques qui permettent de se retrouver, dans des données massives, des informations sensibles voire très sensibles (extraction de connaissances) et cela va bien au-delà des techniques proposées par les nuages numériques dont on parle beaucoup.

Finalement, le traitement de données massives peut permettre d'exploiter utilement même une information d'apparence anodine en jugeant de son niveau de confidentialité. **Cela va devenir de plus en plus difficile de qualifier le niveau de criticité d'une information.**

Si l'on prend le cas du réseau ferroviaire, il suffit de quatre ou cinq personnes pour bloquer pendant quarante-huit ou soixante-douze heures l'ensemble du réseau à condition d'intervenir au bon moment et au bon endroit grâce à **l'exploitation de l'information ouverte**, qui peut devenir une information opérationnelle pour quelqu'un de malfaisant.

Cependant, même si la cybersécurité a son importance, le danger n'est pas où l'on pourrait croire. Ce n'est pas une attaque informatique qui, à elle seule, va bloquer un pays car les systèmes sont suffisamment variés et bien gérés. Les syndromes de type Tarnac, « hacktivismes » extrêmes sont plus inquiétants. En effet, à partir d'une bonne information, beaucoup de dégâts peuvent être causés par un petit groupe de personnes qui disposent de moyens conventionnels. Par exemple, les infrastructures critiques nord-américaines pourraient être bloquées durablement. En fait, si après une panne d'électricité de quelques minutes, beaucoup de choses se remettent en place, il n'en va pas de même après plusieurs heures d'interruption. C'est ainsi qu'une attaque, dans le sud-ouest de la France, a pu provoquer une panne d'électricité chez les abonnés à partir de seulement quatre armoires électriques qui avaient sauté. Cela a montré qu'**il est possible de bloquer relativement durablement Internet, le téléphone, etc**.

Ces attaques vont devenir de plus en plus faciles à mettre en œuvre. La capacité de traitement des informations, notamment par des particuliers, existe désormais et requiert peu de moyens. Elle permet, en quelques jours, d'identifier les points critiques pour des attaques à partir de données uniquement ouvertes. Les informations qui concernent les infrastructures, les personnes, sont soit directement ouvertes soit semi-ouvertes.

Les États-Unis d'Amérique ont avoué avoir exagéré la menace terroriste pour finalement mettre en place une cybersurveillance du monde entier. Quatre-vingts chefs d'État seraient surveillés en permanence. Le côté systématisé et permanent étonne autant que le fait que seuls deux responsables politiques ont réagi ; il s'agit de deux femmes, la présidente du Brésil et la chancelière allemande.

En France, je ne suis pas persuadé que la population et les décideurs aient été indignés outre mesure par l'affaire Snowden. Pourtant, j'avais d'abord été surpris quand l'ancien patron de l'ANSSI avait déclaré que, chez nous, l'affaire Snowden ne changerait probablement rien.

À noter que les Américains eux-mêmes sont également obligés d'acheter des matériels chinois. Dans tous les domaines, la réalité technologique du numérique implique également les Chinois et

les Indiens - même si, au départ, le terme Internet, français, a été inventé par le CERN.

Il faut bien distinguer le peuple américain du gouvernement américain qui a une certaine vision hégémonique. C'est pourquoi il est choquant de ne pas réagir quand il pille systématiquement nos entreprises pour maintenir une suprématie qui n'est pas aussi légitime qu'il le croit.

Face aux Américains qui violent constamment les accords de l'organisation mondiale du commerce, **la France devrait affirmer qu'elle ne veut pas sous-traiter sa sécurité.**

Récemment, Mme Angela Merkel a proposé que soit utilisé un réseau Internet européen, proposition refusée par le chef de l'État français. Le problème est que la France et l'Allemagne ont accepté d'agir pendant de nombreuses années comme sous-traitants de programmes d'espionnage américain, comme le programme *Lustre ;* l'affaire *Orange* a montré que cette société coopérait, notamment sur l'affaire des câbles sous-marins, avec le gouvernement américain. Le Service fédéral de renseignement allemand (*BND*) n'est pas tout à fait clair non plus.

En outre, il faut voir au-delà des faits bruts. Jusqu'en 1995, deux sociétés suisses avaient la quasi-suprématie sur le marché des machines à chiffrer pour usage gouvernemental. En réalité, dès la fin des années 1950, les Américains avaient infiltré une de ces sociétés suisses et fait en sorte que toutes les machines vendues par cette société à des postes diplomatiques, par exemple, soient **accessibles aux Américains comme des livres ouverts**. En 1995, un commercial de premier rang de cette société a été retenu en Iran car il y avait eu des fuites dans la presse qui prouvaient que les occidentaux décryptaient les messages iraniens. Toutes les machines vendues à l'export étaient trafiquées. Néanmoins, si le travail avait été organisé aux États-Unis, les gouvernements allemand, avec *Siemens*, suédois avec *Ericsson* et *Transvertex,* et hongrois étaient impliqués. Cela montrait que les Européens n'étaient pas forcément opposés à ce genre de pratique.

Les prochaines révélations de Snowden vont être passionnantes mais il n'est pas certain qu'elles ne ciblent pas la France. Et il faut s'attendre prochainement à l'apparition d'autres Snowden.

Actuellement, les Russes sont très méfiants vis-à-vis de la technologie occidentale et envisagent de mettre en place une normalisation autonome permettant la protection de toute la société russe.

Dans ce contexte, il semble impossible de rester sans réagir, notamment au moyen du chiffrement pour lequel **la France est bien armée** notamment du fait de son école de mathématiques. Mais l'esprit des chercheurs a malheureusement été pollué par la règle « *publier ou périr* ». Ceux qui font le choix d'aller travailler à la direction générale de l'armement à Bruz produisent de brillants algorithmes mais, de plus en plus, malheureusement, depuis que la France a réintégré le commandement

militaire de l'OTAN, on devra utiliser des algorithmes américains. Les pays, notamment pour leurs armées, ont basculé massivement sur *Windows* et dépendent d'un contrat avec *Cisco*.

Un produit militaire va peut-être devenir un produit standard de chiffrement pour l'Europe : c'est le logiciel de chiffrement *Acid* mis au point par des mathématiciens français de la DGA. Mais, dans l'utilisation européenne de ce chiffrement par blocs, on sera obligé d'intégrer le standard *AES* fourni gratuitement par les États-Unis d'Amérique, ce qui constitue un *diktat* de fait. Actuellement, nous sommes victimes des normes américaines ou chinoises (comme le classement de Shanghai).

Comme l'a mentionné le sénateur Jean-Marie Bockel, il existe une frange importante de jeunes *hackers* qui constituent des ressources de premier ordre. Ils sont loin d'être des autistes et il serait intéressant de les écouter. La France possède l'avantage majeur d'avoir de nombreux jeunes brillants dans le domaine du numérique même s'ils ne sont pas les plus diplômés. Malheureusement, *Google* et d'autres sociétés étrangères sont actuellement en train de piller ce vivier de jeunes. Un sursaut national s'impose pour tirer parti de ces savoir-faire et de ces bonnes volontés. À l'étranger, les États-Unis d'Amérique ou Singapour les accueillent à bras ouverts.

Avant, le chiffrement supposait d'intercepter la transmission. L'arrivée de l'informatique a révolutionné cela. Snowden a révélé que c'étaient moins les algorithmes qui protégeaient, comme des sortes de portes blindées de systèmes informatiques, que la solidité des murs autour des portes, trop souvent aujourd'hui les équivalents de murs en carton. Dès lors, plutôt que de s'attaquer à la porte blindée, il est plus facile de découper le mur à l'aide d'un *cutter*. La plupart du temps, **les normes américaines permettent d'extraire ce qui est sur l'ordinateur au moyen, par exemple, d'une porte cachée (*backdoor*) située sur le disque dur ou dans le système d'exploitation (*firmware*). Il faut donc avoir une vision globale de la sécurité** incluant les portes et les murs.

Or, comme nous n'avons ni la maîtrise de l'informatique ni la maîtrise des systèmes d'exploitation fournis par l'adversaire, quand *Microsoft* fournit un antivirus, il peut faire ce qu'il veut, quand il le veut, sur nos systèmes.

Les processeurs contiennent des portes dérobées. Il faut savoir que leurs codes peuvent être changés à la volée, c'est ce que l'on appelle le microcode. La procédure même de sa mise à jour est opaque et non documentée. Pour l'essentiel, les processeurs sont de marque *Intel*. Les seuls processeurs, pas très puissants encore, mais sur lesquels on peut intervenir sont des processeurs *ARM* fondés sur des architectures *RISC* (*Reduced Instruction Set Computer,* microprocesseur à jeu d'instructions réduit) et développés par la société *ARM Ltd*.

À noter que **le cryptage est une condition nécessaire mais non suffisante**. Quand les ordinateurs sont commandés à des entreprises américaines, Snowden a révélé qu'ils pouvaient être piégés par la *NSA* (programme la section *TAO – Tailored Access Operations* – de la *NSA*).

La réglementation interministérielle (IGI 900) dit bien que, si l'on veut faire un système de sécurité rationnel, c'est un triptyque qui doit comprendre **le chiffrement** (la porte blindée), **la sécurité informatique** – la solidité du mur, **la lutte contre les signaux parasites compromettants** – c'est-à-dire que, si vous travaillez sur un ordinateur et que vous ne chiffrez pas vos informations, le matériel va rayonner et, en captant ce signal, on va pouvoir le traiter mathématiquement, à 150 m en propagation par air et jusqu'à 500 m par conduction. Si l'on travaille sur un ordinateur, on peut capter ses ondes grâce à un canal électrique ou à une conduite de chauffage ou de téléphone ; à ce moment-là des personnes peuvent récupérer l'information, par exemple, dans la chaufferie.

Les techniques sécurisées sont utilisées par les grands corps de l'État, qui savent que **la cryptographie seule ne suffit pas**, et comprennent la sécurité informatique au centre et autour incluant la gestion des personnels et des matériels. Le problème, c'est que tout est occulté sauf la partie cryptographie sur laquelle on se focalise. C'est très simple de mettre un virus dans un ordinateur ou de l'avoir fabriqué en y mettant des fonctions non renseignées ou non documentées dans le système d'exploitation ; au moment où vous saisissez la clé, on pourra la récupérer.

Le cryptage quantique pour l'instant se limite à la transmission sécurisée de clés aussi longue que le message et pas vraiment au chiffrement. On combine un masque de bruit à des données en clair à travers une transmission de données par flot. L'inviolabilité peut être garantie grâce à ce système, comme le protocole *Brassard-Bennett*. Le chiffrement quantique n'est pas encore tout à fait au point. Mais on peut garantir qu'il n'y a pas eu d'écoute. C'est ce que font les banques suisses qui ont beaucoup investi : elles ont été capables de faire des transmissions à faible débit jusqu'à environ 60 km.

Un problème d'implémentation se pose pour la transmission quantique. Or, des chercheurs norvégiens ont montré que, en éblouissant des photons, on pouvait faire des choix en termes d'attaque. Cela est un gain théorique important et très coûteux mais les débits ne sont pas encore au rendez-vous. Cette technologie est donc prometteuse mais entourée de beaucoup d'incertitudes.

Se pose la question de savoir si ce champ de recherche n'a pas été suggéré et favorisé par les Américains pour inciter les autres à engager des dépenses extraordinaires au détriment d'autres domaines de recherche prometteurs comme la cryptographie, sont à favoriser. La France a tous les mathématiciens pour le faire tout en accroissant l'incertitude chez

l'adversaire. Il faut faire en sorte que les interceptions coûtent beaucoup plus cher aux États-Unis que la valeur du renseignement retiré. **Le quantique serait le meilleur moyen d'épuiser les fonds en matière de recherche et d'empêcher d'aller explorer des champs finalement pas si prometteurs que cela.**

Il faut acquérir à nouveau une indépendance conceptuelle en termes de mathématiques et ne plus dépendre de standards étrangers (comme l'*AES*). C'est le choix fait par les Russes avec l'algorithme *GOST*. **Une vision plus large que celle de l'outil s'impose.**

Il faudrait se trouver à nouveau dans la situation où sont actuellement les Américains, c'est-à-dire être à même d'imposer des normes – cela était la vision du Général de Gaulle. En effet, à travers ces normes, vous standardisez la pensée en obligeant à choisir un système dont on ne peut être sûr. **Pour beaucoup de standards, l'absence de preuves d'insécurité est devenue une preuve de sécurité en soi, ce qui est particulièrement gênant**.

De plus, si quelqu'un arrive à décrypter les algorithmes, opérationnellement un algorithme ou un standard de chiffrement, il n'ira pas publier sa découverte. Ce que savent faire les gens n'est pas forcément révélé dans ce domaine. Dans le domaine informatique, l'absence de preuve doit être prise avec beaucoup de précautions. L'école française de mathématiques devrait se demander s'il ne faut pas emprunter d'autres pistes en matière de recherche mais, **au niveau international, il faut publier selon les thèmes qui ne sont jamais choisis par les Français**. Je l'ai vécu en tant que chercheur : dans certains comités de programmes, dans certains domaines très sensibles, comme les fonctions booléennes ou la combinatoire des systèmes de chiffrement, on ne veut pas qu'il y ait des publications et tout le monde est amené à conduire des recherches selon l'orthodoxie américaine. À cet égard, un papier très intéressant a été publié par une Autrichienne, dans le domaine des mathématiques, modélisant les boites de substitution du *Data Encryption Standard* (*DES*), algorithme de chiffrement symétrique ou par blocs, mais on n'a plus jamais entendu parler d'elle. Or, un tel article était de nature à susciter beaucoup d'interrogations et de recherches. Les thèses différentes ou en rupture d'orthodoxie scientifique n'ont pas droit de cité.

Les Américains maîtrisent <u>les revues internationales, les organismes d'indexation de celles-ci, d'évaluation ou de notation</u>. C'est un jeu pervers qui concerne le contrôle des esprits. Un jeune chercheur doit publier pour exister, aller dans le sens de l'orthodoxie ; cela entraîne, peu à peu, le formatage des esprits ainsi qu'une **orientation de la recherche**.

À ce jour, pour un chercheur, accepter de mener des travaux de thèse classifiés (impliquant de ne pas publier) est un risque pour une future carrière universitaire.

L'industrie comprend un peu cette problématique, en particulier *via* le dispositif des thèses CIFRE (Conventions industrielles de formation par la recherche). À l'époque, j'avais proposé de mettre en place un vrai **mécanisme de reconnaissance des études classifiées** évaluées *in fine* par des ingénieurs de l'armement, en précisant que tel sujet était classifié mais que l'ANSSI pourrait néanmoins attester de la qualité du travail qui pourrait alors être reconnu comme valant telle publication de bon niveau ou dépôt de brevet ; ce certificat permettrait de dire qu'il s'agit d'un travail académique, scientifique de tout premier plan et donc de valoriser un dossier académique. À l'heure actuelle, ce mécanisme manque alors qu'il pourrait inciter les jeunes à choisir des sujets beaucoup plus intéressants tout en renonçant à publier.

Aux États-Unis d'Amérique, la politique de recrutement est complètement différente. La *NSA* fait passer une thèse en interne, ce qui est très pragmatique. Dans une conférence de *hacking*, les personnes appartenant à la *NSA* n'ont pas peur de porter un *badge*, de même que celles du *NCIS,* du *FBI* car l'esprit patriotique a une signification aux États-Unis. De la même manière, les personnes passées par la *NSA* ne craindront pas de le faire apparaître dans leur *curriculum vitae*.

En 2003, j'étais militaire et m'occupais de conférences consacrées à la sécurité, dont une sur les techniques de désassemblage, c'est-à-dire sur la manière de pénétrer les secrets d'un système informatique ou de programmes et j'avais repéré un jeune tout à fait brillant mais ne possédant « qu'un BTS ». Il était donc souhaitable que ce jeune demeure sous la tutelle de l'État, y fasse carrière, mais le niveau de salaire ridicule proposé – sur la base de son diplôme officiel et non de son potentiel – fait qu'il a été engagé par une société américaine et que, maintenant, il est dans une société russe. S'il avait été possible de lui procurer un salaire décent, il serait resté au sein de l'administration française. Des jeunes brillants comme lui existent en grand nombre dans notre pays.

Autre exemple, j'avais trois jeunes étudiants dans mon laboratoire qui ont mené, sous ma direction, une recherche dans un domaine de sécurité très pointu. Ce travail a rendu un grand service au Secrétariat général du Gouvernement (SGG) à propos de choix technologiques importants. Il était donc normal de récompenser ces étudiants par un moyen quelconque, comme une décoration. On pourrait imaginer une décoration spécifique pour cette catégorie de chercheurs ou, à tout le moins, de leur adresser des lettres de félicitations adaptées auxquelles ils seraient très sensibles. Tous les jeunes ne recherchent pas forcément la richesse mais une reconnaissance juste et méritée. Il faut restaurer le goût et la fierté de servir l'État chez les jeunes et ce, sans distinction de critères.

COMPTE RENDU DE L'AUDITION PUBLIQUE DU 16 AVRIL 2014 : ÉDUCATION AU NUMÉRIQUE

SOMMAIRE

INTRODUCTION

M. Bruno Sido, sénateur, président de l'OPECST

Mme Anne-Yvonne Le Dain, députée, vice-présidente de l'OPECST

Tables rondes animées par M. Daniel Kofman, professeur à Telecom ParisTech, directeur du LINCS, membre du Conseil scientifique de l'OPECST

Première table ronde : L'éducation au numérique en milieu scolaire

Mme Catherine Becchetti-Bizot, inspecteur général de l'éducation nationale, directrice du projet stratégie numérique, Ministère de l'éducation nationale, de l'enseignement supérieur et de la recherche

M. Pierre Léna, professeur émérite, membre de l'Académie des sciences, président et cofondateur de la Fondation de coopération scientifique pour l'éducation à la science « *La main à la pâte* »

Mme Sophie Pène, professeur en sciences de l'information et de la communication, Université Paris Descartes, membre du Conseil national du numérique

M. Pierre Ricono, chef du département Campus technologique, direction des éditions et du transmédia, Universcience

DÉBAT

Deuxième table ronde : L'éducation au numérique et à sa sécurité dans l'enseignement supérieur et dans la vie professionnelle

M. Jean-Marie Chesneaux, vice-président de la Conférence des directeurs des écoles françaises d'ingénieurs (CDEFI) et directeur de Polytech'Paris-UPMC

M. Gilles Dowek, directeur de recherche à l'Institut national de recherche en informatique et en automatique (INRIA)

M. Philippe Marquet, vice-président de la Société informatique de France (SIF)

M. François Germinet, président de l'Université de Cergy-Pontoise, président du comité numérique à la Conférence des présidents d'université (CPU)

DÉBAT

Troisième table ronde : Regards croisés sur d'autres approches du numérique

M. Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)

M. Éric Delbecque, chef du département de sécurité économique, Institut national des hautes études de la sécurité et de la justice (INHESJ)

M. Gilles Dowek, responsable du secrétariat du groupe de travail sur le rapport de l'Académie des sciences « *L'enseignement de l'informatique en France – Il est urgent de ne plus attendre* »

DÉBAT

Introduction

M. Bruno Sido, sénateur, président de l'OPECST. – Avant de débuter cette audition, je voudrais plus particulièrement saluer toutes les personnalités qui ont accepté de participer à cette audition publique ainsi que les journalistes présents.

Dans le cadre d'une étude de faisabilité sur le risque numérique, permettez-moi de vous accueillir au Palais de Luxembourg, salle Médicis, pour un échange de vues en forme de table ronde. Mme Anne-Yvonne Le Dain, députée et vice-présidente de l'Office, est corapporteur de cette étude, ce dont je me félicite.

Ayant déjà réalisé à ce jour près d'une quarantaine d'auditions, il nous est apparu que la question de l'éducation au numérique était au cœur du risque numérique et de la sécurité des réseaux. C'est pourquoi nous avons sollicité chacun d'entre vous afin d'avoir un échange approfondi sur ce que pourrait être l'éducation au numérique, depuis la maternelle jusqu'à la maison de retraite. Le numérique a envahi nos vies à une vitesse sans cesse accélérée et il serait difficile, voire impossible, de nous en passer si jamais nous en avions le désir. Cependant, souvent, notre apprentissage des outils numériques s'est effectué « sur le tas » – si vous me passez l'expression – alors que, compte tenu de la technicité des nouveaux outils à notre disposition, il serait préférable d'en apprivoiser les possibilités à partir de l'acquisition d'une vraie culture numérique, complétée par l'apprentissage des outils numériques à maintenir au service de l'homme.

Mais je vais me garder d'anticiper davantage sur le contenu de nos débats.

Les échanges de cette matinée se dérouleront en trois parties, entrecoupées de trois débats. Pour les animer, j'ai fait appel à un membre du Conseil scientifique de l'Office, M. Daniel Kofman, qui est d'abord un spécialiste du numérique. En effet, parmi ses nombreux titres et qualités, il est professeur à *Telecom ParisTech*, directeur du *LINCS*, centre de recherche regroupant des universitaires et des industriels sur les technologies de l'information et de la communication. Il a mené des travaux de recherche dans le domaine des réseaux et des services numériques du futur, publié des ouvrages et de nombreux articles scientifiques. Enfin, il a cofondé deux sociétés dans le domaine des technologies, des télécommunications et de l'information. Je le remercie d'avoir accepté ce rôle difficile.

Sans plus attendre, je passe la parole à Mme Anne-Yvonne Le Dain, corapporteur de notre étude sur le risque numérique, qui souhaite également vous adresser quelques mots de bienvenue.

Mme Anne-Yvonne Le Dain, députée, vice-présidente de l'OPECST. – Mesdames et Messieurs, merci de votre présence et de nous donner de votre temps, richesse essentielle pour chacun d'entre nous. Cette table ronde sur l'éducation numérique part du principe que le monde s'accélère. Aujourd'hui, le temps devient une constante instantanée. Nous ne supportons plus rien qui ne soit fait à la seconde, depuis que les *smartphones* nous mettent en connexion avec le monde entier. Les enfants possèdent des *smartphones*, ils communiquent de manière extrêmement rapide, ont inventé leur propre langage, une sorte d'alphabet phonétique très vivant, et sans interférences avec le monde des adultes, qui représente davantage celui de l'action que de la raison. Le temps de l'adulte est à la fois très rapide et très lent, à l'image de ce monde qui change.

Le numérique a bouleversé le monde, ce qu'ont pressenti les Américains depuis une vingtaine d'années alors que les débats actuels, au niveau européen, sont lents et difficiles. Une décision vient toutefois d'être prise dans ce contexte concernant la protection des données personnelles, mais cela représente le fruit d'une maturation de deux années. Deux commissaires européens sont impliqués et l'affaire Snowden a, tout à coup, accéléré le dispositif, occasionnant une inquiétude brutale quant à la protection des données personnelles. En effet, il est apparu que nous avons tous, collectivement et médiatiquement, réalisé que nos données étaient collectées, séquencées, découpées, exploitées et redistribuées dans des canaux filaires et virtuels. Ce monde de données fabrique une nouvelle économie, qui constitue en elle-même un risque.

Bien évidemment, nous sentons que le monde entier a changé et que la question de l'éducation numérique est fondamentale. Il faut s'en saisir immédiatement, d'autant que les enfants ont des appareils numériques dès la poussette grâce à *Fisher Price* : je le dis sous forme de boutade, mais c'est un fait.

La question qui se pose au législateur est d'interdire ou de permettre. Par ailleurs, le numérique, souvent vécu comme un risque, peut également constituer une opportunité.

Que devons-nous, que pouvons-nous faire dans un monde qui change et au premier chef par rapport à nos enfants qui utilisent le numérique intuitivement et sans connaissance ni mesure ? Dans ce monde, en matière d'éducation au numérique, la responsabilité du législateur est d'autoriser dans certains cas, d'interdire dans d'autres. En cas d'autorisation, il est nécessaire de déterminer comment instrumenter, à partir de quel âge, dans quels moments et pour quel usage.

Tables rondes animées par M. Daniel Kofman, professeur à Telecom ParisTech, directeur du LINCS, membre du conseil scientifique de l'OPECST

Première table ronde :

L'éducation au numérique en milieu scolaire

M. Daniel Kofman. – Monsieur le président, madame la vice-présidente, mesdames et messieurs, bonjour.

Il fut un temps où l'écriture était une technologie innovante. Aujourd'hui, elle est immergée dans nos vies et nous savons à quel point elle a révolutionné notre civilisation.

De même, le numérique est immergé dans la vie des citoyens et des entreprises. Il s'agit d'une technologie souvent imperceptible, mais qui, d'ores et déjà, a induit des bouleversements, tandis que d'autres sont à venir.

On parle de quatrième révolution industrielle, alors que des évolutions profondes sont en marche.

Le numérique apporte de nouveaux concepts, mais également de nouvelles formes de pensée. De même que l'écriture a changé le mode de raisonnement, le numérique induit de nouvelles formes de création. La France et l'Europe doivent conserver un rôle de premier plan en la matière et je suis convaincu de la nécessité d'un besoin de formation accru : formation aux usages, aux risques, et surtout formation des acteurs qui créeront le monde de demain grâce à ces nouvelles technologies.

La première table ronde sur l'éducation numérique en milieu scolaire nous permettra d'aller bien au-delà de la notion de programmation, terme extrêmement réducteur en ce qui concerne l'éducation au numérique.

M. Bruno Sido. – La première table ronde réunira Mme Catherine Becchetti-Bizot, inspectrice générale de l'éducation nationale, directrice du projet stratégie numérique au ministère de l'enseignement supérieur et de la recherche ; M. Pierre Léna, professeur émérite, membre de l'Académie des sciences, président et cofondateur de la Fondation de coopération scientifique pour l'éducation à la science « *La main à la pâte* » ; Mme Sophie Pène, professeur en sciences de l'information et de la communication à l'Université Paris Descartes, membre du Conseil national du numérique ; M. Pierre Ricono, chef du département Campus technologique, direction des éditions et du transmédia d'Universcience.

Mme Catherine Becchetti-Bizot, inspecteur général de l'éducation nationale, directrice du projet stratégie numérique, ministère de l'éducation nationale, de l'enseignement supérieur et de la recherche. – Je vous remercie, monsieur le sénateur et madame la députée, de m'avoir

invitée à participer à cette table ronde, qui se situe au cœur de mes préoccupations. J'ai bien compris que vous souhaitiez avoir mon point de vue sur la nécessité d'introduire à l'école ce que vous dénommez la « *culture du numérique* » et non, je le note, « *l'éducation au numérique* », ou « *l'enseignement du numérique* ». Il s'agit d'un choix tout à fait intéressant, sur lequel je reviendrai au cours de ma présentation.

Cette nécessité de former de jeunes utilisateurs responsables et conscients dans l'usage des réseaux connectés, sera exposée au travers de mon point de vue – avec toutes les réserves que cela suppose – et non celui, officiel, du ministère de l'éducation nationale. Je le précise, même si bien sûr, dans mes fonctions actuelles, la question des réseaux et de la protection des données est centrale et si je suis amenée à contribuer à la réflexion générale et à la mise en place de stratégies dans le cadre de la loi de refondation de l'école de juillet 2013.

Cette loi de 2013 met en avant les responsabilités de l'école face au développement rapide des usages du numérique en classe et fait obligation de repenser en conséquence les programmes d'enseignement, les méthodes pédagogiques, les modalités d'apprentissage des élèves, les modes d'évaluation et la formation des enseignants qui en découle. Il s'agit d'une mission très importante de refonte et de redéfinition confiée au Conseil supérieur des programmes (CSP), dont il ne m'appartient pas de dire ce qui émergera des travaux, auxquels participent des parlementaires. Ce conseil doit travailler en toute indépendance, tout en s'appuyant sur des consultations et des expertises.

Toutefois, il est important de souligner que le ministre a clairement mandaté, dans sa lettre de mission, M. Alain Boissinot, président du Conseil supérieur des programmes, pour intégrer les transformations nécessaires induites par l'introduction des outils numériques à l'école, réfléchir aux nouvelles compétences et connaissances à faire acquérir aux élèves pour qu'ils ne soient pas de simples consommateurs, mais, d'une part, des personnes conscientes des contraintes éthiques, juridiques et sociales dans lesquelles s'inscrit l'utilisation du numérique et d'Internet, et, d'autre part, des individus autonomes dans l'utilisation de ces outils, c'est-à-dire maîtres des nouveaux langages, producteurs eux-mêmes et créateurs et *designers* de leur savoir.

Dans ce nouveau contexte, le CSP transmettra des propositions de programmes. Je souhaite toutefois rappeler que, d'ores et déjà, le ministère de l'éducation nationale a beaucoup avancé, ces derniers temps, dans la **prise en compte du numérique comme objet d'enseignement et pas simplement comme un outil au service de pédagogies plus traditionnelles** et sans doute moins adaptées aux attentes et à l'environnement culturel des jeunes d'aujourd'hui, tels que vous les avez décrits.

M. Vincent Peillon a fait inscrire, dans la loi du 8 juillet 2013 de refondation de l'école, la **création d'un service public du numérique**

éducatif, de même que l'**obligation d'une éducation aux médias et à l'information** (article 4) au niveau du collège, éducation qui vise à préparer les élèves à vivre et à travailler en citoyens responsables dans la société de l'information et de la communication. Cette inscription dans la loi constituait une première, symboliquement très forte. L'éducation aux médias et à l'information comporte des éléments de compréhension, à la fois techniques, économiques et sociologiques des médias numériques, et aussi l'approche des processus qui sous-tendent tous ces objets et Internet.

Au ministère, de plus en plus d'acteurs et d'experts s'accordent pour promouvoir une **approche pluridisciplinaire de l'éducation au numérique**. Ils convergent de même sur la recherche de modalités d'enseignement fondées sur la **pédagogie de projet**, sur des **démarches créatives et collaboratives** mettant en activité les élèves avec ces outils.

Pour ma part, mon point de vue est avant tout celui d'une inspectrice générale de lettres, qui s'est toujours intéressée au décryptage des textes, à l'analyse rhétorique, c'est-à-dire à la recherche des intentions et stratégies et de l'écriture masquée qui se cachent sous les formes visibles de textualité. Je me suis également beaucoup intéressée à la relation entre technologie et écriture, c'est-à-dire à la manière dont tout nouveau support technique écrit, depuis la tablette d'argile jusqu'à la tablette tactile, en passant par le rouleau, le codex, le livre imprimé, l'écran d'ordinateur, conditionne nos manières d'écrire, de penser, de comprendre le monde et de vivre en société. C'est pourquoi j'apprécie particulièrement que vous ayez posé la question en termes de culture du numérique et non simplement en termes d'éducation à l'information ou d'enseignement du numérique. En effet, je pense que ce serait mal poser le problème que de le réduire ainsi, et ce changement de terminologie était important.

L'informatique était, à l'origine, une branche des mathématiques qui s'est ensuite autonomisée, constituée en sciences, pour devenir une industrie et qui aujourd'hui, beaucoup plus qu'une technologie, est devenue l'écosystème culturel dans lequel nous vivons. Cette culture impacte très largement tous les secteurs de notre vie quotidienne, notre rapport au savoir, nos relations sociales, nos modes d'échanges et de travail, nos organisations et notre système de représentation.

Par conséquent, **la substitution du terme « numérique » au terme « informatique » reflète bien le passage d'une technologie à une culture**. C'est ce qui s'est passé au moment de l'invention de l'imprimerie.

Aujourd'hui, le numérique constitue « *la nouvelle forme industrielle de l'écriture* », ainsi que l'exprime M. Bernard Stiegler et il est nécessaire de l'introduire à l'école parmi les apprentissages fondamentaux. Il s'agit d'une compétence transversale et du socle commun de compétences et de connaissances. Je sais que M. Alain Boissinot partage cette vision, qui doit traverser toutes les disciplines et relever de la responsabilité de l'ensemble

des enseignants, pas simplement les spécialistes. Les enseignants devront être formés dans la conception et la mise en œuvre de cette responsabilité nouvelle, chacun dans sa discipline, pour introduire cette compréhension du média numérique et de ses usages, dans ses dimensions diverses : sociales, économiques, éthiques, juridiques, et bien sûr techniques… Cette conscience devrait s'accompagner, à mon sens, d'une connaissance des langages permettant d'utiliser les nouveaux instruments de notre culture.

Comme vous le constatez, je prends le parti d'une approche globale et intégrée de la culture numérique, qui me semble bien correspondre aux objectifs de l'école publique et républicaine et qui n'est pas contradictoire avec le fait d'approfondir par ailleurs, dans certaines filières et à certains moments de la scolarité, l'enseignement de l'informatique. C'est d'ailleurs déjà le cas dans l'enseignement général au lycée, puisque nous avons créé, depuis deux ans en Terminale S, un enseignement Informatique et sciences du numérique (ISN). Cet enseignement propose aux élèves, entre autres, une introduction à la science informatique, information numérique, algorithmes, langage et architecture. Il doit être étendu aux autres séries générales (littéraire et économique et sociale), avec les adaptations nécessaires au public des élèves, et les professeurs sont formés dans ce sens.

En deuxième lieu, le brevet informatique et Internet (B2i) est en cours de rénovation, tout d'abord au lycée, puisque ce B2i intègre désormais la culture numérique. Par exemple, le domaine I (« *travailler dans un environnement numérique évolutif* ») est résolument tourné vers la maîtrise des pratiques informatiques, avec les notions de paramétrage. Il permet par exemple d'identifier « *les enjeux associés aux modes de codage et de programmation (diversité de programmations,* open-source*, etc.)* ». En ce qui concerne le B2i Écoles et Collèges, il doit être rénové à son tour pour aller dans le sens du développement de la créativité numérique des élèves. De même, on peut supposer que le Conseil supérieur des programmes fera évoluer l'enseignement de la technologie dans le sens d'une intégration des évolutions de l'informatique et des besoins de la société.

Au-delà de ces enseignements spécifiques, l'ambition de l'école est bien d'assurer son rôle de formation générale de l'être humain et du citoyen, et, en particulier, le développement de son esprit critique. **La réponse de l'école au risque d'un usage dévoyé du numérique est une réponse résolument éducative, et non uniquement sécuritaire**, pour répondre à votre question en introduction, madame la députée. Une telle réponse passe sans doute par l'acquisition de connaissances et de compétences nouvelles, nécessaires à l'indépendance et l'autonomie des usagers.

Le tout va dans le sens d'un rapprochement des disciplines entre elles et vers plus de transversalité dans l'approche pédagogique, plutôt que dans la création d'une nouvelle discipline scolaire. Je rappelle, en effet, que les enfants ont vingt-quatre heures de cours par semaine et il me semble que la création d'une discipline supplémentaire alourdirait l'enseignement.

L'acquisition d'une culture du numérique à l'école ne se fera pas sans une transformation profonde de l'organisation des temps et des espaces scolaires ainsi que des modalités d'enseignement. Elle ne pourra pas non plus intervenir sans l'engagement des élèves dans des projets interdisciplinaires et leur participation à la construction de leur propre savoir. C'est ainsi que j'envisage l'évolution des programmes de l'école. Cette acquisition d'une culture numérique ne pourra pas non plus être envisagée sans un déplacement du rôle du professeur qui doit apprendre aux élèves à structurer le flux d'informations qui circulent et leur faire prendre conscience que la connaissance n'est pas une marchandise ordinaire, vouée à la logique industrielle et commerciale, comme le dit M. Bernard Stiegler. La connaissance doit se construire et se structurer dans une appropriation et un usage bien compris des supports de transmission et de production du savoir.

En conclusion, je retiendrai concrètement trois axes pour l'acquisition de la culture numérique et la protection des élèves de toutes les manipulations :

- apprendre à gérer, traiter, organiser et évaluer les informations qui arrivent en flux permanent ;

- apprendre à produire eux-mêmes de l'information et à la diffuser, en respectant un certain nombre de règles : il s'agit de créer, échanger, participer, designer, collaborer à la construction des savoirs en utilisant les outils technologiques et en gérant leurs profils et données personnelles ;

- comprendre les médias numériques dans leur fonctionnement global pour acquérir la distance critique suffisante : comprendre l'économie des médias, leur organisation, leur architecture, leur stratégie, de même que les processus par lesquels se structurent l'information, les langages et les codes qui sous-tendent, les algorithmes qui la traitent. Il s'agit finalement d'apprendre aux élèves à manipuler eux-mêmes ces langages pour en faire les instruments de leur expression et de leur pensée.

Je me situe finalement dans **une approche humaniste et non seulement techniciste des médias numériques**. Elle me semble possible et plus ambitieuse qu'une simple éducation à l'informatique. Elle nécessite que nous envisagions au premier chef la formation de l'individu, que nous repensions la pédagogie dans le sens du développement de l'enfant et du citoyen.

M. Pierre Léna, professeur émérite, membre de l'Académie des sciences, président et cofondateur de la Fondation de coopération scientifique pour l'éducation à la science « *La main à la pâte* ». – Monsieur le président, madame la vice-présidente, merci infiniment de m'avoir invité ce matin. Je ne suis pas un spécialiste de l'éducation numérique, mais vous m'avez sollicité au titre de l'action conduite par l'Académie des sciences depuis près de vingt ans, « *La main à la pâte* », qui nous a amenés à rencontrer

un certain nombre de problèmes similaires à ceux connus aujourd'hui par l'enseignement du numérique : sans doute peut-on en extrapoler quelques résultats. Vous avez intitulé votre table ronde « *Le risque numérique* ». Il existe effectivement plusieurs catégoriques de risques :

- le risque encouru par les enfants et les adolescents devant les réseaux et les écrans : je ne l'évoquerai pas, puisque l'Académie des sciences a formulé un avis assez considérable il y a un an, « *L'enfant et les écrans* », qui a d'ailleurs connu un écho retentissant dans le public et la presse et qui montre à quel point, dans notre pays, les parents, les éducateurs sociaux, les médecins, les psychologues, sont sensibles à cet aspect du risque ;

- le risque que notre école manque la révolution de l'histoire, que représente le numérique, avec toutes les conséquences que cela implique pour l'avenir professionnel des jeunes et la culture ;

- le risque pour l'économie du pays.

Pendant les dix-huit années passées, « *La main à la pâte* », en lien très étroit avec les ministères mais en se situant à l'extérieur du système éducatif, a entendu transformer l'enseignement des sciences expérimentales au collège et au primaire pour tous les élèves, avec l'objectif de citoyenneté. La pédagogie a été progressive et active dès l'école primaire, avec la nécessité d'accompagner les professeurs, d'autant que beaucoup d'entre eux, à l'école primaire, n'avaient des sciences qu'une vision limitée. Au collège, le cloisonnement disciplinaire déjà souligné par l'Office dans son récent rapport sur la culture scientifique n'était pas non plus idéal. L'objectif de mutualiser et de partager les succès a été suivi par toutes sortes de méthodes. Le parti a également été pris de ne pas se limiter au niveau national et de profiter des liens très étroits des académies des sciences entre elles, pour travailler au plan européen et même international.

Il a été caractéristique d'amener des professeurs à envisager autrement les sciences de la nature et de l'observation. Finalement, le problème est assez semblable pour le numérique car il est nécessaire de convaincre les professeurs, dont les parcours professionnels sont très différents, de regarder autrement ce monde qui surgit.

J'articulerai ma réflexion autour de cinq points : la science informatique ; les technologies de l'information (TIs) ; les champs de créativité pour les élèves ; les manuels numériques et le développement professionnel des enseignants.

À propos de la science informatique, le rapport de l'Académie des sciences sur « *Faut-il enseigner l'informatique* » et dont M. Gilles Dowek a été la cheville ouvrière avec d'autres, est le produit d'un très important travail de l'Académie, dont M. Gilles Dowek vous reparlera tout à l'heure.

Au fond, le rapport est construit sur les quatre idées centrales qui structurent cette science informatique aujourd'hui : algorithmes, machines,

langage et information. Chacune de ces composantes existe depuis des centaines d'années voire davantage, mais c'est leur convergence autour de technologies, langages et algorithmies nouvelles, qui fait la puissance de la science informatique aujourd'hui.

Il est possible – et il s'agit de la thèse du rapport que je reprends ici, tout en fait en consonance avec les propos de Mme Becchetti-Bizot – de **commencer une entrée dans cette science dès l'école primaire**. On y retrouve un certain nombre de compétences et de culture : créer un matériel, modéliser, entrer dans le langage formel, traiter des données, abstraire, rechercher des invariants dans un problème, interagir avec un objet matériel et finalement conduire un projet.

En ce qui concerne les technologies de l'information (TIs), je serai très bref sur cet aspect, sur lequel le ministère de l'éducation nationale a accompli une action importante depuis dix ans, notamment avec le brevet informatique. Ce n'est pas à mes yeux l'aspect le plus important car les jeunes sont en général beaucoup plus rapides et efficaces que nous sur l'utilisation basique de l'outil. De plus, en se limitant à l'utilisation, il est, en outre, certain que nous amputons le contenu même de ce que doit être l'éducation au numérique.

Pour revenir au point précédent, je rapporterai une question sur laquelle nous avons été consultés par le Conseil supérieur des programmes et M. Alain Boissinot : faut-il mettre cet enseignement de la culture numérique dans le socle commun de compétences et de culture. Si oui – ce que nous pensons indispensable – qui peut l'enseigner ? Est-il nécessaire de former des professeurs spécialisés pour une nouvelle discipline informatique, ou bien existe-t-il une alternative ?

Cette dernière reviendrait à considérer que tous les professeurs, quelle que soit leur discipline, deviennent soudain qualifiés sur l'impact de la culture numérique dans la conception même, intellectuelle et abstraite, de leur discipline. Cela peut s'appliquer au français, avec l'utilisateur du correcteur d'orthographe, ou à l'histoire et l'utilisation des bases de données, ou encore la géographie et l'utilisation des systèmes cartographiques de *Google*, ou même la physique, avec la simulation numérique, etc.

Les débats à l'Académie des sciences ont été nombreux et les arguments ont été présentés en faveur de l'un ou l'autre de ces aspects. Personnellement, je pencherais pour la solution de faire percoler l'enseignement du numérique et de l'informatique dans l'ensemble des disciplines, mais son corollaire particulièrement aigu est celui de la formation continue des professeurs. En effet, il ne faut pas sous-estimer le coût que représente une telle formation à grande échelle. Aussi est-il sans doute raisonnable d'**inclure l'informatique dans le socle commun, comme un objectif contraignant à terme**, mais que des étapes soient prévues, à la condition qu'un très important programme de **formation continue des**

professeurs soit lancé. La formation doit être continue car il me paraîtrait déraisonnable de ne former que les jeunes professeurs issus de l'école, en laissant les 800 000 professeurs en fonction hors du champ de la transformation de leur pédagogie.

Au sujet du point essentiel de la créativité des élèves et de la transformation de leur mode d'accès au savoir, il est à noter que **l'enseignement des langues est bouleversé par la traduction automatique de grande qualité** qui émerge depuis quelques années et qui rendra bientôt dérisoire l'exercice de la version ou du thème. Cette nouvelle articulation des outils et des savoirs est une opportunité formidable de créativité, qui ne saurait toutefois se développer sans être guidée par le professeur.

Quant aux manuels numériques, les éditeurs sont les premiers intéressés, étant précisé qu'il existe plusieurs sortes de manuels. Pour moi, un manuel vertueux est celui qui guide l'élève, ou le professeur, de manière précise, dans le cheminement sur Internet. Nous savons tous que pour préparer un sujet, nous pouvons aller puiser dans l'immense réservoir que représente Internet, mais que la manière de le faire et la sélection que nous en retenons, sont en fait extrêmement complexes. En réalité, pour nous guider dans cette complexité, nous avons besoin de tous nos savoirs antérieurs. Le manuel numérique doit aider l'élève comme le professeur dans cette exploration, par une construction en couches, et je crois que nous n'avons aujourd'hui que **très peu d'exemples de bons manuels**.

Enfin, la question du développement professionnel des enseignants est située au cœur du sujet et « *La main à la pâte* » a mesuré la complexité d'accompagner ce développement. Dans la plate-forme Magistère du ministère de l'éducation nationale, nous mettons en place un premier *Massive Open Online Course (MOOC)*, « *Vivre la science en classe* », qui sera destiné à des milliers d'enseignants de l'école primaire et relatif à l'enseignement scientifique. Ce *MOOC* sera disponible dans les neuf Maisons pour la Science au service des professeurs, que j'ai déjà eu l'occasion de présenter à votre Office il y a quelques mois et qui constituent le lieu où faire entrer le maximum de professeurs. Après huit ans d'existence à la fin de l'année 2008, ces Maisons auront touché plus de 60 000 enseignants et nous avons bien l'intention de **faire entrer l'informatique dans l'offre**.

Ce dernier point est absolument central et constitue probablement le seul moyen d'accompagner à des coûts raisonnables le corps professoral des collèges qui est très diffus sur le territoire alors que celui des lycées est relativement concentré dans les villes moyennes et les grandes villes. De ce fait, un grand nombre de ces professeurs de collèges sont très isolés, même s'ils sont bien suivis par leurs inspecteurs pédagogiques régionaux. Pour autant, les contenus demandent sans doute d'autres modalités d'accompagnement, pour lesquelles le monde du numérique offre une chance exceptionnelle.

Mme Sophie Pène, professeur en sciences de l'information et de la communication, Université Paris Descartes, membre du Conseil national du numérique. – J'évoquerai en premier lieu les risques les plus couramment décrits pour les enfants : le risque d'être exposé à des images dégradantes, de manipulation psychique, de spoliation d'identité, les risques concernant les données personnelles ainsi que ceux d'escroquerie qui s'ensuivent, le risque d'addiction… En réalité, les risques concernant les plus petits (de six à douze ans), au moment où ils grandissent combinent l'insécurité informatique, les mauvaises rencontres et les fragilités psychiques. Le pari, qu'il est possible de faire, est que **personne ne peut prémunir les enfants contre ces risques, sinon eux-mêmes**. L'une des premières raisons à l'éducation à la littératie numérique, combinant une littératie informationnelle et une littératie technique, est effectivement d'atteindre l'objectif placé dans le socle : la responsabilité face aux objets informatiques. Cette éducation, non pas défensive, mais visant à faire en sorte que les enfants comprennent que sous le texte, est le code, semble une nécessité.

Néanmoins, je me situerai dans une perspective quelque peu emphatique, pour dire qu'il est malgré tout difficile de prétendre préparer les enfants à leur environnement de travail, puisque celui-ci nous est encore inconnu à l'horizon de dix ans. Nous ne savons donc pas à quoi nous les préparons, mais nous savons qu'il faudra une imagination hors du commun aux générations à venir pour dépasser les risques qu'ils vont affronter : risques énergétiques, économiques, écologiques, démographiques, alimentaires… Il s'agit alors de se demander comment une **culture digitale, informationnelle et informatique précoce**, rendra ces enfants aptes à affronter ces difficultés.

De plus, la puissante économie de services que nous avons bâtie après notre société industrielle, va elle-même subir des chocs très rapides et violents, avec la montée en puissance de l'intelligence artificielle et de la robotique. Nous savons que de nombreux emplois, aujourd'hui présentés comme désirables à nos enfants, vont disparaître. Parmi ceux-ci, les métiers d'intermédiaires sont concernés et on parle non seulement du commerce mais également des avocats, ou des professeurs. Nous savons en tous cas que ces métiers vont se reconfigurer très profondément et qu'il en restera ce que nous pourrons collectivement définir comme leur part créative irréductible. Par exemple, en médecine, si les médecins n'analysent pas ce qui est précieux dans leur rapport singulier au malade, leur métier disparaîtra au service d'une mise en concurrence avec des bases Internet. Il en sera de même pour les professeurs.

Tel est donc le contexte futur, tracé à traits grossiers, mais faisant entrevoir que peut-être seulement 30 % des enfants d'aujourd'hui auront des emplois proches des représentations actuelles du travail. Il leur faudra donc beaucoup de créativité pour vivre dans une économie très différente, où la part du non-marchand sera importante, avec un entreprenariat social hors

des circuits directs de la monnaie. La création de la valeur en dehors de circuits monétaires constituera un enjeu pour eux.

Je me centrerai à présent sur la manifestation qui a eu lieu, il y a une quinzaine de jours, réunissant le CNAM, l'INRIA et *Cap Digital*, dénommée « *Décoder le code* », et qui a réuni un impressionnant écosystème associatif, avec une participation importante de professeurs.

Ce tissu associatif est aux portes de l'école et prend en charge des enfants à partir de cinq ou six ans en développant une **culture de la programmation**. Il leur explique qu'il s'agit de machines et qu'ils doivent apprendre à les faire agir. Le **code** est découvert et traité comme un objet de lecture. Il s'agit également de comprendre et connaître les limites de la **pensée algorithmique** et de prouver que l'**informatique** sert à fabriquer ensemble, que le **droit à l'erreur** existe, que plus on fait d'erreurs et plus on apprend. Ce faisant, on entre dans une culture de la coopération, de la formation de pair à pair, de la contribution et de la transformation constante des objets, mais également de l'interrogation critique et du respect des matériaux. Le tout est fondé sur des techniques très simples, qui permettent de fabriquer en un après-midi des objets connectés dans une ambiance de jeu, où les parents sont présents et apprennent avec les enfants.

Ces pratiques sont issues des cultures de *hackers* informatiques et artistes. Les enfants se forment à une informatique « frugale » qui les rend heureux et leur ouvre les portes d'un monde de « bâtisseurs de possibles ».

Pour être plus précise, j'effectuerai la synthèse du point de vue d'une vingtaine d'intervenants. Cette formation précoce agit sur les modes d'attention, sur la capacité d'autonomie et pourrait donc compenser certaines difficultés rencontrées par l'école, liées à une certaine démotivation. De six à huit ans, les instructeurs stimulent en priorité la logique et cherchent la manifestation immédiate d'une **efficience logique sur des objets visibles**. Sont ainsi construites des expériences de référence et une base conceptuelle.

De huit à dix ans, les enfants travaillent très volontiers sur des projets répétitifs, mais il convient de leur donner des schémas simples car ils ne travaillent pas chez eux.

De onze à quatorze ans, l'engagement est très passionné et peut continuer à la maison sans instructions. Toutefois, la puissance de la vie sociale et des amitiés nécessite de trouver des projets qui combinent les deux.

À partir de la classe de troisième, les enfants sont tout à fait capables de construire des **systèmes intelligents et complexes**, par exemple en domotique.

Le bilan des valeurs attachées à cet enseignement précoce aboutit à divers constats d'apprentissages chez les enfants : le sens de ce que sont les

langages ; la beauté des matériaux et des machines ; le plaisir de faire et de créer ensemble ; l'attraction que représente le fait d'obtenir le résultat d'un travail collectif, qui peut se reconfigurer et s'améliorer sans cesse ; la pédagogie de projet et, enfin, l'immersion des enfants dans des stratégies cognitives de leur époque.

Pour notre culture, on peut dire que les valeurs de créativité, de solidarité et de réflexivité, trouvent là un terreau favorable qui sera ensuite repris par l'école. De même, les ingénieurs et chercheurs qui étaient présents, ont affirmé que cette formation précoce des enfants, donnerait des ingénieurs très différents, c'est-à-dire sensibilisés au code mais également aux arts et à l'humanisme. Dans un monde où la robotique et l'intelligence artificielle prennent une place de plus en plus importante, il est bien évident qu'il s'agit d'un très considérable enjeu sur la façon dont les dispositifs seront conçus, utilisés. En d'autres termes, la part politique d'analyse, dépendra beaucoup des profils et des sensibilités des ingénieurs qui seront formés demain, dont les chercheurs eux-mêmes disent qu'ils sont aujourd'hui trop « monoculture ».

En tout état de cause, l'alliance vertueuse entre les associatifs et les professeurs se créé encore aux portes de l'école et nous en connaissons la raison.

Je terminerai en disant que M. Bastien Guerry a réalisé une carte de France collaborative de toutes les personnes engagées dans ces actions et qui se proposent comme des ressources. Cette informatique transformera non seulement les métiers mais aussi les disciplines et les façons de travailler de la recherche, et nous voyons dès lors l'importance de commencer très tôt.

M. Pierre Ricono, chef du département Campus technologique, à la direction des éditions et du transmédia, au sein d'Universcience. – Bonjour à toutes et à tous. Je représente **Universcience**, entité née de la fusion du Palais de la Découverte et de la Cité des Sciences. C'est Mme Claudie Haigneré, sa présidente qui avait été invitée à évoquer aujourd'hui le sujet de l'éducation au numérique en dehors de l'école, dans les musées. Aujourd'hui, le numérique dans un musée, est omniprésent et se développe le plus à travers les jeux vidéo et la fabrication numérique. Les imprimantes 3D permettent de concevoir et de fabriquer directement un objet, de sorte que nous nous trouvons face à une nouvelle révolution liée au numérique à travers la relocalisation de la production.

En tant qu'institution muséale qui contribue à la diffusion de la culture sciences et techniques, j'évoquerai l'évolution de l'espace multimédia de la Cité des sciences, consacré depuis 2001 aux apprentissages du numérique. Les cinq mille espaces publics numériques ouverts, entre 2000 et 2010, en France avaient justement pour vocation de combler les divers « fossés numériques ». La Délégation aux usages d'Internet (DUI) coordonnait les actions de plusieurs labels (Cyberbase, ECM, EPN, Netpublic…). Avec l'aide de la Caisse des dépôts et des consignations, nous

avons ouvert une Cyberbase au sein de la Cité et contribué à former plus de mille animateurs multimédia. Ces derniers ne sont pas des formateurs ni des enseignants, mais des passeurs destinés à faciliter les apprentissages de base et les nouveaux outils tels que l'ordinateur et maintenant ceux liés à la fabrication numérique.

En 2005, grâce à des financements européens, nous avons transformé l'espace public numérique, labellisé Cyberbase tout en continuant de combler les fossés numériques, dans la mesure où certaines personnes effectuaient encore cinquante ou soixante kilomètres pour venir chez nous apprendre ce qu'est un ordinateur ainsi que les logiciels de base. Notre vocation consiste également de ne pas mettre l'accent sur un logiciel particulier, mais de **populariser à la fois l'informatique propriétaire et l'informatique libre.**

Depuis 2005, la Cyberbase est devenue un carrefour numérique, c'est- à-dire un lieu dans lequel les artistes et les créateurs ont la possibilité d'exposer leurs œuvres. De même, nous sommes passés d'activités permettant la réduction des fossés numériques, à celles favorisant la création de sites *web,* de *blogs* ainsi que d'un certain nombre de projets collaboratifs et participatifs.

Depuis 2013, avec l'irruption de la fabrication numérique, principalement grâce au *MIT* qui a réfléchi au concept de *Fab Lab,* nous mettons à disposition de nos visiteurs des machines telles qu'imprimantes 3D, découpeuses lasers, qui leurs permettent désormais de répondre à leurs besoins quotidiens de réparation ou de prototypage d'objet. Par exemple, si la poignée de mon réfrigérateur est défectueuse, plutôt que de racheter un autre appareil complet, je dessine moi-même la poignée exactement adaptée et je la fabrique grâce à l'imprimante 3D dans un *Fab Lab*.

En matière de jeux vidéo, nous avons organisé l'an dernier la première convention *MineCraft* - sorte de jeu de *Lego* - dans laquelle les joueurs peuvent participer, seuls ou en réseau à la création d'une ville à partir de rien. La démarche est itérative et intéressante. De plus en plus, il est constaté que ces outils entraînent un copartage, qui va dans les deux sens. Les jeunes utilisateurs ont des habiletés que les plus anciens n'ont pas, ce qui créé de la cogénération de contenu à partir de besoins propres, et les rôles se mélangent finalement davantage.

Trois expériences conduites cette année illustrent ces nouvelles tendances :

- le projet *One Laptop Per Child* : **des ordinateurs très bon marché sont démontés pour que les utilisateurs en comprennent les principaux constituants.** Le but est de former des utilisateurs responsables et parties prenantes dans les choix de nos sociétés. Les personnes de cette association en partenariat avec nous montrent comment, avec des ordinateurs très

basiques et une informatique libre, se créent de nouvelles formes d'échanges entre enfants et parents.

- Beta testeurs de jeux vidéo à seize ans : **il s'agit, pour les enfants, de donner leur avis à toutes les étapes du *process* de création d'un jeu vidéo, dès la phase de conception.** Des doctorants du CNAM travaillent actuellement à un nouveau type de jeu vidéo, et, pour notre part, nous impliquons nos visiteurs comme Beta testeurs et ceux-ci sont réinvités un mois plus tard pour voir si leur avis a été pris en compte. Cette démarche d'innovation, ouverte et remontante constitue une occasion d'aider la recherche et de rendre les futurs acteurs davantage contributeurs et de prendre en compte leurs propositions et leur actions.

- *Loungeshare* : des matériaux recyclés sont mis à disposition d'adolescents et de jeunes adultes, réunis pendant quarante-huit heures par équipes de trois avec la présence d'un *designer*, pour **réaliser du « sur cyclage », c'est-à-dire un objet-mobilier ayant des qualités et un contenu beaucoup plus riche que le matériau de départ.** Il s'agit par conséquent de nouvelles formes de pratiques, dénommées des *hackathons,* c'est-à-dire des marathons se déroulant tout au long d'une fin de semaine dans le but de bricoler, détourner des usages et fabriquer ensemble un objet.

Dans le même esprit, a été organisé, la semaine dernière, le *Space apps Challenge,* à l'origine créé par la *NASA.* Cette manifestation consiste à **réunir des jeunes pour développer un objet, une application, un service, etc., qui sera primé par la *NASA*, en raison de son apport estimé à la conquête spatiale.** Ces jeunes sont donc mis en position d'être chercheurs et contributeurs. Une vingtaine de propositions ont été réalisées et le premier prix a été attribué à une serre flexible pour la planète Mars.

Pour conclure, il convient de souligner que **l'importance de l'éducation numérique dépasse le strict cadre de la technique,** pour intégrer les nouvelles formes d'apprentissage, de contributions participatives issues de l'univers des jeux vidéo et des pratiques d'intelligence collective qui les entourent. Ceux-ci servent en effet réellement de moteurs dans les acquisitions de base, dans toutes les disciplines.

Éduquer, c'est quitter la position frontale de l'enseignant comme source unique de savoir ou de savoir-faire, avec l'idée de cogénération de contenus, tout en laissant sous-jacente la notion d'erreur constructive. Il est souhaitable que, à l'avenir, chaque visiteur d'une institution muséale puisse un jour apporter sa touche personnelle et laisser une trace de son passage lors de sa venue.

M. Daniel Kofman. – Pour ouvrir le débat, j'ai retenu quatre points.

En premier lieu, **le monde numérique requiert une approche holistique, dans une logique pluridisciplinaire** recouvrant les sciences, les technologies, mais également les aspects juridiques, sociétaux, éthiques et économiques. Il faut comprendre le fonctionnement des acteurs, pour mieux

envisager les risques. Dans ce contexte, la première question est de savoir s'il existe en France un risque d'illettrisme numérique. Quelles sont les urgences, au regard de l'ensemble de ce qui a été exposé ? Nous avons également évoqué l'éducation, *versus* l'approche sécuritaire, et je suis personnellement tout à fait favorable à la première optique.

En deuxième lieu, j'ai retenu le point lié à la connaissance et au **développement de l'esprit critique**. Trop d'informations risque d'amoindrir la connaissance et d'affaiblir la capacité créative, et le risque est bien réel, d'une part, pour parvenir à distinguer la qualité et, d'autre part, à repérer les mécanismes qui permettent de transformer cette information en connaissance. Parfois, cette transformation s'effectue de manière informatisée – on parle alors d'algorithmes et de *big data* – mais nous en ignorons les objectifs réels.

Le troisième point tient aux méthodes. Il est nécessaire d'adopter des **méthodes intégrées et nouvelles, en mode projet**, telles que les *Fab Labs* ou les *Living Labs*, c'est-à-dire des lieux où les usagers partagent avec les créateurs des nouvelles technologies et conçoivent ensemble des usages futurs.

Se pose donc la question des **programmes**, ce qui requiert une conception transversale pour acquérir une vision d'ensemble.

Le dernier point à retenir est celui de la **formation continue des enseignants** et des mesures à prendre en la matière pour disposer des forces vives nécessaires.

Je pose donc à nouveau ma première question : existe-t-il un risque réel d'illettrisme numérique en France ? Dans l'affirmative, quelles seraient les actions à mettre en place ?

M. Gérard Roucairol, président de l'Académie des technologies. – Je n'interviendrai pas exactement en réponse à la question qui vient d'être posée, mais souhaite revenir sur quelques aspects des interventions.

Tout d'abord, j'ai été surpris par les propos de Mme Catherine Becchetti-Bizot qui a qualifié l'informatique de branche des mathématiques, ce qui est historiquement faux.

De plus, vous avez affirmé que, depuis que l'informatique était passée d'une technologie à une culture, il était utile de l'enseigner. Par conséquent, il semblerait plus judicieux de démissionner de mon siège de président de l'Académie des technologies, pour me faire embaucher à l'Académie des arts et lettres. Je suis désolé de vous le dire directement, madame, mais en votre qualité d'inspecteur général de l'éducation nationale vous pourriez être responsable de la perte actuelle de milliers d'emplois : ce n'est en effet pas la culture qui crée l'emploi, même si elle est indispensable, mais la technologie. Je le dis fortement, en tant que représentant du secteur industriel, absent de vos débats.

En troisième lieu, je souhaite insister sur le caractère très exagéré des effets de peur. Les peurs du XVIIIe siècle n'étaient pas très éloignées de celles qui sont décrites actuellement et il convient, au contraire, d'éduquer pour apprendre à les maîtriser. En tant qu'industriel et universitaire, j'ai accompli quarante années de carrière dans le numérique, ce qui me donne quelque légitimité pour m'exprimer. Historiquement, **le numérique est l'alliance entre l'informatique et les télécoms**. Finalement, il est important de définir les finalités de ces technologies et de les envisager de façon à élaborer un enseignement qui apportera du sens, de la maîtrise et de la compétence professionnelle ultérieure.

Dans une première phase de ces techniques, le travail humain a été automatisé, ce qui a changé la nature de ce travail. Nous savons, depuis l'invention du métier à tisser, que les révolutions industrielles tuent d'abord l'emploi, avant d'en recréer des années plus tard, et que, globalement, sur une centaine d'années, des emplois sont créés.

Le rôle essentiel du numérique actuellement est un rôle d'intégration des systèmes, surtout compte tenu du vieillissement de la population. Ce point est fondamental et conditionne toute l'évolution de la société future. La question est d'ailleurs similaire en matière de transports et d'énergie.

Par ailleurs, si certains ont évoqué les matières à enseigner, il semble que **la notion de modélisation de l'environnement par les données numériques** était absente des présentations alors qu'elle est fondamentale. La modélisation est également celle du système et il est très important d'introduire cette notion. De même, la culture du *hardware* est tout à fait essentielle et les acquis antérieurs vont donc s'avérer obsolètes dans les années à venir. Par conséquent, la culture à acquérir est celle de l'innovation, en ne figeant pas l'enseignement mais en donnant les capacités aux formateurs et aux élèves de comprendre les évolutions. Il est donc nécessaire d'élaborer des manuels adéquats, car, dans dix ans, l'informatique sera totalement différente de celle qui existe actuellement car la loi de Moore ne se vérifiera plus et les modèles de calcul seront totalement autres.

M. Daniel Kofman. – Nous sommes dans une table ronde sur l'enseignement en milieu scolaire, et non pas en milieu industriel, bien que je partage totalement certains de vos propos. Nous y reviendrons certainement.

Mme Catherine Becchetti-Bizot. – En réalité, je partage beaucoup de choses qui viennent d'être dites, mais suis quelque peu surprise par l'agressivité avec laquelle vous les avez exposées, d'autant que je ne les pense pas contradictoires avec mes propos. À l'école, il y a des réalités. On peut être expert d'une science, ce qui n'est pas mon cas en matière informatique, sans pour autant être spécialiste de l'éducation ou des besoins du système. Je n'ai pas la prétention de dire comment enseigner en informatique mais je pense être relativement bien placée pour savoir où en sont les apprentissages fondamentaux, ainsi que l'urgence en matière

d'acquisition de connaissances. Il faut compter sur deux choses : la capacité du système scolaire à avoir une vision globale et la liberté pédagogique des enseignants. Ceux-ci peuvent développer des méthodes et des pratiques, en continuité avec le périscolaire. Il n'y a aucune opposition entre l'école-sanctuaire et l'extérieur. Les pédagogies peuvent par conséquent parfaitement être actives et prolongées sous forme d'ateliers et d'expériences. Dans le numérique, je suis particulièrement intéressée par la possibilité de création et d'inventivité. **L'informatique c'est une science, le numérique c'est une culture au-delà de l'enseignement d'une science**, c'est-à-dire une façon de travailler et de produire du savoir, une évolution dans les habitudes, etc.

Mme Anne-Yvonne Le Dain. – J'ai été surprise de la tonalité générale de la conversation, qui a produit des propos théoriques, et des propos universalistes. Or, la vraie question est de savoir que faire du présent. L'éducation nationale fonctionne souvent par expérimentations qui n'aboutissent pas car le système ne les prend pas en charge. Mon souci est de déterminer que faire devant l'élève. « *La main à la pâte* » est restée très périphérique, mais ne s'est pas généralisée, ce qui est regrettable. Cette idée que l'appareil éducatif a du mal à s'approprier les dispositifs et les généraliser, est préoccupante.

En réalité, il semble que le réel problème soit une logique de classes, consistant à passer d'abord par le baccalauréat général pour faire évoluer les enseignements. Dans le Languedoc-Roussillon, nous distribuons des ordinateurs à toutes les classes de seconde, pour un coût de quinze millions d'euros par an. Il s'avère que les plus grands succès sont rencontrés avec les enseignants de lycées techniques professionnels, en particulier dans les zones difficiles. Ceux-ci ont en effet parfaitement intégré les approches pédagogiques nouvelles, ainsi que l'intérêt qu'elles représentent. La pression provient plutôt des parties les plus aisées de la population, qui affirment posséder déjà un ordinateur à la maison mais ne s'en servent pas comme outil pédagogique.

De ce fait, d'où provient le problème ? Émane-t-il de l'institution, qui suppose qu'il convient d'abord de passer par les classes les plus aisées pour que les enseignements fonctionnent ? L'évolution ne se fera pas uniquement sur la base du volontariat de ceux qui sont chargés d'appliquer ces réformes. Pour moi, c'est un réel souci car il existe encore des professeurs qui considèrent qu'il ne sert à rien d'acheter des ordinateurs aux enfants, parce qu'ils en ont déjà chez eux.

Mme Catherine Becchetti-Bizot. – Vous avez entièrement raison et nous avons conscience de ces difficultés. Le fait d'inscrire dans la loi ces dispositifs en fait une obligation. La culture évolue lentement et il ne suffit pas de décréter pour légitimer. En tout état de cause, un grand nombre d'enseignements s'effectuent avec l'informatique et le numérique, même en lettres. L'approche de l'erreur et de la dédramatisation est également

importante. Toutes ces choses existent déjà, mais ne peuvent réussir en peu de temps.

M. Gilles Dowek. – Je souhaite rebondir sur un propos de M. Gérard Roucairol, que je partage tout à fait, concernant l'opposition relativement récente entre la culture et la technologie, valorisant les aspects culturels et dévalorisant les aspects techniques. Vous avez employé, tout à l'heure, le mot « *technicisme* » et l'ajout du suffixe « *isme* » est en soi péjoratif. Cette opposition se comprend assez facilement puisque la culture est la maîtrise de la langue et que la technologie est la maîtrise des machines. Je répète que cette distinction est récente puisque, en latin, le mot *ars* désigne aussi bien les beaux-arts que les arts et métiers. C'est seulement à partir du XIX^e^ siècle que les deux ont été séparés, en considérant que les beaux-arts étaient réservés aux bons élèves et que les arts et métiers étaient l'apanage des mauvais.

Comme l'a rappelé M. Pierre Léna, la naissance de l'informatique procède de la rencontre de la notion de machine et de celle de langage. Auparavant, les machines à vapeur pouvaient fonctionner sans maîtriser un langage, tandis que les langues étaient pratiquées sans utiliser les machines. **Soudainement, les machines et les langages se sont rejoints, pour donner naissance à l'informatique. Le point d'entrée dans la pensée spécifique informatique est précisément d'abandonner cette opposition entre culture et machine, puisqu'il s'agit justement du même objet.** Par parenthèse, à cet égard, la lecture de Michel Serres serait sans doute plus utile que celle de Bernard Stiegler. En définitive, si l'on continue à penser le monde dans lequel on vit en opposant culture et technique, on risque purement et simplement de reproduire le paradigme de l'ancien monde.

Mme Catherine Becchetti-Bizot. – Non seulement je ne dévalorise pas la technologie, mais je rappelle depuis des années la nécessité du contraire. Le mot « techniciste » n'a rien à voir avec la technologie, mais évoque une entrée par l'outil. En tant qu'humaniste, je rappelle toujours qu'une technologie crée une culture. Je me suis sans doute mal exprimée, mais il s'agit d'un vrai sujet.

M. Gilles Dowek. – Une technologie ne crée pas une culture, mais une technologie est une culture.

M. Daniel Kofman. – Ce débat est certes très important, mais il risque de retarder le déroulement de nos tables rondes. J'ai posé tout à l'heure la question du plan d'action car il existe certaines urgences et il n'y a pas été répondu. J'espère que nous aurons le temps lors de la prochaine table ronde.

M. Pierre Léna. – Vous avez évoqué « *La main à la pâte* », menée pendant dix-huit ans, et qui était pourtant dans la loi et dans les programmes. Or, **en dix-huit ans, nous n'avons pu sensibiliser qu'un tiers des élèves. Il est donc assez scandaleux que deux tiers des élèves sortant**

du primaire n'aient pratiquement jamais rencontré la science. Cependant, enseigner la science est relativement facile par rapport à l'informatique et nous avons, en outre, une longue tradition de grands noms et d'expériences.

Le problème concernant l'informatique est entièrement nouveau, et, à supposer qu'il soit tranché dans le sens de l'interdisciplinarité sans créer de corps spécialisé de professeurs, quelle est l'ampleur de l'action à mener pour obtenir une transformation globale du système par la formation continue ?

M. Pierre Ricono et Mme Sophie Pène ont évoqué la richesse créative des associations et des projets de toutes sortes, mais qui ne sont aucunement à l'échelle du problème posé, qui vise à **transformer 320 000 enseignants de primaire et de 300 000 enseignants de collèges et de lycées en enseignants interdisciplinaires**, alors que parallèlement nous connaissons les réticences des professeurs sur ce point. J'adresse donc ma question à la fois à Mme Catherine Becchetti-Bizot et à la représentation nationale.

Avez-vous réfléchi à cette question en termes de coût et de volumes ? **À l'INRIA, nous n'aurons pas de mal à trouver les experts qui construiront les processus de formation continue ainsi que les outils, mais le coût sera important.**

Deuxième table ronde :
L'éducation au numérique et à sa sécurité dans l'enseignement supérieur et dans la vie professionnelle

M. Jean-Marie Chesneaux, vice-président de la Conférence des directeurs des écoles françaises d'ingénieurs (CDEFI) et directeur de Polytech'Paris – UPMC. – Je me recentrerai sur les problèmes du risque lié au numérique, qui se situe à trois niveaux :

– risque pour chaque citoyen : il convient de **sensibiliser les enfants dès l'école primaire aux ravages potentiels des réseaux sociaux**, en l'introduisant même éventuellement dans le B2i ;

– risque pour la France du fait de **piratages dans les entreprises** et du **comportement des cadres** : les écoles d'ingénieurs sont concernées et **il est important que tous les étudiants ingénieurs soient formés au risque numérique**, dans tous les grades master en sciences et technologies. Cela est d'ailleurs possible grâce au Certificat informatique et Internet, niveau 2, des métiers de l'ingénieur (C2i2mi) qui prévoit une rubrique entièrement consacrée à la maîtrise de l'informatique et des systèmes d'information. Ce certificat n'est aujourd'hui pas obligatoire, mais si cette compétence était diffusée chez tous les grades *Master* en sciences et technologies, la lutte contre le piratage industriel serait sans doute plus efficace.

– le troisième niveau de risque incite à **former des experts en sécurité informatique**, ce qui relève de l'État.

M. Gilles Dowek, Directeur de recherche à l'INRIA. – C'est la deuxième fois que vous m'invitez pour évoquer les risques informatiques. Cette question est évidemment importante, mais je propose que vous m'invitiez prochainement pour parler également des joies que procure l'informatique et de ses apports dans notre vie quotidienne ainsi que dans notre pensée intellectuelle.

La sécurité informatique constitue un exemple intéressant car elle suppose d'acquérir un grand nombre de connaissances fondamentales en informatique. Par exemple, il faut absolument comprendre la notion de flux d'information et maîtriser les outils logiques de modélisation. De même, une bonne connaissance de l'architecture des machines est nécessaire pour comprendre les attaques potentielles, ainsi que la notion de réseaux, leur structuration et celle de complexité algorithmique.

Dès lors, on s'aperçoit que **la protection des systèmes d'information et des infrastructures françaises contre les attaques malveillantes nécessite une connaissance approfondie des sciences fondamentales de l'informatique par les cadres de l'industrie, or on peut s'interroger pour savoir lesquels d'entre eux seraient effectivement préparés**.

L'analyse des *masters* en informatique à l'université permet de constater que les étudiants ont reçu une préparation efficace dès le niveau licence. En revanche, plus inquiétant est le cas des écoles d'ingénieurs généralistes, qui n'ont aucune connaissance de base telles que décrites, et sont **totalement imperméables aux questions de sécurité** car ils ne comprennent ni l'architecture ni les outils de modélisation. L'illustration du retard pris se traduit par le fait que **l'informatique n'est enseignée en classe préparatoire scientifique que depuis deux ans seulement, à raison de deux heures par semaine, mais sans avoir les professeurs nécessaires**. C'est pourquoi il a été décidé de former des professeurs de mathématiques de classes prépa, mais cette formation ne se déroule que sur trois jours.

Dans beaucoup d'écoles d'ingénieurs classiques, **l'enseignement de l'informatique s'effectue en quarante heures. Il ne s'agit donc pas d'illettrisme mais d'analphabétisme.** Il existe cependant un certain nombre de raisons d'espérer car des réponses parallèles ont souvent été données au cours des siècles aux déficiences de notre système d'enseignement supérieur et secondaire. Aujourd'hui, le même processus est en œuvre en parallèle des écoles ingénieurs, au travers de réponses non institutionnelles.

Le deuxième espoir réside dans l'immigration, par exemple en allant **chercher en Finlande, au Royaume-Uni, en Bavière, ou en Corée du Sud, des ingénieurs pour les faire travailler en France et les former puisque les élèves de ces pays apprennent l'informatique dès leur plus jeune âge**. Ainsi, à l'INRIA, le nombre de doctorants non français a dépassé le nombre de doctorants français. Nous savons donc donner, par l'immigration, une réponse aux défaillances de notre système éducatif.

En second lieu, la question de la formation tout au long de la vie professionnelle, tant en **informatique** qu'en **sécurité informatique**, se pose également. Il ne serait donc pas inutile que tous les ingénieurs suivent une vraie formation en la matière tant qu'ils sont en activité. Nous devrions tenter un nouveau changement de paradigme, qui est le passage du « cinq + deux » au « quatre + un + deux ».

Le « cinq + deux » a consisté, après que les ouvriers eurent travaillé durant les sept jours de la semaine au XIX^{e} siècle, à réduire la semaine à cinq jours de travail et deux jours de repos. Une formation professionnelle de qualité tout au long de la vie demanderait de consacrer un jour de la semaine à la formation, pour quatre jours de travail. À plus court terme, nous devrions commencer à penser une véritable respiration du temps, par exemple à raison d'une demi-journée tous les quinze jours, pour se former de manière régulière.

Cette évolution suppose une réorganisation des entreprises et également des universités. L'enseignement en ligne *(MOOC)* propose déjà une possibilité de se former de manière régulière à son propre rythme. Cependant, les *MOOCs* prévus en formation initiale sont très différents de ceux prévus tout au long de la vie, ces derniers ne supposant pas de

présentiel pour se former. De plus, les études empiriques sur l'enseignement en ligne montrent que ce sont les étudiants les plus autonomes dans leur formation initiale, qui sont les plus à même de bénéficier de l'enseignement en ligne. La concentration nécessaire à l'apprentissage doit donc être acquise dans la formation initiale, que rien ne remplace en informatique.

En définitive, **l'informatique et la culture numérique doivent s'apprendre depuis la première classe de maternelle, en adaptant la pédagogie aux enfants**. Ce sont, en effet les, enseignements précoces qui déterminent l'avenir.

M. Philippe Marquet, vice-président de la Société informatique de France (SIF). – Monsieur le président, madame la vice-présidente, mesdames et messieurs, je traiterai de l'enseignement supérieur en informatique et en sécurité. Aujourd'hui, les filières informatiques de l'enseignement supérieur fonctionnent parfaitement. De nombreux étudiants suivent la formation comportant un aspect fondamental, technologique et évolution des technologies, qui offre de nombreux débouchés dans l'industrie informatique. Il existe donc une formation généraliste en informatique dans l'enseignement supérieur, à l'université ou dans les grandes écoles d'ingénieurs.

En matière de sécurité et de réseaux, certaines spécialités proposées en dernière année de *master* existent, au côté de certaines licences professionnelles.

En fait, **il existe aujourd'hui un petit nombre de personnes formées à l'informatique et seulement quelques spécialistes formés à la sécurité** car cette compétence suppose des connaissances poussées en informatique. En réalité, **la grande majorité du public des universités n'est formée ni à l'informatique ni à la sécurité informatique**.

Dans l'attente de changements majeurs, il serait d'ores et déjà possible d'**ajouter des modules sur la sécurité, à l'intention des informaticiens**. De même, il serait envisageable de **mettre en œuvre une sensibilisation à la sécurité pour tous**, en insistant sur les usages. Par exemple, le fait de s'assurer de la présence d'un « cadenas vert » sur l'*URL* de la page avant de transmettre une information confidentielle, suppose malgré tout de comprendre au minimum le fonctionnement d'une page sécurisée.

La situation actuelle est telle que les étudiants sont analphabètes en informatique à l'entrée à l'université. Si l'on effectue le parallèle avec la science et la biologie, chacun au collège a reçu une formation en biologie et, en termes de fonctionnement de l'appareil digestif, a bénéficié des campagnes de prévention sur l'obésité, de sorte que les élèves s'approprient les recommandations de sécurité alimentaire tenant au fait de manger moins, mieux, de pratiquer une activité physique, etc. Il en est de même pour l'éducation à la pollution et la compréhension de l'effet des particules fines

sur l'appareil respiratoire. La culture générale dans ces domaines permet finalement de ne pas envisager les recommandations comme des messages obscurs, mais, au contraire, de se les approprier car elles sont comprises.

En matière informatique, si l'apprentissage précoce était décidé comme pour les autres disciplines, les informaticiens pourraient réellement être formés à la sécurité. Ils bénéficieraient ainsi de la connaissance des aspects théoriques mais également d'une compréhension fine des réseaux et des systèmes, d'une maîtrise technique, et utiliseraient finalement ces compétences dans leur vie professionnelle au quotidien.

De même, dans l'enseignement supérieur, en fonction des débouchés et de la discipline, il est envisageable d'instaurer une **formation à la sécurité informatique à partir de chacun des enseignements disciplinaires de base**. Par exemple, pour les métiers du droit et de la justice, il serait utile de prévoir des formations sur la sécurité numérique et les nouveaux usages. Les étudiants en philosophie pourraient être formés aux aspects sécuritaires liés à l'éthique numérique. Les étudiants en médecine, en commerce, en aéronautique, pourraient également recevoir un enseignement spécifique à leur discipline et orienté vers la sécurité informatique.

L'enseignement supérieur est également le lieu où sont formés les professeurs et les enseignants, ce qui implique deux conséquences. En premier lieu, l'aspect pédagogique suppose d'acquérir une culture générale numérique et informatique, pour que les enseignants deviennent des acteurs en la matière.

En second lieu, les futurs enseignants seront les premiers transmetteurs de la culture numérique et devront, à ce titre, en avoir compris les sous-jacents, tout en ayant acquis du recul sur les recommandations de sécurité transmises à leurs élèves.

Enfin, en matière de formation professionnelle, **chaque profession devra être formée aux enjeux numériques et de sécurité spécialement liés à son environnement**. Par exemple, un gendarme pourra désormais avoir à traiter des situations liées aux *bit coins,* supposant des notions de cryptographie. Après-demain, les technologies seront, de la même manière, basées sur des fondamentaux de l'informatique.

Pour chacun des citoyens, le bon sens allié à une connaissance de base de l'informatique, pourrait éviter d'être la cible de tromperies. Pour tous, des **campagnes de prévention grand public**, à partir d'une nouvelle culture numérique et de nouveaux usages, devraient donc être mises en œuvre et leur appropriation serait facilitée si les connaissances de base étaient acquises.

En conclusion, **une réelle éducation à la sécurité numérique, demain, passe par une éducation au numérique et à l'informatique dans le secondaire aujourd'hui**.

M. François Germinet, président de l'Université de Cergy-Pontoise, président du comité numérique à la Conférence des présidents d'université (CPU). – Mesdames et Messieurs, en ma qualité de président de l'Université de Cergy-Pontoise et également de président du comité numérique de la Conférence des présidents d'université, j'articulerai mon intervention autour de quatre points.

Tout d'abord, la citoyenneté numérique. Il s'agit, pour l'université, d'accueillir des étudiants qui auront été sensibilisés à la citoyenneté numérique au collège et au lycée, qui constituent des lieux d'acquisition des connaissances de base. J'ai, à cet égard, les mêmes préoccupations que celles déjà exprimées par mes collègues. L'émergence du numérique à travers les ordinateurs, les *smartphones* et les réseaux sociaux, constitue un pan entier de notre vie quotidienne ainsi que de celles des élèves, et on peut raisonnablement se demander s'il est judicieux de les laisser dans l'ignorance du monde numérique sur lequel s'appuie le quotidien.

Sur l'identité numérique et la citoyenneté numérique, les prises de conscience semblent plus rapides car les jeunes sont confrontés aux traces qu'ils laissent sur Internet et les réseaux sociaux. Il existe, en effet, une conscience que l'identité numérique se construit et il convient d'y sensibiliser la population dès le plus jeune âge.

L'université peut accompagner ce mouvement, d'autant qu'elle accueille certains étudiants sortant d'un cadre scolaire assez rigide pour commencer à s'ouvrir au monde et à évoluer. L'université et les établissements d'enseignement supérieur ont la responsabilité d'accompagner cet éveil à la citoyenneté, en particulier la citoyenneté numérique. Les étudiants commencent à construire leur future identité professionnelle dès l'université. Dès lors, ils doivent être conscients qu'ils auront leurs premiers contacts sérieux avec l'entreprise, stages et apprentissage, dès l'université.

Les certifications de niveau 1 et 2 font également partie des dispositifs offerts aux étudiants pour obtenir des compétences en termes de numérique.

Deuxième point, la formation. Le phénomène des *MOOCs* n'est pas encore totalement maîtrisé, même s'il existe une intuition sur l'importance qu'ils revêtent. Pour autant, il n'est aujourd'hui pas possible d'imaginer la place qu'ils prendront dans quelques années dans la stratégie de formation des établissements. Le phénomène ne saurait toutefois être passé sous silence, c'est pourquoi les universités et le ministère travaillent au projet France Université Numérique pour porter la question des *MOOCs* sur le devant de la scène.

Il convient toutefois de **ne pas attendre des *MOOCs* une révolution de l'enseignement**, en escomptant qu'ils forment entièrement les ingénieurs et les cadres de demain, ou encore qu'ils éduquent une population entière

dans certains pays ne disposant pas de ressources enseignantes suffisantes. En effet, les *MOOCs* ne sont aujourd'hui pas qualifiants, même s'ils ont vocation à devenir certifiants. Cependant, avant de mettre en place des cours suivis par des centaines de milliers d'étudiants et formant des opérationnels à un métier précis, un long délai sera encore nécessaire.

En revanche, certaines formations alternatives s'inspirent des *MOOCs* et de leur modèle de pédagogie inversée et de production collective de travaux, mais s'effectueront à des échelles plus faibles – une vingtaine ou trentaine d'étudiants –, avec un encadrement plus serré. On parle ainsi de *Small Private Online Courses*, ou cours en ligne, dans lesquels figurent, d'une part, des principes massifs et ouverts à tous, et, d'autre part, des cours en ligne avec un tutorat plus serré, dans lesquels l'accent sera mis sur le caractère professionnel.

Dans les écoles et les universités, l'enseignement à distance est déjà présent, mais reste encore du présentiel enrichi. Dans certains cas, des *Small Private Online Course (SPOCs)* existent en matière de formation initiale et de formation continue et ont tendance à se développer. Il semble que, dans les années à venir, avec le développement des *MOOCs*, nous serons les témoins et les acteurs d'une hybridation de nos formations, avec la coexistence de cours traditionnels dans les salles de classe, sur un modèle descendant et d'unités de cours autonomes traitées à distance. Le tout laisse présager un certain degré de mutualisation des ressources pédagogiques entre établissements et la plus-value de l'enseignant consistera, non à répéter ce que les étudiants peuvent trouver sur le *MOOC* ou *Wikipédia*, mais à posséder la capacité pédagogique d'accompagner le cheminement intellectuel de l'étudiant vers les bons modes de pensée. Un tournant dans le métier des enseignants laisse présager qu'ils délaisseront l'aspect détenteur de savoir, vers l'accompagnement des apprentissages.

Le tout fait partie de la stratégie des établissements et il y aura là un contrat à passer entre les établissements et l'État.

Troisième point, les besoins des entreprises. Il est à noter que l'accompagnement de la formation professionnelle s'effectue de plus en plus en collaboration entre les branches professionnelles, qui font part de leurs besoins, et l'université.

Enfin, pour l'image des universités et le positionnement international, les *MOOCs* peuvent constituer un moyen de se positionner dans la compétition internationale en matière d'enseignement. À cet égard, les pratiques de certaines universités américaines consistent à utiliser les *MOOCs* comme **un moyen de repérer, sur l'ensemble de la planète, les meilleurs étudiants**, en faisant le constat très froid que ceux d'Harvard et du *MIT* ne sont finalement pas les meilleurs. Dès lors, les *MOOCs* deviennent un moyen de repérage des étudiants, qui se voient ensuite offrir des bourses pour venir étudier dans ces universités.

M. Daniel Kofman. – L'un des moyens d'apprentissage est la formation par l'exemple. Je souhaiterais donc avoir votre opinion sur l'idée suivante : il nous manque des acteurs de confiance, nécessaires d'un point de vue technique pour structurer l'architecture numérique, mais également pour donner l'exemple d'utilisation du numérique.

Le deuxième point sur lequel j'aimerais revenir a été évoqué par M. Gérard Roucairol et pose l'informatique comme un élément intégrateur, par exemple en matière de santé, pour mettre en place les applications transversales de demain. Néanmoins, pour y parvenir, il est nécessaire que les divers acteurs (médecins, acteurs de la sécurité, des transports…) travaillent ensemble : comment pourrait-on s'organiser pour réussir cette intégration au niveau de l'enseignement supérieur ?

M. Jean-Marie Chesneaux. – Cette intégration existe déjà. **Dans le domaine de la santé, un grand nombre de formations traitent du numérique appliqué à la santé.** En revanche, il n'est pas certain que ces formations soient suffisantes. En tout état de cause, il existe une réelle conscience que les emplois de demain se situeront dans le numérique.

Je souhaite également revenir sur un aspect non évoqué. *IBM* a fêté les quarante ans du ***Main Frame*, efficace en matière de sécurité alors que le *cloud* est une passoire**. Or, il ne faut jamais oublier que les *hardwares* et les technologies sont également importants en matière de sécurité.

M. François Germinet. – Au sujet des acteurs de confiance, et en particulier dans le nuage numérique, un appel d'offres au niveau du Commissariat général à l'investissement (CGI) a fait émerger deux acteurs. Se pose donc à l'État la question de construire des centres de données totalement publics et maîtrisés, destinés à garantir la sécurité de la donnée publique. Sans doute conviendra-t-il de construire des centres de données par régions, en maillant le territoire national car la construction de salles de serveurs dans tous les établissements est très coûteuse et pose des problèmes de main-d'œuvre qualifiée et de sécurisation des données.

M. Daniel Kofman. – La notion de nuage numérique personnel pourrait apporter quelques solutions.

M. Philippe Marquet. **– Il est nécessaire que chacun comprenne ce que sont le code, le serveur, les réseaux, pour comprendre les enjeux. En effet, l'utilisateur doit bien connaître la destination des données qu'il introduit dans un logiciel, savoir si elles vont rester en France et s'interroger sur le droit applicable.**

M. Daniel Kofman. – Ce sujet est revenu plusieurs fois : pour développer la culture de sécurité numérique, il faut en comprendre les mécanismes et commencer l'éducation dès le plus jeune âge. Lorsqu'on regarde l'international, **les pays les plus avancés ont développé des synergies fortes entre l'enseignement primaire, secondaire et supérieur**.

M. Pierre Léna. – Si on observe aujourd'hui la **totale inconscience avec laquelle chacun d'entre nous pose des données confidentielles sur des réseaux dont nous ne savons rien**, dont l'exploitation est faite aux États-Unis d'Amérique et probablement en Chine demain, peut-on penser que cette éducation de base suffira à compenser les risques de cette dissémination de données, alors que par ailleurs elle nous est éminemment profitable ?

M. Daniel Kofman. – Depuis deux jours, nous savons que *Google* lit nos messageries électroniques.

M. Philippe Marquet. – **Aujourd'hui, chacun voit les caractères très séduisants du service, mais ne voit pas que ses données ont une valeur, qu'elles sont transportées hors de France et sont exploitées.**

M. Jean-Marie Chesneaux. – Le parallèle qui a été effectué avec la prévention contre l'obésité est très pertinent. **Si des actions de prévention et d'éducation au numérique étaient menées dès l'école primaire, de même qu'au collège, âges auxquels les enfants sont particulièrement réceptifs, les succès seraient certains.** En revanche, au lycée, le sujet est plus délicat. J'ai en effet fait partie de la commission qui a réussi à intégrer, de haute lutte, deux heures de l'enseignement de l'informatique en classe préparatoire, et je me demande si cela ne serait pas aussi difficile au lycée.

M. Gilles Dowek. – Les informations traitées par *Twitter* ou *Facebook* sont peu de choses, comparées à celles dont connaissent aujourd'hui les *MOOCs*. En effet, **les *MOOCs* observent des étudiants et recueillent quantité de données les concernant** : leurs modes d'organisation pour travailler, leur sérieux, leur créativité, leur confiance en eux, leur rapidité, etc. La façon de répondre aux questionnaires à choix multiples (QCM), ou le délai pris pour rendre un devoir, sont également très évocateurs de la personnalité de l'étudiant et de son futur mode de travail dans l'entreprise. Or toutes ces informations, dans le *business model* initial du *MOOC*, sont vendues aux chasseurs de tête et sont, en réalité, beaucoup plus importantes pour trouver un emploi que les photos publiées sur *Facebook*.

Aujourd'hui, **certaines personnes s'inscrivent sur les *MOOCs* sous leur vrai nom et donnent une quantité d'informations sans avoir conscience de leur utilisation potentielle**. Lorsque l'INRIA travaillait avec le ministère de l'éducation nationale sur la mise en place de *MOOCs*, le postulat de départ a été de poser que les données appartiendraient aux étudiants, seraient non monnayables et se situeraient sur un nuage numérique en France afin de répartir l'information et d'éviter certaines failles de sécurité.

Cependant, il est vrai que le comportement peut être changé par l'éducation. Pour autant, il ne redeviendra pas celui du monde d'avant. Par exemple, la notion d'intimité au XIX^{e} siècle est totalement différente de celle du XX^{e} siècle et il en sera de même de la notion de vie privée.

Mme Sophie Pène. – Aujourd'hui, nous disposons de peu d'alternatives. **Les outils donnés par les directions des systèmes d'information (DSI) aux universitaires ne sont pas de qualité** car ils ne correspondent pas aux fonctionnalités d'usage et constituent, au mieux, des distributeurs de polycopiés numériques. Il existe donc sans doute un problème de politique industrielle française, qui devra absolument effectuer un sursaut pour remédier aux faibles plages de marchés numériques offertes aux enseignants. En effet, le système est totalement centralisé et le prescripteur n'est aujourd'hui pas le payeur, l'argent se trouvant chez les collectivités locales. En outre, il existe un **blocage complet pour acquérir une réelle culture de l'édition numérique**.

M. Daniel Kofman. – Je me souviens d'une réunion organisée l'an dernier par l'OPECST, au cours de laquelle un participant avait développé l'idée que le service totalement gratuit n'existait pas : **lorsque le service est offert, c'est l'utilisateur qui est le produit. Se pose ainsi la question de la valeur des données personnelles et, au-delà, de l'ensemble des créations personnelles.**

Mme Sophie Pène. – Je pense que la valeur n'est plus dans le document mais dans le service. Le fait que la ressource soit gratuite n'est pas nécessairement gênant.

M. Daniel Kofman. – La création peut être matérielle ou immatérielle et l'éducation devra également transmettre cette notion de valeur des créations personnelles. Une fois que les citoyens auront été éduqués, il sera nécessaire de les aider à gérer leurs propriétés et il conviendra, pour ce faire, de structurer davantage toutes les plates-formes disponibles.

Troisième table ronde :
Regards croisés sur d'autres approches du numérique

M. Guillaume Poupard, directeur général, Agence nationale de la sécurité des systèmes d'information (ANSSI). – Je me concentrerai uniquement sur le domaine de la sécurité car je n'ai aucune prétention en termes de pédagogie et d'enseignement. La sécurité concerne la protection des citoyens et de leurs données mais également celle de notre patrimoine économique, scientifique et technique et donc celle de nos emplois. En effet, aujourd'hui, on observe au quotidien que **la perte de savoir-faire et de connaissances au sein de nos entreprises est très inquiétante et est directement liée à une déficience de sécurité numérique**.

La compétitivité des entreprises est donc en jeu, de même que le potentiel de défense de la Nation, les attaques informatiques les plus graves touchant les opérateurs d'importance vitale que sont les transports, l'énergie, les communications, etc. Si l'on imagine les conséquences des catastrophes en cascade que représente la faille numérique, il devient même difficile de prévoir comment la contenir. C'est pourquoi dans un grand nombre de domaines, **il est vital de prendre en compte le risque numérique**.

Une fois ce discours anxiogène tenu, il convient toutefois de se souvenir à quel point **le numérique constitue également une opportunité** pour garder notre compétitivité et notre avance dans l'univers très mondialisé. Très clairement, **la France a un rôle majeur à jouer et les partenaires étrangers viennent nous chercher car nous présentons une alternative crédible en matière de produits et de services**. Le tout suppose la formation de personnes capables de tenir ces postes.

La formation à la sécurité **est donc indispensable. Les attaques qui réussissent passent souvent par des maillons humains**, des comportements inadaptés et par des entorses à « *l'hygiène informatique* ». La prise en compte du facteur humain dans la conception et l'exploitation des systèmes d'information est donc absolument essentielle, tout comme est évidente la nécessité de mettre en place des systèmes adaptés tant aux besoins métiers qu'à leur exposition aux risques.

Concernant l'enseignement de la sécurité informatique, il existe des notions simples mais souvent inconnues et des concepts très complexes. Par exemple, **peu de personnes comprennent ce qu'est un certificat numérique** et la vulgarisation de la notion suppose à la fois un travail de technicien et de pédagogue.

Un autre exemple de la difficulté d'enseigner la sécurité informatique est celui de la faille de *Heartbleed*. Le sujet intéresse manifestement, a figuré plusieurs fois à la une du Monde.fr et peut

s'expliquer assez simplement à une personne qui dispose de notions d'informatique. La faille de *Heartbleed* permet à ceux qui l'exploitent de **récupérer illégitimement des données sur un serveur qui permet l'accès à des mots de passe et des modes de connexions sensibles**.

En conclusion, l'enseignement de la sécurité est essentiel et doit être dispensé par des professionnels à différents niveaux. Aujourd'hui, **les spécialistes ne sont pas assez nombreux**. Au moment où l'activité humaine est numérisée et alors qu'il existe quarante-sept *masters* en sécurité. **Les formations ne s'adressent toutefois pas toujours aux bonnes personnes** et certaines d'entre elles sont majoritairement suivies par des élèves étrangers.

En outre, **l'intégration de modules de sensibilisation aux enjeux liés à la cybersécurité dans les formations supérieures constitue une priorité absolue**. Le travail déjà entrepris devra être poursuivi et constitue une **priorité nationale**, ainsi qu'il l'a été rappelé dans le Livre Blanc de la Défense et de la sécurité nationale.

Les principes d'hygiène informatique devraient également être enseignés très tôt, dès le secondaire.

Le dernier point concerne la formation continue à la sécurité informatique. Un grand nombre de spécialistes dans le domaine des télécoms pourraient en effet évoluer vers des problématiques de sécurité informatique et bénéficier de formations professionnelles en ce sens.

M. Éric Delbecque, chef du département de sécurité économique, Institut national des hautes études de la sécurité et de la justice (INHESJ). – Je serai sans doute l'un des moins spécialisés sur le thème dans cette assemblée. Pour vous expliquer rapidement le domaine d'intervention de notre organisme, qui dépend du Premier ministre, je m'occupe au sein de l'INHESJ de la thématique de la cybersécurité. Nous avons, à ma connaissance, la seule formation en la matière délivrée par un organisme d'État, en partenariat assez fort avec l'ANSSI et avec le CIGREF représentant le monde des entreprises. Nous formons avant tout des acteurs du secteur privé et des hauts fonctionnaires. En outre, du stade expérimental, la formation est passée à un stade plus professionnel.

Globalement, le risque numérique nous concerne pour trois types de raisons.

La première n'est pas essentielle mais mobilise souvent les médias et met en rapport le risque numérique avec la lutte contre le terrorisme, à travers des dispositifs de surveillance généralisée. Très concrètement, cette question est traitée par des hommes et des logiques de terrain et non par du « fétichisme technologique ». En d'autres termes, même si l'outil technologique est évidemment très important dans la lutte anti-terroriste, il n'est pas le déterminant du problème et n'en constitue qu'un moyen.

Les deux autres problématiques paraissant davantage au cœur du débat, concernent la protection de la vie privée et l'évolution de l'intimité et également le potentiel de nos entreprises ; je ne reviendrai pas sur la menace effectivement déterminante pour les entreprises qui subissent la fuite d'informations.

Néanmoins, le risque numérique n'implique pas uniquement les dysfonctionnements mais également les phénomènes de guerres d'information et d'atteinte à l'image. Nous savons aujourd'hui que le meilleur moyen de déstabiliser une entreprise est d'attaquer son dirigeant et de casser son image. De ce fait, le risque technologique implique donc également une question de contenu. Certains responsables dans le public et le privé sont malheureusement assez néophytes sur le sujet.

La question sur l'évolution de l'intimité met également en valeur le fait indiscutable, notamment pour les plus jeunes, que le débat sur l'intimité vient aussi d'un défaut d'anticipation et de projection : en effet, il existe un problème de rapport au temps, **les plus jeunes ne se rendant pas compte des conséquences de la mise en ligne d'une information**. De plus, la capacité de scénarisation est tout à fait considérable pour le débat sur l'intimité. Il s'agit donc d'un motif d'éducation philosophique, historique et sociologique, sur les catégories de la pensée. Ne devrait-on pas **apprendre aux plus jeunes à faire de la prospective à usage individuel** et à s'interroger réellement sur ce qu'il adviendra des données mises en ligne ? La contribution à la « société de surveillance » est également le fait de l'individu lui-même. Pour notre part, nous essayons de porter l'attention sur le moyen, dans le comportement, les projections et les connaissances du monde, de minimiser le risque technologique en dehors de la problématique technologique. En réalité, le risque technologique réside avant tout dans les usages, ce qui explique le titre de notre formation à la « *sécurité des usages numériques* ».

En matière de secret des affaires, **les entreprises ne sont pas toujours conscientes de l'existence d'un cœur stratégique à protéger** et certaines grandes entreprises sont bien en peine de savoir ce qui mérite une protection accrue. Certaines d'entre elles effectuent des études sur la « perméabilité organisationnelle » et se rendent compte avec effroi, à cette occasion, de toutes les informations qui circulent sur leur compte en dehors d'elles. Les informations sont ainsi perméables car **les grandes entreprises et les administrations fonctionnent en silo, chaque direction ignorant ce que fait l'autre, de sorte que toute personne qui prend le temps de collationner les informations peut faire des découvertes incroyables**. Cette question n'est donc pas maîtrisée par les entreprises et intervient avant même la sécurité en tant que telle. Elle est avant tout liée aux pratiques humaines. C'est pourquoi nos formations prennent avant tout en compte les questions juridiques, historiques, géopolitiques, pour acquérir une capacité à lire les stratégies avant même de prendre des mesures très opérationnelles en

matière de sécurité informatique. Les unes ne sont évidemment pas exclusives des autres mais il ne faut pas confondre les deux aspects. Hormis quelques philosophes et sociologues, **nous n'avons pas tiré le dixième des conclusions qui s'imposent sur le monde numérique en tant que révolution anthropologique**. À titre personnel, je pense qu'il s'agit de **la plus grande révolution dans notre conception du temps** depuis l'invention de l'imprimerie, y compris dans l'acquisition culturelle.

Aujourd'hui, nous pensons, d'une part, que la mémoire n'a plus d'utilité puisque les données sont stockées et croyons, d'autre part, que la multiplication des données va nous servir de réflexion. Or si aucun travail humain d'interprétation de la connaissance n'est réalisé, celle-ci est quasiment inutile. **L'éducation numérique consiste, en premier lieu, à faire réfléchir tous les publics sur l'ensemble des conséquences humaines de la révolution numérique.** Il est impossible d'être opérationnel immédiatement et d'attendre des « boîtes à outils » sans avoir préalablement réfléchi au contenu.

M. Gilles Dowek, responsable du secrétariat du groupe de travail sur le rapport de l'Académie des sciences « *L'enseignement de l'informatique en France - Il est urgent de ne plus attendre* ». – Vous m'avez demandé, dans cette intervention, de vous parler du rapport rédigé par l'Académie des Sciences. L'Académie a une réflexion assez ancienne sur la nécessité et l'importance d'enseigner l'informatique à tous les niveaux. Depuis 2006 et l'organisation d'un premier colloque sur le sujet par M. Maurice Nivat, la réflexion est continue sur la question.

Le comité de réflexion sur l'enseignement des sciences, présidé à l'époque par M. Pierre Léna, avait demandé aux informaticiens d'écrire un rapport sur l'importance de l'enseignement de l'informatique et d'inclure une esquisse de *curriculum* de l'enseignement de l'informatique, de la maternelle jusqu'au doctorat.

Les trois informaticiens qui se sont saisis du sujet étaient MM. Maurice Nivat, Gérard Berry et Serge Abiteboul, entourés d'une équipe d'une dizaine de personnes, dont je faisais partie, pour rédiger le rapport d'une manière collective. Le texte est donc signé collectivement et je suis, pour ma part, coauteur de son brouillon.

Les motivations pour enseigner l'informatique sont de trois ordres :

En premier lieu, la question est économique pour **préparer les jeunes à leur métier de demain, ce qui constitue l'une des deux grandes missions de l'École avec la préparation des jeunes à leur rôle de citoyen**. Pour ma part, j'appartiens à la petite minorité qui estime que l'école est également destinée à **préparer la jeunesse à la citoyenneté**, alors que la plupart des enseignants conçoivent soit l'unique rôle économique, soit l'unique rôle citoyen. Heureusement, notre groupe de réflexion était équilibré sur le sujet et le rapport commence par l'aspect économique.

En effet, il faut préciser que 30 % de la recherche et du développement dans le monde s'effectue dans le domaine de l'informatique au sens large, alors que, en France, ce taux n'est encore que de 17 % à 18 %. L'idée de former les informaticiens est certes importante mais il est encore plus essentiel de considérer que **tous les métiers supposent des connaissances en informatique**.

Par exemple, le métier d'archéologue a été transformé deux fois par l'informatique, la première fois en stockant leurs informations dans l'ordinateur au lieu du cahier et la seconde en utilisant des algorithmes pour assembler, par exemple, des fragments de poterie. Notamment, un travail inédit a été réalisé sur la Gueniza d'Alexandrie, sorte de lieu de stockage dans lequel pendant deux mille ans les gens ont stocké des documents en quatre ou cinq langues. Il était donc nécessaire de reconstituer ces documents, ce qui a pu être partiellement réalisé grâce à un algorithme. La manière aujourd'hui de concevoir le métier et le rôle de l'archéologue a ainsi été radicalement révolutionnée par l'informatique.

Dans le même ordre d'idée, les ouvriers tourneurs ou les comptables ont vu leur métier transformé, de même que le métier d'enseignant ou de chauffeur de taxi.

L'aspect concernant le citoyen n'est sans doute pas suffisamment traité car il implique des problèmes à forte composante technique. Par exemple, **la loi Hadopi aurait été moins ridicule si la compréhension des questions techniques sous-jacentes avait été meilleure de la part de ses auteurs**. La loi Hadopi s'est en effet concentrée sur l'échange de fichiers par *peer to peer*, alors même que cette technique était en train de disparaître.

Par ailleurs, **les questions de neutralité du *Net* sont aussi importantes que celles relatives à la guerre et à la justice** et les citoyens doivent absolument les maîtriser lorsqu'ils élisent leurs représentants, pour connaître la position de chaque homme politique sur le sujet.

Il est même possible d'aller plus loin, ainsi que je l'ai fait lors d'une présentation à l'Union des démocrates et indépendants (UDI), au cours de laquelle j'ai mis en avant l'idée que les institutions étaient des algorithmes de compression. Cette présentation des institutions a intéressé l'assistance car elle était inédite.

En tout état de cause, la pensée informatique est spécifique et peut être ainsi résumée : à la question « *comment parvenir à ce résultat* ? », la réponse est « *par la création d'un algorithme* ». Les algorithmes permettent de répondre à un grand nombre de questions mais ils ne résument pas à eux seuls la pensée informatique. Celle-ci implique également la notion de langage, indispensable pour comprendre le monde actuel. De la même manière, la notion de flux d'informations et de localisation géographique dans l'espace est fondamentale. À ce propos, je suis en désaccord avec l'idée que l'informatique sera fondamentalement différente dans cinquante ans :

certes, les outils auront évolué, mais **les notions fondamentales de l'informatique et la pensée algorithmique resteront**. Nous apprenons donc aux enfants des notions qui leur seront encore utiles dans des dizaines d'années.

La seconde partie du rapport est l'esquisse d'un *curriculum*. Il n'était pas question de tomber dans le piège d'une trop grande précision mais, au contraire, d'esquisser à gros traits les contenus des programmes. À titre d'exemple, le programme de français, de la maternelle au lycée, est évoqué. Les professeurs de français enseignent la lecture et l'orthographe en primaire, la littérature au lycée, tandis que le collège reçoit un mixte des deux. Nous souhaitions donc parvenir à ce même type de description très macro, en comptant sur le fait que les personnes ayant une meilleure connaissance du terrain seraient susceptibles d'affiner.

En décrivant cette esquisse grossière, est apparue l'idée centrale et organisatrice d'**un programme informatique à la maternelle et au lycée et constituée par la programmation**. Certains étudiants n'ont jamais appris à programmer et on leur fournit un algorithme à observer. D'autres possèdent des notions et développeront eux-mêmes un algorithme. En effet, il s'avère que **l'approche est toute autre avec un outil que l'élève a lui-même construit**. Il passe ainsi d'une situation de spectateur du *Net*, à une démarche d'acteur.

Le *curriculum* propose donc que cet enseignement soit celui du collège. Il s'appuie en premier lieu sur un document néo-zélandais proposant l'informatique débranchée *(unplugged)*, c'est-à-dire sans utiliser d'ordinateur. Pour autant, il a été choisi de ne pas retenir exclusivement cette approche « technophobe » et fausse – car l'informatique suppose à l'évidence l'utilisation d'un ordinateur – et nous avons recensé des activités possibles avec un ordinateur. Par exemple, le simple fait d'envoyer un courrier électronique et de se demander comment il parvient à destination, ouvre un vaste champ de questions, qui conduisent à s'interroger sur la manière dont les ordinateurs sont reliés entre eux en réseau d'un continent à l'autre, la manière dont les informations sont acheminées sur ces réseaux, etc.

Au collège, devrait être enseigné l'apprentissage de la programmation et, au lycée, il est possible de commencer à s'interroger sur la façon d'utiliser le langage de programmation, à étudier les algorithmes fondamentaux. La représentation d'objets, la modélisation, la connexion d'ordinateurs en réseaux, font également partie du cursus. Le tout est aujourd'hui étudié en licence en France alors qu'un grand nombre d'autres pays l'inscrivent au programme des lycées.

Je terminerai en évoquant les blocages. Les professeurs, y compris ceux des disciplines scientifiques, comprennent qu'il est désormais impossible d'enseigner les sciences comme par le passé. Les choses évoluent et il s'agit de l'intérêt de toutes les sciences. Les parents sont également favorables – ainsi qu'il ressort d'un texte publié par la PEEP – de même que

les lycéens. Un sondage sur la perception du numérique par nos concitoyens montre que **60 % des parents sont favorables à l'apprentissage précoce de l'informatique**.

Les blocages résident donc uniquement dans l'institution. Toutefois, l'enseignement suppose la présence de professeurs, y compris dans les *MOOCs*. En outre, il existe **une fausse croyance que l'informatique peut s'enseigner sans professeurs**. L'informatique est un domaine scientifique qui a connu un très grand succès et qui a impacté tous les métiers. Or, comme l'informatique est partout, elle n'est nulle part et il existe ce sentiment qu'il n'est pas besoin de professeur d'informatique. D'autres disciplines, telles que le français ou les mathématiques, se retrouvent également partout et pourtant les enseignements nécessitent des professeurs spécifiques.

Bien entendu, un travail interdisciplinaire est indispensable mais le véritable enseignement de l'informatique ne pourra pas se développer de la maternelle au doctorat, sans la présence de professeurs d'informatique.

M. Daniel Kofman. – Grâce à l'informatique, nous construisons des systèmes de plus en plus complexes et des services flexibles, mais qui impliquent des trous de sécurité nécessitant des technologies évoluées pour tenter de les colmater. Nous avons ensuite évoqué la stratégie et les usages et il existe effectivement un besoin d'éducation en la matière.

Il est vrai que l'informatique pénètre aujourd'hui tous les métiers mais qu'il existe, en parallèle, une certaine normalisation des métiers non techniques.

M. Jean-Marie Chesneaux. – L'un des problèmes liés à la sécurité concerne l'usage alors que le risque d'attaque d'une entreprise réside dans le matériel et sa protection. Si l'on examine la naissance de l'informatique à l'université, on constate que **les blocages ont toujours été liés au manque de professeurs**. Mais il est dangereux de s'arrêter là et il convient de trouver des solutions transitoires. Pour l'ISN (Informatique et sciences du numérique), les professeurs ne font pas de blocage et acceptent la formation continue à une matière qu'ils connaissent un peu déjà. À cet égard, les établissements du supérieur ont formé des formateurs qui ont eux-mêmes formés d'autres professeurs de lycées et de classes préparatoires. Il ne s'agit pas non plus d'enseigner l'informatique neuf heures par semaine mais il doit être possible de **mettre en place un système simple, en primaire, au collège et au lycée**.

M. Éric Delbecque. – Un point qui pourrait paraître anecdotique, mais qui ne l'est en réalité pas, **tient à la nécessité d'apprendre à des cadres d'entreprises qu'on n'arrive pas dans n'importe quel pays avec son ordinateur rempli de données et laissé sans surveillance**. De même, **les informations confidentielles ne doivent pas être transmises par *SMS***. Il s'agit donc d'une question d'usage dans les entreprises et plus l'échelon

est haut, plus il se pense immunisé de tout risque en la matière. Du point de vue du citoyen ou dans l'entreprise, le problème est de penser au premier chef au sort réservé à l'information.

M. Gilles Dowek. – Lorsqu'on débute une nouveauté, il est indispensable d'utiliser les moyens disponibles. Or l'esprit pionnier fonctionne au début mais s'essouffle traditionnellement dans la durée. Le second paradoxe tient aux difficultés de recruter des professeurs de sciences : de ce fait, pourquoi ne pas aller chercher les professeurs d'informatique dans les *masters* en informatique, au lieu de les recruter pour les universités de sciences, où les étudiants sont déjà rares ?

M. Jean-Marie Chesneaux. – En effet, nous ne sommes pas obligés de recruter des candidats au CAPES de mathématiques pour enseigner l'informatique alors même qu'un grand nombre d'étudiants en informatique sont tout à fait attirés par l'enseignement.

Mme Sophie Pène. – L'enseignement de l'informatique est considéré aujourd'hui comme impossible par crainte qu'il n'enlève quelque chose à d'autres. Chez M. Vincent Peillon, la stratégie pour l'école primaire procédait de la volonté d'**ouvrir du temps à des intervenants qui n'étaient pas des professeurs**. Il est donc nécessaire de passer par cette ouverture.

M. Daniel Kofman. – Le retard sera très significatif si nous n'en passons pas par là.

M. Pierre Léna. – Ce débat se situe au cœur du sujet. Le propre de l'institution « école » est le temps et l'implantation d'une réforme est d'une lenteur considérable. L'avantage de l'ISN est d'avoir commencé petit puis d'avoir rencontré des limites au bout de quelques années. Face à ce constat, les solutions consisteraient à confiner toute innovation hors du temps scolaire, se résignant ainsi à l'idée de la rigidité des programmes. Devant une commission parlementaire, j'ai eu l'occasion de contester vigoureusement cette conception de l'enseignement des sciences, uniquement confiées à des animateurs socioculturels.

La seconde possibilité serait d'abandonner la politique du « tout ou rien », en établissant un plan de transformation progressive sur la durée. Il est clair que sur le sujet qui nous occupe, **il faut former l'ensemble des professeurs dans toutes les disciplines tout en recrutant des professeurs spécialisés qui irrigueront progressivement l'ensemble des établissements**. Il serait en effet illusoire de penser que dès demain, nous aurions un corps de professeurs d'informatique pour irriguer les 7 000 collèges.

M. Bruno Sido. – Je vous remercie vivement pour l'ensemble de ce que vous nous avez apporté et laisse à ma collègue, Mme Anne-Yvonne Le Dain, le soin de conclure.

Mme Anne-Yvonne Le Dain. – Je dois avouer que je suis impressionnée par l'ampleur du sujet, qui fait apparaître des divergences

peu importantes entre vous, d'importantes convergences et quelques éléments de réponses.

Notre rapport porte sur le risque numérique mais le risque que vous énoncez va bien au-delà puisqu'il évoque une société qui s'arrête et n'est plus productrice. J'étais déjà quelque peu inquiète, je le suis encore davantage.

Je vous remercie de tous les éclairages apportés.

MME MYRIAM QUÉMÉNER, MAGISTRAT, SPÉCIALISTE DES PROBLÈMES DE LA CYBERSÉCURITÉ

11 juin 2014

Tous les jours, nous recevons des rapports émanant, entre autres, d'éditeurs de logiciel, qui nous donnent une idée de l'ampleur du préjudice dans le domaine de la sécurité numérique. D'ailleurs, les compagnies d'assurance ont développé des départements de façon à assurer le risque numérique, comme l'ont fait les Anglo-saxons.

Il n'existe pas, en France, de vue d'ensemble au niveau des chiffres. C'est l'une des préconisations du rapport du groupe interministériel présidé par M. Marc Robert, procureur général. Selon l'Institut national des hautes études de la sécurité et de la justice (INHESJ) et l'Observatoire national de la délinquance et des réponses pénales, **180 000 entreprises auraient été victimes d'actions de *phishing*, de vol en ligne, de vol d'informations, d'altération de leur site, ou d'infection de leurs machines**.

Deux tendances apparaissent, la fraude externe mais aussi la fraude interne avec des contentieux qui se développent. Des salariés par vengeance, par exemple, ou dans le cadre d'une procédure de licenciement, dérobent des éléments à une entreprise. La problématique droit du travail et nouvelles technologies s'est assez intensifiée ces derniers temps.

Le fléau identifié au niveau des entreprises c'est la contrefaçon en ligne qui s'est fortement développée avec Internet. 40 % de l'activité du Service national de douane judiciaire (SNDJ) sont constitués d'affaires de contrefaçons en ligne.

En réaction, les entreprises, face parfois à un manque de moyens étatiques, ont créé leur propre service de veille avec souvent d'anciens commissaires divisionnaires ou d'anciens gendarmes.

Assez peu de condamnations par la Justice interviennent. Les affaires comme, par exemple, les escroqueries en bande organisée, ne sont souvent pas repérées en tant qu'actes de cybercriminalité alors qu'il peut y avoir des personnes qui créent leur réseau de « mules » – d'intermédiaires –, par exemple des particuliers, qui acceptent de voir transiter sur leur compte bancaire des sommes de provenance frauduleuse, du blanchiment, moyennant un pourcentage qu'elles vont recevoir ou non.

Nous avons eu le cas d'un réseau créé en Roumanie et en Chine, ce qui illustre la problématique internationale de la cybercriminalité.

La majorité des escroqueries sont des abus de confiance ou des fraudes aux cartes bancaires. On compte également beaucoup d'atteintes aux personnes comme l'**usurpation d'identité en ligne**, la **création de faux profils**. C'était le cas d'un webmestre qui, par vengeance, pour déstabiliser une entreprise, avait créé le profil d'un salarié qui n'existait pas ; il a été condamné pour usurpation d'identité en ligne.

Comme exemple de déstabilisation du site d'une entreprise, on peut citer le cas d'un grand laboratoire pharmaceutique, en l'occurrence *Sanofi*, dont l'une des filiales située en Algérie, a été inondée de courriels menaçants, faisant l'apologie du terrorisme, de sorte qu'une cellule de crise a dû être créée. L'auteur de cette attaque, qui ne s'est pas présenté à l'audience, a été condamné à un an d'emprisonnement.

Au niveau de la cyberdéfense, de la cybersécurité, qui sont des enjeux de sécurité nationale, il existe avec l'ANSSI un dispositif tout à fait structuré, étoffé.

Concernant les opérateurs d'importance vitale (OIV), nous avons parfois des rapports de l'ANSSI et ensuite c'est la Direction générale de la sécurité intérieure (DGSI) qui est saisie. Le dispositif est renforcé, c'est parfait et lisible.

En revanche, comme le Livre blanc sur la défense et la sécurité nationale l'indique, **la cybercriminalité n'est pas intégrée dans la sécurité nationale mais il y a une porosité entre les trois niveaux suivants : cyberdéfense, cybersécurité et cybercriminalité** qui est la criminalité transposée à l'ère numérique.

De plus en plus, il existe des affaires d'extorsion. Au départ, il s'agit d'une rencontre virtuelle par le truchement d'un site et ensuite un guet-apens est tendu. Cela permet des rencontres qui n'auraient jamais eu lieu.

Le dispositif autour de la cybercriminalité doit être amélioré. On parle parfois d'une certaine nébuleuse. Au niveau des services, il y a la police et la gendarmerie, ainsi que l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC).

L'Office central pour la répression de la grande délinquance financière (OCRGDF) a sorti des affaires d'escroquerie aux faux ordres de virement. Certaines entreprises, comme le *Géant vert*, ont osé en parler. Une sensibilisation commence à avoir lieu. C'est pourquoi, par exemple, *Infogreffe* est très vigilant sur la communication de renseignements, de noms, d'adresses électroniques de dirigeants.

Les délinquants vont demander, de préférence le vendredi soir, des ordres de virement.

La Délégation interministérielle à l'intelligence économique vient de mettre sur son site une alerte à destination plutôt des PME pour les sensibiliser à ces nouveaux modes opératoires.

Beaucoup d'initiatives sont prises mais pas nécessairement de façon coordonnée.

Certains magistrats ne connaissent pas l'activité de la Délégation interministérielle à l'intelligence économique.

Il est nécessaire de coordonner l'ensemble des actions de lutte contre la cybercriminalité.

Au niveau des services d'enquête, d'importants efforts sont consentis avec des formations spécialisées notamment des cellules dites NT (nouvelles technologies) dans la gendarmerie et avec des investigateurs en cybercriminalité (ICC) dans la police nationale. **Pour les magistrats, il n'y a pas de spécialisation pour l'instant.**

Aucune définition de la cybercriminalité ne figure dans le code pénal. Il faudrait qu'il y ait des orientations de politique pénale et que la notion de cybercriminalité soit définie ; en France, nous en avons une conception assez large. Cela comprend les infractions strictement informatiques, qui ont pour cibles les systèmes d'information, les systèmes de traitement informatisé des données, ainsi que les infractions classiques comme les fraudes, les escroqueries, qui vont être facilitées, démultipliées, par le recours à Internet. La Commission européenne parle d'infractions de contenu comme la pédophilie sur Internet, le racisme, mais cela concerne moins le domaine de l'entreprise.

La cybercriminalité n'est mentionnée que dans le code de procédure pénale dans la liste des trente-deux infractions qui peuvent se dispenser de la double incrimination en matière de mandat d'arrêt européen. Le manque de définition officielle contribue à une réticence sur ce sujet.

On dispose d'**un arsenal juridique extrêmement complet** avec la loi de 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée en 2004, qui percevait les ordinateurs comme pouvant porter atteinte aux libertés individuelles. Mais il y a **énormément d'infractions qui sont sous-utilisées** comme la collecte illégale de données ; cette infraction peut intéresser les entreprises car le vol de données peut être réprimé. La doctrine est contre le fait de retenir le vol d'éléments immatériels mais, par le biais de la collecte illégale de données, on pourra apporter une réponse juridique. C'est comme le détournement de finalité. Par exemple, pour réserver une chambre d'hôtel, vous avez, communiqué vos données bancaires alors qu'on ne sait pas ce qu'en font certains hôteliers.

Tout comme la loi de 1978, la loi Godfrain de 1988, relative à la fraude informatique, est sous-utilisée ; elle ne donne lieu qu'à une centaine de condamnations par an, ce qui est assez faible.

Le dispositif législatif s'est complété au fil du temps notamment en matière de droit matériel avec l'usurpation d'identité en ligne par exemple mais surtout en matière de droit processuel, c'est-à-dire le droit de la procédure pénale, après les attentats du 11 septembre 2001 et les lois de sécurité intérieure. Au minimum une loi par an sur la cybercriminalité est adoptée depuis.

L'infiltration, c'est-à-dire entrer en contact avec une personne soupçonnée de commettre des infractions, est maintenant possible en matière de contrefaçons. La captation de données à distance n'est pas encore opérationnelle même si la loi d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI 2) commence à dater. Cela pose des problèmes techniques de mise en œuvre : il ne faut pas confondre le logiciel espion des délinquants avec celui des officiers de police judiciaire. Les moyens d'investigation existent. Il est possible aussi de faire des copies. L'interception de communications est transposable au réseau Internet.

On ne fait pas suffisamment l'état des lieux des dispositions qui existent. Par exemple, la géolocalisation, la possibilité de surveiller quelqu'un en temps réel, est soumise au régime de l'interception téléphonique. Les arrêts de la Cour de cassation du 22 octobre 2013, ont conduit à l'adoption d'une nouvelle loi, le 28 mars 2014. Or, la surveillance était prévue par la loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité et a été étendue par la loi du 6 décembre 2013 relative à la lutte contre la fraude fiscale et la grande délinquance économique et financière. Mais le problème reste que **personne n'a dit que la géolocalisation est une forme de surveillance**. La doctrine l'avait dit, en prenant l'exemple de la surveillance numérique. Le traité de procédure pénale Desportes-Lazerges avait d'ailleurs indiqué que la géolocalisation pouvait correspondre à de la surveillance.

La surveillance est limitée à la surveillance physique. Or, les flux financiers, les flux illicites, étant de plus en plus dématérialisés, la surveillance présente un intérêt moindre cependant il devient intéressant d'intercepter des flux illégaux.

Il existe toujours un décalage entre le droit et la réalité.

La France a tenu compte de la réglementation internationale en effectuant la transposition de la plupart de ses textes. La convention de Budapest du Conseil de l'Europe sur la cybercriminalité, même si certains la trouvent dépassée, demeure un outil qui fixe les bases d'une réglementation internationale pénale intéressante.

La notification des failles a été mise en place. Elle est effectuée auprès de la CNIL pour les données personnelles et auprès de l'ANSSI

quand cela touche à la sécurité des systèmes d'information, notamment celle des OIV**.**

Le milieu bancaire est très inquiet car il est déjà soumis à une surveillance étroite selon un dispositif extrêmement contraignant, par l'Autorité des marchés financiers (AMF), l'Autorité de contrôle prudentiel et de résolution (ACPR), etc. Il ne sait plus trop où il en est.

Certains cadres ignorent encore la notion d'opérateur d'importance vitale (OIV) ; cela est encore apparu récemment, lors d'une intervention chez *Total*. **Une formation continue associant l'ensemble des acteurs de l'entreprise est donc absolument nécessaire.** Les différents départements d'une entreprise doivent se parler. C'est l'intérêt de la création du poste du directeur de la sécurité. La nécessité de décloisonner les services ressort des réflexions que je mène avec le Club des directeurs de sécurité des entreprises.

Il faut mieux faire connaître l'action judiciaire auprès des entreprises. Surmontant leurs réticences premières, de grandes entreprises s'engagent maintenant à porter plainte. Pour cela, il faut mettre en place des stratégies, prendre contact avec des services spécialisés, des offices de préférence ou l'ANSSI, qui peut prendre le relais, par l'intermédiaire de son chargé de mission, pour s'engager dans une démarche de dépôt de plainte qu'il faut dédramatiser. Cela nécessite des contacts directs avec le procureur de la République ou un magistrat référent.

J'ai piloté un groupe de travail dans le cadre d'un conseil régional de politique pénale Paris-Versailles, pendant un an et demi. Nous avions mis en place, malheureusement de façon empirique, **un magistrat cyberréférent au sein des parquets** des principaux tribunaux de la région parisienne.

Ce qui constitue une source d'insécurité pour les entreprises c'est le problème du vol de données, d'éléments immatériels. Il y a eu quelques décisions, notamment à Clermont-Ferrand, mentionnant le vol d'éléments immatériels. Un **projet de directive européenne** prévoit la répression de la violation du secret des affaires – ce projet de texte émanant de la Délégation interministérielle à l'intelligence économique.

Il faudrait prévoir des infractions assez simples susceptibles d'être comprises par tous et **sur lesquelles les magistrats se spécialiseraient.**

Depuis trente ans, l'institution judiciaire connaît une évolution avec des spécialisations, des compétences nationales sur des sujets pointus comme le terrorisme, les crimes contre l'humanité, la santé publique, etc.

En 2004, il y a eu la création des juridictions interrégionales spécialisées (JIRS) mais elles sont tellement spécialisées en tout qu'elles traitent assez peu d'affaires en lien avec la cybercriminalité. Plus de 50 % des affaires traitées par les JIRS concernent des gros trafics de stupéfiants.

Au sein des JIRS, il faudrait spécialiser des magistrats en criminalité informatique.

M. Jean-Marie Bockel avait préconisé dans son rapport, pour les attaques visant les OIV et pour des affaires complexes d'envergure qui nécessiteraient des investigations mettant en cause plusieurs pays, la création d'une juridiction spécialisée à Paris. Le procureur de Paris, M. François Molins, a écrit une note en ce sens prônant la création d'**un pôle numérique** en reprenant plusieurs éléments d'un ouvrage que j'ai écrit avec M. Yves Charpenel.

En revanche, **les JIRS auraient vocation à traiter les petites affaires d'attaques d'entreprises en province**. Il y aura peut-être des calages à opérer sur la compétence territoriale, par exemple, à Nanterre où il y a une concentration d'entreprises avec La Défense. L'OCLCTIC a un contact « TIC » au parquet de Nanterre qui est son interlocuteur privilégié. **La compétence territoriale est l'une des problématiques** car on a vu des procédures relatives à des escroqueries qui ont tourné dans différents parquets qui se demandaient s'ils étaient vraiment compétents. Il faut mettre un terme à ces situations qui s'apparentent à une forme de déni de justice. Le parquet de Nanterre, qui dispose d'une plate-forme de signalement, appelée « *PHAROS* », gérée par l'OCLCTIC, pourrait avoir vocation à traiter les procédures au même titre que Paris.

Au niveau de l'administration centrale, **tous les pays européens se sont dotés de services spécialisés en matière de lutte contre la cybercriminalité numérique sauf la France**. La Chancellerie a vocation à appréhender de façon officielle ce sujet en créant, par exemple, un pôle numérique rattaché soit au Secrétariat général, qui est complétement transversal, soit à la Direction des affaires criminelles et des grâces.

Pour l'instant, les magistrats qui traitent ces affaires soit ont une appétence particulière pour le sujet soit sont à la Cour de cassation. D'ailleurs, celle-ci a lancé, en 2013, tout une série de conférences consacrées au numérique, intitulée « Le numérique dans tous ses états » avec des experts, des universitaires. J'ai moi-même participé à une séance sur la preuve numérique car **l'un des sujets majeurs c'est l'harmonisation des modes de preuve, au moins au niveau européen.** En effet, beaucoup d'avocats qui, eux, se spécialisent, font des requêtes en nullité dans ce domaine de la preuve, fondées sur la relativité, la fragilité de la preuve numérique.

À titre d'exemple, lors d'une affaire, des avocats ont invoqué la nullité des moyens d'investigation en disant qu'il s'agissait de géolocalisation et que la loi de mars 2014 n'avait pas été appliquée. Or, il s'agissait de bornage c'est-à-dire d'interception *a posteriori.* Ce qui montre que **les magistrats doivent avoir une idée des modes opératoires.**

Il y a des affaires de fraudes à la téléphonie qui causent des préjudices très importants aux entreprises avec les numéros surtaxés. Des escrocs montent ainsi des entreprises. Il n'est pas inutile de faire de la pédagogie. Les escrocs sont défendus par des cabinets d'avocats spécialisés en la matière.

La criminalité financière et la cybercriminalité peuvent se recouper mais **il y a des modes opératoires et des spécificités qui nécessitent une formation obligatoire** alors qu'elle n'est encore que facultative ; elle est également ouverte aux officiers de police judiciaire. **Cette formation devrait être imposée aux magistrats dès la formation initiale.** Il faudrait au moins que les magistrats sachent où chercher. La Chancellerie a un rôle d'expertise et de conseil aux juridictions à jouer sur ce sujet-là. On peut envisager un forum, des formations à distance (*e-learning*). Cette formation devrait être pluridisciplinaire, dispensée par des experts, des avocats, des officiers de police judiciaire, qui montreraient des cas pratiques et qui dédiaboliseraient ce domaine encore ésotérique pour de non-spécialistes.

Au niveau international, on voit apparaître des opérations qui concernent l'entreprise alors qu'avant il s'agissait surtout d'opérations internationales de lutte contre la pédophilie sur Internet qui suscitent un consensus. Maintenant, il existe des affaires de contrefaçons de médicaments, les opérations PANGEA.

Récemment, la chambre criminelle a validé une procédure initialement américaine, visant à repérer des délinquants qui allaient sur des forums donnant des renseignements pour s'y livrer à de la cybercriminalité, du *carding*, du *skimming*, tout ce qui constitue une escroquerie aux cartes bancaires. La chambre criminelle a pris position et validé cette procédure en disant que l'on avait affaire à une **provocation à la preuve** et non pas une **provocation à l'infraction** qui aurait été invalidée, elle, par la chambre criminelle.

Il convient de mener une veille juridique assez importante. La Chancellerie aurait dû faire connaître et commenter cette décision de la chambre criminelle qui date d'environ trois semaines.

Pour la géolocalisation, dès 2011, le milieu universitaire avait alerté sur le fait qu'elle avait été validée en Allemagne parce qu'il existait un texte général qui prévoyait sa réglementation. En raison de l'absence de veille en France, le problème de la géolocalisation a abouti à une loi adoptée dans la précipitation.

En matière d'arsenal pénal, on dispose de tout ce qu'il faut.

Mais, contrairement aux contentieux sur les violences conjugales, les stupéfiants, la politique d'immigration, **la cybercriminalité**, elle, **ne dispose pas de politique pénale d'ensemble**. Il n'existe que des circulaires, des commentaires, etc. Il incombe au ministère de la justice de mettre en place cette politique pénale et de **donner des conseils de stratégie procédurale à**

adopter notamment lorsqu'il s'agit d'infractions commises au préjudice des entreprises.

Des projets sont en cours au niveau du ministère de l'intérieur pour obtenir des éléments chiffrés plus précis. Pour l'instant, cela dépend d'éditeurs de logiciels qui publient certes des rapports extrêmement intéressants mais il est un peu gênant de dépendre du secteur privé pour la justice.

La coopération du secteur public et du secteur privé est prometteuse dans ce domaine mais la justice est parfois un petit peu trop prudente dans cette démarche nouvelle. L'État se voit obligé de travailler avec le secteur privé en raison des dispositifs comme la plate-forme d'interception qui sera mise en place au niveau national – il y a des accords avec *Thales*. Une collaboration, avec des prestataires techniques, etc., doit être menée dans le respect du rôle de chacun.

La Chancellerie devra mettre l'accent sur ce type de travaux. Le Conseil de l'Europe organise des ateliers, mène des conférences d'experts sur la cybercriminalité.

Il faudrait réfléchir à créer de nouveaux outils procéduraux plus rapides au niveau européen. Les commissions rogatoires internationales en matière de cybercriminalité sont très longues à obtenir, très lentes, avec en plus le problème de la traduction. Et pendant ce temps-là, il y a un risque dépérissement des preuves.

Il existe beaucoup de textes pour lesquels il faudrait procéder à une mise à plat avec l'aide de la commission de codification de la Chancellerie. Certains articles devraient être simplifiés, y compris ceux de la loi Godfrain même si elle reste une base très intéressante. Les systèmes ont traversé les années.

La Chancellerie a un rôle d'expertise et de conseil aux juridictions. Il faudrait expliquer ce qu'est un système de traitement automatisé des données, par exemple. Au sujet du système de vidéoprotection, les entreprises ne savent même pas qu'il existe des textes et ne connaissent pas, en l'occurrence, la loi Godfrain.

Les magistrats sont très demandeurs de conseils, de formations. Tout le monde est un peu noyé dans la masse, dans les efforts pour gérer la crise. **De nouvelles problématiques apparaissent comme la monnaie virtuelle.** Il va falloir réglementer sur ce sujet pour encadrer ce dispositif. Il ne s'agit pas véritablement de monnaies, il s'agit plutôt de moyens de transaction.

C'est un droit en devenir et nous sommes en formation continue.

COMPTE RENDU DE L'AUDITION PUBLIQUE DU 19 JUIN 2014 : SÉCURITÉ DES RÉSEAUX NUMÉRIQUES

SOMMAIRE

INTRODUCTION

Mme Anne-Yvonne Le Dain, députée, vice-présidente de l'OPECST

M. Bruno Sido, sénateur, président de l'OPECST

Sécurité des réseaux numériques :
cadre juridique, risques, aspects sociétaux

Mme Isabelle Falque-Pierrotin, présidente de la Commission nationale de l'informatique et des libertés (CNIL)

M. Gilles Babinet, responsable des enjeux de l'économie numérique pour la France (*French Digital Champion*), Commission européenne

QUESTIONS AUX INTERVENANTS

M. Pascal Chauve, conseiller du secrétaire général de la défense et de la sécurité nationale (SGDSN)

Mme Mireille Delmas-Marty, membre de l'Institut de France (Académie des Sciences morales et politiques), professeur honoraire au Collège de France (Études juridiques comparatives et internationalisation du droit)

M. Jean-Dominique Nollet, lieutenant-colonel de la Gendarmerie nationale, chef d'unité de laboratoire de recherche, Centre européen de lutte contre la cybercriminalité (EC3) à Europol

M. Charles Huot, président d'*Aproged*, président du comité éditorial du portail *Alliance Big Data*

Me Christiane Féral-Schuhl, avocat spécialisé en droit de l'informatique et des technologies, ancien bâtonnier du Barreau de Paris

DÉBAT

Sécurité des réseaux numériques : cadre juridique, risques, aspects sociétaux (suite)

Table ronde animée par M. Pierre Lasbordes, ancien député, ancien membre de l'OPECST

M. Bernard Stiegler, philosophe, directeur de l'Institut de recherche et d'innovation du Centre Georges Pompidou (IRI), membre du Conseil national du numérique

M. Maxime Chipoy, responsable des études, UFC-Que-Choisir

M. Jean-Pierre Quémard, président de la commission de normalisation SSI et chef de délégation française à l'*ISO/IEC* JTC1/SC27

M. Philippe Wolf, ingénieur général de l'armement, auteur de nombreux articles et ouvrages sur le numérique

Me Éric Caprioli, docteur en droit, avocat à la Cour d'appel de Paris, vice-président du Club des experts de la sécurité de l'information et du numérique (CESIN)

Me Pierre Desmarais, avocat à la Cour d'appel de Paris, correspondant informatique et libertés, spécialisé dans les questions de sécurité numérique

Mme Valérie Maldonado, chef de service, Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC)

M. Benoît Virole, docteur en psychopathologie, docteur en sciences du langage, membre de l'Observatoire des mondes numériques en sciences humaines (OMNSH)

DÉBAT

CONCLUSIONS

Mme Anne-Yvonne Le Dain, députée, vice-présidente

M. Bruno Sido, sénateur, président

LES ASPECTS NORMATIFS DU RISQUE NUMÉRIQUE (SÉCURITÉ DES RÉSEAUX NUMÉRIQUES)

Introduction

Mme Anne-Yvonne Le Dain, députée, vice-présidente de l'OPECST. – L'Office parlementaire d'évaluation des choix scientifiques et technologiques a été créé en 1983. C'est le seul organe qui soit commun au Sénat et à l'Assemblée nationale. Composé de dix-huit députés et de dix-huit sénateurs, il élabore des rapports sur des thèmes scientifiques et technologiques particulièrement complexes afin de les vulgariser, pour que tous les parlementaires puissent, en peu de temps, être à même de réagir lorsque des projets de loi sont présentés dans ces domaines. C'est en tout cas son acception initiale.

Depuis, la question scientifique et technologique est entrée dans les inquiétudes du monde moderne et beaucoup de commissions, au Sénat ou à l'Assemblée nationale, se saisissent de sujets qui ont une connotation ou une force scientifique.

Ce n'est pas toujours simple. C'est aussi la raison pour laquelle l'Office parlementaire considère qu'il est de son devoir d'être sur tous les champs et de sortir très largement du domaine dans lequel il semblait peut-être s'être spécialisé, à savoir le nucléaire. En trente ans, l'Office a abordé beaucoup de domaines.

Dès l'an dernier, l'Office a organisé une journée sur le risque numérique que nous approfondissons actuellement par un travail de fond conduit par deux parlementaires, le sénateur Bruno Sido et moi-même, sur les grandes questions autour du numérique, entre risques et opportunités, entre France et Europe, entre Europe et monde. C'est une question importante.

C'est à la suite d'une saisine de la commission des affaires économiques du Sénat que l'Office conduit cette étude autour du risque encouru par les entreprises qui utiliseraient sans trop de précaution les moyens numériques actuels. La commission pense en particulier au stockage des données dans les nuages *(cloud computing)*, mais aussi aux composants présents dans les cœurs de réseaux.

Pour traiter de ces thèmes extrêmement techniques, les rapporteurs ont choisi de prendre comme exemples les entreprises du secteur des

télécommunications et celles du secteur de l'énergie, ces deux secteurs étant considérés comme d'importance vitale.

On sent bien également que ces secteurs touchent à de grandes entreprises et à des ETI, mais aussi à des innovations importantes qui peuvent être portées par de très petites entreprises et des entreprises débutantes. Nous sommes en plein dans le champ de la nouvelle économie du XXIe siècle.

En général, chacune des études de l'OPECST donne lieu à une centaine d'auditions. Dans ce cadre, M. Bruno Sido, en tant que président de l'OPECST, et moi-même, en tant que vice-présidente, avons été désignés. Actuellement, nous avons procédé à plus d'une soixantaine d'auditions incluant des visites sur le terrain. Parmi celles-ci, deux journées d'audition publique ouverte à la presse ont été organisées, l'une portant sur l'éducation au numérique et celle d'aujourd'hui qui porte sur le cadre juridique de cette technique, à laquelle vous avez bien voulu participer. Je vous en remercie.

Une troisième journée d'auditions donnera lieu à un dialogue, d'une part, avec les opérateurs d'importance vitale, et, d'autre part, avec les sociétés de sécurité numérique, ce dont je les remercie vivement.

La présente audition est enregistrée en vidéo et figurera, dès les jours prochains, sur les sites de l'Assemblée nationale et du Sénat. Elle fera également l'objet d'un compte rendu qui sera annexé au rapport final.

Comme il a été indiqué à chacun d'entre vous, les interventions d'horizons fort divers seront toutes axées sur la sécurité des réseaux numériques en ce qu'elle concerne les entreprises mais ce sera, à chaque fois, selon les angles d'attaque qui vous sont propres et qui vous caractérisent, selon vous-même, selon l'organisme auquel vous appartenez ou encore en fonction de vos thèmes de recherche privilégiés, selon votre choix et donc votre liberté.

Quant à moi, compte tenu de la grande qualité des intervenants rassemblés aujourd'hui et de l'actualité brûlante de nos débats et de ce sujet qui est très présent dans l'espace public national et européen, j'ai insisté auprès de Mme Axelle Lemaire, secrétaire d'État chargée du numérique, auprès du ministre de l'économie, du redressement productif et du numérique, M. Arnaud Montebourg, pour qu'elle vienne parmi nous à l'occasion de cette journée. Mme Axelle Lemaire nous rejoindra vers 16 heures.

Je vais donner la parole à Mme Isabelle Falque-Pierrotin. Les missions dévolues à la CNIL, qui fut, dès 1978, l'une des premières institutions, non seulement française, européenne, mais mondiale, à travailler sur ces questions-là, ont considérablement évolué. Il s'agit maintenant de les concilier avec celles dont l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est en charge.

Sécurité des réseaux numériques : cadre juridique, risques, aspects sociétaux

Mme Isabelle Falque-Pierrotin, présidente de la Commission nationale de l'informatique et des libertés (CNIL). – À la CNIL, nous avons dressé un constat. Cet univers numérique pose des questions de sécurité extrêmement complexes et un peu nouvelles.

Premièrement, nous sommes face à un écosystème qui fait intervenir de multiples acteurs, avec des relations qui ne sont pas toujours précises entre les prestataires, les acteurs principaux et toute une série d'acteurs qui interviennent derrière. Il y a une forme de **dilution des responsabilités**.

Deuxièmement, dans cet univers où les technologies se renouvellent en permanence, **les questions de sécurité sont sans cesse renouvelées**. Le nuage numérique ou *cloud*, les données massives ou *big data*, les objets connectés ou le *Bring Your Own Device (BYOD)* posent, chacun, une question de sécurité et une manière d'assurer la sécurité qui sont nouvelles.

Troisièmement, **cette culture de l'Internet place l'individu au centre**. C'est à la fois formidable de par les pouvoirs d'actions que cela lui donne, mais en même temps, cela conduit certains d'entre eux à adopter une pratique de contournement. On l'a vu dans des législations qui ne recevaient pas l'approbation de la masse des individus, je pense au téléchargement de musique. Cela peut aussi conduire beaucoup d'individus à se mettre eux-mêmes dans une situation de péril par rapport à leur propre sécurité. Notamment au sein des réseaux sociaux, les individus divulguent beaucoup de données personnelles. Évidemment, cela pose de nouvelles questions de sécurité.

À ces comportements s'ajoute une dimension supplémentaire : l'attractivité des données personnelles. Les données qui sont au cœur de l'économie numérique sont un gisement extrêmement séduisant et attractif pour les entreprises mais aussi pour les gouvernements dans le cadre de la lutte contre le terrorisme ou dans celui de l'espionnage. Cette convoitise vis-à-vis des données renouvelle également les questions de sécurité.

Ces quatre facteurs nous conduisent à rechercher une nouvelle manière de traiter les problèmes de sécurité dans cet univers numérique. Première question : sommes-nous armés pour les traiter ? Je crois que la réponse est oui, à une condition : que nous ayons une réponse qui corresponde à la culture de l'univers auquel nous faisons face. Concrètement, nous devons apporter une réponse de « sécurité en réseau ». En effet, **aucun acteur n'a l'ensemble des clés pour piloter** à lui seul **la sécurité de cet univers.** En revanche, si l'on s'adresse à l'ensemble des acteurs concernés, et que chacun d'entre eux a une action, une responsabilité

particulière en termes de sécurité, alors nous pouvons collectivement garder cet univers sous contrôle, en tout cas au niveau de la sécurité de celui-ci.

Qu'est-ce que signifie avoir une « sécurité en réseau » ? Le premier axe, ce sont les entreprises. Vous l'avez dit, madame Le Dain, c'est le cœur de votre préoccupation d'aujourd'hui. L'objectif est de **responsabiliser ces acteurs** professionnels et ces entreprises, afin qu'ils intègrent dans leur propre fonctionnement cet objectif de garantie de la sécurité des réseaux, et pour nous, à la CNIL, de la sécurité des données personnelles.

Ces acteurs professionnels, nous les connaissons : à travers l'article 34 de notre loi informatique et libertés qui responsabilise en termes de sécurité les responsables de traitement. Ce sont à la fois les opérateurs de réseau et ceux qui offrent des services. Tous ces acteurs professionnels ont la responsabilité des données personnelles qui transitent chez eux ou qu'ils utilisent. Ils doivent en assurer l'intégrité et veiller à ce que l'accès par des tiers auxdites données soit strictement encadré. Dans cet « accès par les tiers », on voit arriver ceux qui convoitent les données à des fins commerciales ou de renseignement.

Cet article 34 est la pierre angulaire de l'enjeu de sécurité au regard de la loi informatique et libertés. Nous l'appliquons de façon uniforme en général mais avec des régimes particuliers liés à certaines catégories de données.

Par exemple, les données de santé font l'objet dans notre législation d'une protection plus forte en termes de sécurité et il existe, notamment, un régime juridique des hébergeurs des données de santé qui doivent être agréés.

On distingue aussi des catégories particulières d'acteurs. Les opérateurs de communications électroniques sont ainsi tenus, depuis 2011, **de notifier les failles de sécurité** (article 34 *bis* de la loi). Cela signifie que celles-ci doivent être signalées dans un délai court à la CNIL, quel que soit le niveau de la faille. Et s'ils ne le font pas, ils encourent des sanctions pénales. Par ailleurs, ces opérateurs ont l'obligation d'informer les personnes de l'existence de cette faille, sauf si celle-ci n'a porté atteinte à aucune donnée personnelle ou qu'ont été prises des mesures pour qu'il n'y ait pas de violation de données personnelles dans le cas où la faille interviendrait. Par exemple, si les données ont été cryptées, il n'y aura pas d'obligation de notification aux personnes même si un tiers y a accès. Les opérateurs ont donc une obligation renforcée en termes de sécurité des données personnelles, par rapport à la responsabilité générale de l'article 34.

Enfin, certaines technologies ou usages font l'objet d'un encadrement spécifique de la CNIL par des recommandations, par exemple, sur le vote électronique ou la carte bancaire sans contact.

Tout cet arsenal est-il efficace ? À ce stade, dans la politique de contrôle que nous menons, et qui ne porte pas spécifiquement sur cette

question de la sécurité, je dirais que nous constatons**, dans la plupart des cas, des manquements en termes de sécurité des traitements**. Même si certains de ces manquements peuvent être aisément corrigés ou révèlent surtout un manque de culture « *privacy* », plutôt qu'une volonté de contourner la loi, ce constat est loin d'être positif.

D'autre part, concernant les failles de sécurité, les opérateurs de réseau ont eu beaucoup de réticences à appliquer cette législation, à tel point que nous avons dû les réunir au début de l'année pour leur adresser le message ferme que cette législation s'appliquait, qu'on la leur expliquait, mais que cela faisait désormais partie de leurs obligations.

J'aurais donc tendance à penser que la prise en compte de ces questions de sécurité est progressive mais lente, même si les outils de conformité existent. Je n'ai pas mentionné les outils pédagogiques que nous développons par ailleurs. Nous travaillons ici en étroite collaboration avec l'ANSSI.

De plus, nous rencontrons des difficultés dans la mobilisation de ces outils. Les sanctions que nous pouvons prononcer, notamment les sanctions pécuniaires, obéissent à une procédure contradictoire assez sophistiquée. Pour qu'il y ait sanction pécuniaire, il faut une mise en demeure préalable. Or, dans le cas des failles de sécurité, lorsque nous sommes saisis, la faille est en général déjà fermée. Donc la mise en demeure ne sert pas à grand-chose.

Au cours de l'année **2013**, selon la société *Symantec*, les failles de sécurité ont augmenté de 62 %, dont **plus de dix failles majeures, c'est-à-dire concernant plus de 10 millions de personnes**. Face à des situations de ce type, dans la plupart des cas, nous ne pouvons au maximum que prononcer un avertissement public. Ce n'est pas satisfaisant.

Comment, dès lors, améliorer le dispositif ? D'abord, nous avons fait des propositions qui ont été prises en compte dans la loi du 17 mars 2014 sur la consommation (loi n° 2014-344 du 17 mars 2014, article 105 modifiant l'article 44 de la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés). Nous avons demandé la possibilité d'opérer des **contrôles en ligne**. Dans le cadre des failles de sécurité, ces contrôles à distance sont extrêmement efficaces.

Ensuite, nous avons fait une proposition à la ministre, Mme Axelle Lemaire, pour que nous puissions prendre **des sanctions sans mise en demeure préalable dans certains cas** très particuliers d'urgence ou de gravité extrême. Notamment lorsqu'on se trouve en présence d'une faille majeure qui doit être très rapidement traitée, nous pourrons ainsi avoir la possibilité d'aller au-delà d'un seul avertissement.

Le règlement européen est un autre élément qui va changer la donne sur la question de la responsabilisation des opérateurs économiques. Il va donner à la sécurité une dimension nouvelle pour deux raisons. Premièrement, **les sous-traitants vont se voir attribuer des responsabilités**

spécifiques au regard de la loi informatique et libertés, au même titre que les responsables de traitement, ce qui n'est pas le cas aujourd'hui. Les sous-traitants sont actuellement soumis à une obligation de sécurité, mais nous ne pouvons prononcer de sanctions que par rapport aux responsables de traitement.

La deuxième avancée du règlement européen est la mise en place de l'*accountability*, c'est-à-dire la **responsabilisation des entreprises** par rapport aux données personnelles, à travers un certain nombre d'instruments internes aux entreprises par lesquels elles doivent démontrer qu'elles appliquent effectivement les principes de la loi informatique et libertés. Par exemple**,** le *Privacy Impact Assessment (PIA)*, **outil d'analyse d'impact,** va les conduire à mener une analyse de risque sur les traitements importants qu'elles mettent en œuvre. Ces *PIAs* peuvent renforcer la responsabilisation des acteurs professionnels.

En conclusion, concernant les acteurs professionnels, je crois que nous disposons des outils et nous les complétons à la marge mais que la prise de conscience ne se fait pas aussi vite qu'on pourrait le souhaiter.

La deuxième cible, ce sont les individus. J'ai compris en vous écoutant, madame Le Dain, qu'ils n'étaient pas au centre des préoccupations de votre étude. Mais, en réalité, l'individu est un personnage central dans la sécurité. On sait bien qu'**une partie des failles de sécurité vient des individus eux-mêmes, notamment au sein de l'entreprise**. Il est donc absolument essentiel de faire passer des messages auprès d'eux. À cet égard, je vois deux leviers.

Le premier levier consiste à développer une culture de la sécurité auprès des individus, montrant l'interdépendance nouvelle entre les uns et les autres à travers cette interconnexion généralisée, et les réflexes nouveaux qu'il faut avoir. C'est l'une des briques très importantes au sein du programme général d'éducation au numérique que nous promouvons avec d'autres. La CNIL a en effet pris l'initiative de construire un collectif visant à **faire reconnaître l'éducation au numérique comme une grande cause nationale en 2014**. Il faut faire passer un message général auprès des individus en leur disant qu'ils sont, désormais, acteurs de la sécurité et qu'ils doivent en être conscients.

Le deuxième levier, probablement plus positif, est de dire à l'individu que, par rapport à ces atteintes à la sécurité, notamment relatives à ses données, il peut, lui-même, améliorer la maîtrise de ses données personnelles et donc celle de sa sécurité, en mobilisant les droits qui sont les siens, au regard de la loi informatique et libertés ou du futur projet de règlement européen.

Par exemple, le droit à l'oubli qui va être consacré par le projet de règlement européen. Il s'agit de la capacité qu'a l'individu de maîtriser le

devenir de sa donnée et c'est aussi un moyen d'assurer la sécurité de ses données par rapport à d'éventuelles captations par des tiers.

Le droit à l'oubli vient d'être renforcé par un arrêt de la Cour de justice de l'Union européenne qui a affirmé un droit complémentaire qui est le droit au déréférencement, c'est-à-dire la possibilité pour chaque individu, non seulement d'aller voir le site auprès duquel l'information a été initialement publiée, mais de s'adresser aux moteurs de recherche pour demander le déréférencement de sa donnée dans certaines conditions. C'est la première fois que ce droit est affirmé. C'est un élément de sécurisation, par l'individu lui-même, de ses données.

Un autre exemple est le droit à la portabilité des données. Ce droit n'existe pas actuellement en droit français, mais il existera en application du projet de règlement européen. Ce droit à la portabilité offre aux individus la possibilité d'aller voir la plate-forme, le vendeur auprès duquel il a déposé toute une série de données personnelles, pour récupérer celles-ci et les porter ailleurs. Là aussi, c'est un moyen pour l'individu de maîtriser ses données et d'en assurer lui-même la sécurité.

Concernant la responsabilisation des individus, toutes les nouvelles initiatives qui se développent aujourd'hui vont permettre à l'individu de récupérer ses données pour les valoriser d'une autre façon et pour profiter d'un certain nombre de nouveaux services. Je pense, par exemple, au projet *MesInfos* (fing.org). Tous ces services nouveaux visent à placer l'individu dans la chaîne de sécurité, en lui faisant passer le message suivant : **vous êtes les acteurs de votre propre sécurité**.

La troisième dimension est collective. Les enjeux de sécurité sont systémiques. Bien que la CNIL soit moins directement concernée par cet aspect, l'affaire *Prism* a révélé que nous sommes face à une infrastructure générale d'information qui conduit à automatiser la surveillance, de manière systématique et indifférenciée, de tous les citoyens européens à travers l'usage quotidien qu'ils font des plates-formes. Pour des raisons de lutte contre le terrorisme, nous dit-on. Ce dispositif de surveillance révèle la complexité des partenariats entre les acteurs publics et privés, mais, au fur et à mesure que s'égrènent les révélations de M. Snowden, nous apprenons que **la question ne concerne pas que l'Europe et les États-Unis d'Amérique, mais aussi ce qui se passe chez chacun**.

Par rapport à ces révélations, la CNIL pose deux questions : comment assurons-nous la maîtrise de notre gisement informationnel, c'est-à-dire les données de nos concitoyens européens, par rapport à des tiers étrangers ? Comment assurons-nous, sur ce gisement de données informationnelles, la protection des libertés de nos concitoyens français ou européens, y compris vis-à-vis des services de renseignement du pays de chacun ?

En tant qu'autorité en charge de la protection des données personnelles, la CNIL s'est intéressée à ces deux objectifs. Des réponses commencent à se mettre en place. Elles sont complexes et pas encore conclusives.

Lors d'une audition qui s'est tenue quelque temps après l'affaire *Prism*, nous avions proposé au Parlement européen une première réponse, qui a été reprise par les parlementaires. C'est l'introduction, dans le projet de règlement, de l'article 43a, qui dit la chose suivante : dès qu'une autorité administrative étrangère veut avoir accès à des données concernant des citoyens européens, elle doit, d'une manière ou d'une autre, avoir l'accord d'une autorité nationale européenne. Un tel accord reste à définir, mais c'est un verrou car on ne peut plus, dès lors, aspirer, sans rendre des comptes, le gisement de données de citoyens européens pour des raisons de renseignement, de lutte contre la corruption, de contrôle des données passagers, etc. On ne le sait pas, mais, en réalité, beaucoup de finalités ont déjà conduit à des demandes d'accès de ce type. Or, cela ne peut être fait sans qu'il y ait une négociation et un cadre qui soient élaborés entre l'autorité étrangère qui demande l'accès et les autorités nationales européennes concernées. Ce débat est assez technique, mais essentiel car il peut permettre de « glisser un pied dans la porte » si je puis dire.

Faut-il aller au-delà et imaginer une loi de blocage au niveau européen ? Il faut y réfléchir. On sent bien qu'on ne peut pas continuer à laisser se mettre en place une surveillance généralisée, systématique et automatisée, d'autant qu'un deuxième élément est intervenu. L'arrêt de la Cour de justice de l'Union européenne du 8 avril 2014 a invalidé la directive *data retention* relative à la conservation des données de connexion au regard de la charte des droits fondamentaux – articles 7 et 8. En résumé, les juges disent qu'il existe une forme de disproportion dans le dispositif qui a été adopté. Le rapport d'analyse et d'évaluation qui a été rédigé par la Commission quelques mois avant, avait également conclu que ce dispositif n'était pas optimum.

On voit bien que, vis-à-vis de tiers extérieurs à l'Union, il faut apporter des réponses et affirmer la souveraineté numérique de l'Europe. Mais, d'une façon générale, des accès aussi massifs, indifférenciés et automatisés, concernant des citoyens européens, y compris par leurs propres autorités de renseignement, ne sont pas acceptables.

Cela a conduit la CNIL à faire une proposition aux autorités nationales françaises. Aujourd'hui, les fichiers de renseignement ne font l'objet d'aucun contrôle externe de qui que ce soit. Cela n'est pas sain, compte tenu de l'ampleur de la surveillance qu'a révélée l'affaire *Prism*. Désormais, il est nécessaire d'apporter des garanties aux citoyens sur l'existence d'un cadre, proportionné, de ladite surveillance. **Nous avons proposé aux pouvoirs publics que la CNIL puisse être chargée du contrôle des fichiers de souveraineté** dans certaines conditions, notamment dans des

conditions d'habilitation « secret défense », avec un collège spécifique qui existe déjà à la CNIL à travers le droit d'accès indirect. Ces fichiers de souveraineté sont totalement dérogatoires au regard de notre loi par rapport aux autres fichiers de police. Nous demandons que ce collège spécialisé de la CNIL puisse contrôler non pas l'activité des services de renseignement, mais le fait que ces fichiers fonctionnent dans le respect du droit des personnes.

Je terminerai par une dernière proposition pour améliorer cette « sécurité en réseau ». La CNIL travaille avec d'autres autorités publiques : l'ANSSI, l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), *Signal Spam* et toute une série d'autorités avec lesquelles nous avons signé des conventions sur ces questions de sécurité pour travailler ensemble. Il me semble que nous gagnerions collectivement beaucoup si, sur cette question de la sécurité, nous allions peut-être plus loin à travers un groupe de contact, en tout cas des échanges continus entre les acteurs publics concernés, sur ces questions qui sont d'intérêt commun.

M. Bruno Sido, président de l'OPECST. – Merci madame la présidente pour l'éclairage nouveau que vous avez su donner à votre présentation. Je suppose qu'elle va donner lieu à des questions après l'intervention de M. Gilles Babinet.

Mme Le Dain et moi-même nous sommes rendus à Bruxelles la semaine dernière pour une journée d'entretien avec des responsables de la sécurité numérique. Il nous est apparu que l'imbrication des normes juridiques et techniques internationales, européennes et nationales, avait atteint un certain degré de complexité – c'est un euphémisme –, peut-être au détriment de leur efficacité.

Pour autant, des solutions ne sont pas davantage à attendre d'un surcroît de normes que d'une simplification de celles-ci. Elles viendront plutôt d'une réflexion d'ampleur sur tous les changements de mentalité et de comportements que suppose le recours généralisé à l'usage des outils du numérique sur des réseaux dont les failles techniques viennent souvent aggraver les failles humaines.

M. Gilles Babinet, responsable des enjeux de l'économie numérique pour la France *(French Digital Champion)*, Commission européenne. – Ce débat d'aujourd'hui est essentiel. Je vais vous faire des commentaires directement liés aux enjeux de sécurité, en particulier sur ce qui se fait au niveau européen, puis je ferai des commentaires plus généraux sur les sujets de la donnée.

En matière de sécurité, plusieurs initiatives existent ou ont existé au niveau européen. Ces éléments de normalisation peuvent être le fait directement de l'Europe, ou le fait d'agences de normalisation qui n'y sont pas directement rattachées, mais dont l'impact sur la façon de structurer les

réseaux est très conséquent. Je pense à l'*European Telecommunications Standards Institute (ETSI)* par exemple. Ils peuvent aussi être le fait de la correspondance entre des organismes techniques liés à la création de formats de sécurité sur Internet en particulier. Ces travaux sont principalement techniques, ils n'ont pas de nature à proprement parler juridique (recherche d'algorithme, de modèles d'échanges les plus performants entre les systèmes au sens large).

D'une façon générale, l'Europe se réveille un peu en retard en matière de sécurité. Les grandes sociétés de conseil font assez régulièrement des comparaisons en matière de processus de sécurité dans les entreprises, je pense à l'étude de *Capgemini*, par exemple, il y a deux ans. Elles montrent clairement que **les sociétés américaines accordent plus d'attention à la sécurité que les sociétés européennes**. Et au sein de l'Europe, il y a de grandes différences entre les pays.

Malheureusement, la France n'a pas investi beaucoup, même s'il y a un rattrapage dans ce domaine. J'en tiens pour preuve un exercice que j'ai lancé avec le journal *Les Échos* il y a deux mois, qui consiste à mesurer l'agilité numérique des entreprises du CAC 40. Le sondage comporte une centaine de questions et à ce jour, j'ai pris connaissance de vingt-six formulaires. Sans révéler de noms, je peux vous dire que **la prise de conscience est extrêmement récente** et qu'elle se traduit par **un accroissement important des budgets consacrés à la sécurité**. Approximativement, pour les entreprises dont nous avons dépouillé les résultats, la croissance des budgets en matière de sécurité entre 2012 et 2013 est de l'ordre de 40 %. Le budget moyen se situe aux alentours de 70 millions d'euros. Ce sont des montants importants qui sont affectés à la fois aux processus technologiques et aux formations des cadres dirigeants, des cadres intermédiaires et des équipes en général.

Deux affaires publiques, que l'on peut évoquer, ont réveillé les consciences puisque, semble-t-il, il y a eu des fuites importantes au sein d'*Airbus* et d'*Areva*, alors qu'une attention forte était donnée à la sécurité. En tout cas, dans l'une de ces deux entreprises, ce n'est pas en soi les processus techniques qui ont failli, mais une **formation insuffisante des équipes** qui n'étaient pas éveillées au risque de faille dans la sécurité.

À l'échelle européenne, je peux également vous dire qu'il y a la volonté d'une sorte de souveraineté de la sécurité européenne. Mme Neelie Kroes s'est exprimée à cet égard, elle y est sensible et pense qu'il faut absolument une coordination européenne à cet égard. Au-delà, il existe des financements européens qui sont affectés à une trentaine de projets, dont quelques-uns ont une taille significative.

Je pense en particulier au financement des réseaux quantiques. Ceux-ci ont une caractéristique : **sur la partie transport, ils sont impossibles à espionner**, c'est-à-dire que l'on ne peut pas extraire de la donnée sans que

ce soit visible dans le réseau. Les travaux qui sont menés à cet égard sont assez prometteurs. Cela ne résout pas tout, parce qu'il peut y avoir des failles humaines ou des failles de traitement. Je ne parle pas d'ordinateur quantique, mais juste de transmission de données. Mme Neelie Kroes s'est encore récemment exprimée sur ce sujet. C'est intéressant de voir que l'Europe peut être chef de file dans ce domaine, c'est ce qui semble être le cas aujourd'hui.

Je ne suis pas un spécialiste de *Prism*. Je lis la même chose que vous dans la presse et je me garderai bien de faire des commentaires de comptoir. En revanche, sur l'accord commercial transatlantique TAFTA *(Trans-Atlantic Free Trade Agreement*), je peux vous dire objectivement qu'il a été très mal vécu au sein de la Commission européenne, laquelle l'a perçu comme une trahison. D'ailleurs, cela a ralenti les discussions. Et sans connaître aucunement ce qui se dit en matière de traité transatlantique pour les données, puisque par définition ces négociations sont secrètes, je crois savoir que cela a permis aux Européens d'être beaucoup plus attentifs à cette notion et donc assez exigeants.

Je voudrais aussi vous dire que depuis l'affaire *Prism*, des initiatives sont prises par différents pays. En particulier, l'initiative allemande me semble assez intéressante à certains égards. Elle comporte plusieurs aspects.

Il y a d'abord **cette idée selon laquelle il faut que les données soient localisées dans des pays européens. Je trouve cette initiative infondée. Cela n'a pas de sens au plan technique**. Ce qui est important, c'est la sécurité que l'on assure à ces données et la façon dont on les traite. La localisation technique des données n'a aucun sens. Je peux vous dire que, dans bien des cas, les administrateurs des nuages numériques (*clouds)* ont eux-mêmes du mal à savoir où se trouvent les données. Pour des raisons techniques de sécurité des données, mais aussi pour des besoins de performance, ces données sont répliquées. Dans certaines grandes entreprises, les expériences ont montré que **les mêmes données sont localisées dans plus de trente endroits à la fois**. De fait, imposer une localisation géographique, cela créerait, d'une part, des contraintes supplémentaires dans la gestion de ces données, et, d'autre part, cela limiterait la performance des réseaux et donc des acteurs propriétaires de ces données.

Le nuage numérique européen est une initiative très populaire dont on entend beaucoup parler. Je regrette que l'argent investi par la France dans cette idée de « nuage souverain » n'ait pas été investi en sécurité des données. Cela m'aurait semblé beaucoup plus pertinent. Je me suis déjà exprimé à ce titre, j'en profite pour le redire.

Les Allemands ont également pris l'initiative d'émettre leurs normes de sécurité. Ils ont recommandé que ce soit une norme nationale largement répandue. J'ai émis exactement la même idée auprès du ministère du redressement productif. J'aurais beaucoup apprécié que ce soit une

norme européenne, mais **il est possible de créer, ou en tout cas d'utiliser les normes existantes « adaptées »**, pour faire en sorte que ce soient des normes européennes ou nationales et qu'elles soient très sûres.

On sait, par exemple, qu'il y a des failles très importantes dans le *SSL*, une norme massivement utilisée et que l'on continue malgré tout à utiliser. Comme c'est une norme vieillissante, il a tendance à disparaître, mais c'est une norme percée qui continue à être utilisée.

Voilà les commentaires que je voulais vous faire sur ce qui se passe en Europe. D'une façon plus générale, et comme vient de le dire Mme Falque-Pierrotin, tout cela repose très largement sur le droit, un droit qui soit le plus constant possible et dont l'assiette géographique soit la plus large possible.

Il faut garder à l'esprit deux modèles anthropologiques qui s'affrontent. Le modèle anglo-saxon, une culture de la *common law* facilite à mon sens très largement l'expérimentation. Il considère que l'innovation est une notion intrinsèquement prioritaire, il faut d'abord expérimenter et on verra après. Bien que j'aie de très nombreuses critiques à son égard, c'est le modèle qui prédomine dans les *GAFA* (*Google*, *Amazon*, *Facebook*, *Apple*). Le modèle tente un tas de choses et il essaie de préserver une contrepartie implicite, c'est-à-dire qu'on vous rend un service de la plus grande valeur, souvent gratuitement, et en contrepartie, vous acceptez les conditions. On considère que votre droit, c'est de ne plus les accepter. Évidemment, on peut juger cela assez inégal. Il n'empêche qu'aujourd'hui des milliards de gens acceptent ce contrat implicite sous cette forme.

Cela doit nous faire réfléchir. Sans vouloir défendre nécessairement ce modèle anglo-saxon, je pense que le modèle qui consiste à avoir une régulation *ex ante*, *a priori*, est problématique dans certains cas, dans la mesure où certaines sociétés vont chercher à s'en affranchir. J'ai été surpris, dans le cadre des auditions que j'ai menées sur le CAC 40, qu'un certain nombre de sociétés m'avouent avoir décidé d'héberger leurs données en dehors de l'Europe, voire de les faire héberger avec une sorte d'isolation juridique, pour s'affranchir des contraintes de régulation européenne. C'est quand même lié aussi à des enjeux de sécurité et cela nous pousse à y réfléchir.

Au-delà, j'observe que tous ces principes de régulation sont jugés éminemment complexes et ils sont confiés à des autorités administratives. Il y a une difficulté à avoir un débat citoyen de bonne qualité sur ce sujet. Lorsque vous êtes dans des zones extrêmement exploratoires et innovantes, le risque est d'avoir une régulation mal calée, qui finalement impacte la capacité d'innovation ou même d'inclusion sociale des nations.

Je pense en particulier au système de santé. Les systèmes de santé numériques recèlent des opportunités extraordinaires. Je ne cesse de le dire à une époque où les finances publiques sont en grand péril. On devrait

accélérer notre mutation vers ce système de santé. Mais nous sommes tous conscients qu'il comporte également des risques très importants pour les citoyens. Pour caricaturer, une société d'assurance qui découvrirait dans un traitement de données que quelqu'un va avoir un cancer n'a aucun intérêt objectif à l'assurer. Cela est bien compris par tous. Pour autant, les croisements de données ont des capacités prédictives, des capacités d'augmentation de la qualité de prescription, de diagnostic, qui sont absolument incroyables. J'écris actuellement un livre sur ce sujet. Je pense qu'une des raisons qui ont ralenti notre capacité à faire émerger une médecine digitale du XXIe siècle, c'est un *a priori* qui consiste à croire que l'on ne peut rien faire sans que la régulation soit parfaitement calée.

Le risque, qui est à mon sens aujourd'hui avéré, c'est finalement que les gens en viennent à confier leurs données à *Apple* par exemple, lequel vient de faire une annonce en ce sens. La qualité et la capacité de traitement de ces sociétés vont devenir tellement importantes à court terme, en quelques années, qu'il est probable que toute cette partie de traitement et de diagnostic soit progressivement extraite du système de santé publique pour être confiée à des acteurs privés. Ceux-ci vont récupérer des quantités de données incroyables qui seront affranchies dans une certaine mesure du droit européen parce que ce sera une exigence citoyenne. Les citoyens vont vouloir utiliser ces services. Il y a là quelque chose qui devrait nous pousser à réfléchir en matière de sécurité. Toutes ces données qui partent à l'extérieur des institutions et des entreprises européennes, c'est finalement une perte de souveraineté.

Je finirai par un mot sur le droit à l'oubli, qui a été abordé. Selon l'arrêté de la Cour de justice de l'Union européenne, ce droit donne la possibilité de modifier les données vous concernant. Là aussi, j'ai beaucoup d'inquiétudes. J'ai rencontré une association d'archivistes qui m'a dit que, dans une certaine mesure, c'est une **possibilité de réécriture de l'histoire**. Évidemment, je me place avant tout du côté des citoyens et des individus, mais je pense que, dans bien des cas, des gens qui ont été justement critiqués pourraient demander la modification des données qui les regardent.

De mon point de vue, cela reflète malgré tout un manque d'agilité numérique des institutions en général qui ont du mal à comprendre les enjeux. Finalement, il me semble que l'ensemble de la régulation et l'harmonisation de la régulation ne doivent pas passer nécessairement par des analyses techniques, mais plus par des analyses éthiques et d'usages en général. Cela est également vrai dans le domaine de la sécurité, où **ce n'est pas la technologie qui résout les problèmes, mais davantage la formation des gens**.

Pour conclure, je dirais qu'**il faut accélérer la prise de conscience à l'égard de l'ensemble de cette formidable révolution digitale**. C'est le point principal de mon intervention. C'est la seule façon pour accroître la sécurité

et finalement, pour arriver à l'émergence d'une Europe numérique et l'inclusion citoyenne dans cette nouvelle ère.

Questions aux intervenants

M. Bruno Sido. – Je vous remercie pour les éclaircissements européens que vous nous avez apportés et l'annonce de nouvelles perspectives qui, je l'espère, apporteront des solutions pragmatiques dans les meilleurs délais.

Parallèlement, la question de la place du numérique dans les négociations du nouveau traité de partenariat transatlantique se pose, ainsi que celle du rythme de négociation de ce traité par rapport à l'élaboration du règlement européen annoncé.

Nous allons maintenant entamer un bref débat à partir des questions que les autres intervenants de la matinée voudront bien adresser à Mme Isabelle Falque-Pierrotin et à M. Gilles Babinet.

Mme Anne-Yvonne Le Dain. – Je serai un peu plus incisive. Je souhaiterais demander à Mme Falque-Pierrotin comment elle réagit aux propos de M. Gilles Babinet.

Mme Isabelle Falque-Pierrotin. – Je partage ce qui a été dit sur l'insuffisante prise en compte de ces questions de sécurité globalement par la sphère économique française. Cette prise en compte est très récente et insuffisante jusqu'à maintenant.

Sur la localisation des serveurs, je crois effectivement que, **sur un plan technique, cela n'a pas grand sens**. C'est d'ailleurs un élément qui est dans l'arrêt de la Cour de justice de Luxembourg sur les données puisque la Cour dit que les données des opérateurs de communications devraient être hébergées en Europe. Pour ma part, je crois que, sur le plan de la protection des données personnelles, imposer l'obligation de localiser les serveurs en Europe n'apporte pas de protection. En réalité, **la question est de savoir qui opère lesdits serveurs**. Dès lors que c'est par une société qui est en fait soumise au droit américain, directement par une société américaine ou une filiale, que le serveur soit basé en Europe, à Paris ou aux États-Unis, les données sont accessibles par la *NSA* ou par une autorité publique américaine. Donc **la localisation n'apporte rien, si ce n'est, par rapport au régulateur que nous sommes, qu'elle permet des contrôles sur place** qui sinon n'existent pas. Symboliquement et peut-être aussi opérationnellement, on peut se rendre sur place pour voir les *logs* et les fichiers. Mais je ne suis pas sûre que, sur le plan de la protection de notre gisement informationnel par rapport à des accès qui seraient demandés, au titre de lois étrangères, par des autorités ou des acteurs étrangers, ce soit en imposant la localisation en Europe que l'on va changer quoi que ce soit.

Peut-être que pour certaines données, on peut avoir un service à valeur ajoutée dans lequel on garantit que la donnée reste totalement sur le territoire national, je pense à la donnée de santé. Mais, sur le fait d'en faire une obligation générale, je partage la position de M. Gilles Babinet. Cela ne me paraît pas décisif.

Sur les autres propos, je n'ai pas de commentaires. Sur l'opposition entre les deux systèmes, dire qu'une régulation mal calée empêche l'innovation, c'est vrai, c'est un propos de bon sens. Mais il est vrai aussi que l'autorégulation débridée conduit à une impasse. Aux États-Unis d'Amérique, montent de plus en plus, de la part de la société civile, des demandes au titre de la protection des données auprès de la *Federal Trade Commission (FTC)* et d'autres autorités publiques américaines. On ne peut pas utiliser de façon aussi excessive que le droit américain, à certains égards, le permet aujourd'hui, les données des citoyens américains. Chacun des deux systèmes a ses limites. En Europe, nous sommes marqués par une tradition de régulation. C'est notre force, mais aussi notre faiblesse, si elle est mal mise en œuvre. La question est donc de savoir comment moderniser cette approche de la régulation pour qu'elle soit raisonnable et non pas handicapante par rapport à l'innovation.

En même temps, cette approche nous donne un avantage compétitif par rapport aux acteurs étrangers, qui est considérable. On va le ressentir de plus en plus au fur et à mesure que se mettra en place la maturité des citoyens et des consommateurs européens. Les études récentes montrent que ce qui s'est passé avec *Prism* a cristallisé un certain nombre d'interrogations que se posent les consommateurs et les citoyens. Il y a des stratégies de contournement, de dissimulation de leur identité, qui commencent à se mettre en place. Toutes les études sur le sujet le montrent. Les consommateurs et les citoyens ont des attentes sur les garanties qu'on peut leur apporter en termes de protection des données personnelles. Donc, **profitons de notre tradition de régulation, faisons-en une arme de conquête par rapport aux acteurs étrangers**, consolidons la démarche européenne, puisque c'est au niveau européen, à l'occasion du projet de règlement, que l'on doit le faire et alors on pourra se battre d'une façon équilibrée avec ces *GAFA* et tous les autres acteurs du numérique.

Nous devons cesser de nous fragiliser nous-mêmes. Et nous moderniser, nous hybrider avec les solutions des autres, d'une façon réaliste, et si on peut emprunter aux autres, notamment à travers l'*accountability*, cette approche beaucoup plus pragmatique, je crois que c'est très positif pour la régulation européenne. Mais, de grâce, arrêtons de considérer que nous sommes les mauvais élèves de la classe ! Ce n'est pas vrai. Simplement nous nous battons avec nos armes à nous.

Mme Anne-Yvonne Le Dain. – Monsieur Babinet, une réponse ?

M. Gilles Babinet. – Nous avons chacun nos points de vue et avons l'occasion d'en débattre. Nous ne sommes pas d'accord sur tout, mais ce qui compte, c'est que nous en débattions. Je n'ai pas grand-chose à ajouter.

Mme Mireille Delmas-Marty, membre de l'Institut de France (Académie des Sciences morales et politiques), professeur honoraire au Collège de France (Études juridiques comparatives et internationalisation du droit). – Je voudrais rebondir sur les propos de Mme Falque-Pierrotin à propos de l'articulation entre l'autorégulation et la régulation. Vous avez parlé d'hybridation. En fait, on a besoin des deux. On peut l'exprimer aussi en termes de *soft law* et *hard law*. **On a besoin d'un droit souple et d'un droit dur.** Mais concrètement, comment bâtir cette articulation ? Comme répartir dans les contentieux ce qui relève de l'autorégulation et de la régulation ? Si je suis tout à fait d'accord avec l'objectif, je ne vois pas comment concrètement le rationaliser un petit peu.

Vous avez donné un exemple qui m'a frappé au sujet de la communication des données. Vous avez dit qu'un accord a été négocié entre les autorités nationales de régulation, mais on aurait besoin d'une loi de blocage. Autrement dit, on est dans la *soft law*, on aurait besoin de *hard law*. Mais y a-t-il des critères sous-jacents qui commandent la répartition entre les deux processus ?

Mme Isabelle Falque-Pierrotin. – Je peux vous donner l'exemple de la Fédération des industries électriques, électroniques et de communication. La FIEEC a souhaité développer tout une série d'innovations autour du compteur intelligent, le nouveau compteur gris dans les maisons qui va enregistrer de façon beaucoup plus fine les données de consommation électrique, ce qui apporte toute une série de services. Les gestionnaires de réseaux électriques vont pouvoir optimiser la charge du réseau, les services pour le consommateur seront optimisés et vont permettre de diminuer la facture, et peut-être d'autres types de services seront-ils élaborés.

Les industriels nous ont sollicités pour développer ce compteur, mais en même temps, ils avaient un peu peur que cette innovation soit mal ressentie par nos concitoyens qui y verraient plutôt l'installation d'une sorte de « mouchard » chez eux, capable de dire que la consommation a augmenté, qu'ils sont trois et non plus deux, ou, c'est curieux qu'ils prennent des bains à deux heures du matin, d'ailleurs ils se promènent beaucoup à l'intérieur de leur maison…

Dans le *big data* médical, les capteurs font partie des éléments qui pourraient permettre de déceler les troubles de l'Alzheimer. On sent bien que ces objets ne sont pas totalement neutres. Et donc, les industriels ont souhaité bâtir avec la CNIL des scénarios d'innovation, intégrant, dans la mesure du possible, les questions informatique et libertés qu'on aurait à se poser. Ils viennent d'être rendus publics. Pendant neuf mois, nous avons élaboré avec eux des scénarios d'innovation qui correspondent à leurs

besoins, en intégrant le plus en amont possible la préoccupation informatique et libertés.

Typiquement, c'est une forme d'hybridation. Des principes généraux se traduisent ensuite concrètement par une sorte de **code de conduite** que souhaite adopter une profession, de façon extrêmement fine et plus appliquée, afin de décliner les dix principes dans des usages professionnels. De plus en plus, nous essayons de développer cette approche avec les acteurs professionnels. Avec cette sorte d'ombrelle qui a été négociée avec eux, nous pouvons entrer dans la finesse de leurs préoccupations de métiers à partir de nos principes. C'est une forme d'autorégulation encadrée sous l'œil du régulateur.

Nous avons également une réflexion sur une autre approche qui consiste à **faire appel à des tiers certificateurs** sur un certain nombre de points. Elle est expérimentée sur des flux internationaux de données. Le régulateur fixe des principes, des référentiels, et ce sont des acteurs externes privés qui gèrent l'opérationnel relatif à ces référentiels.

Il y a donc différentes manières de combiner l'action d'un régulateur, et en même temps, de laisser aux acteurs privés la possibilité de pouvoir développer des offres en parallèle.

M. Gilles Babinet. – Je veux bien répondre car je crois que cela cristallise notre principal point de désaccord. Sur cette affaire de compteurs, les sociétés qui vous ont consultés sont probablement *ERDF* ou ces grandes entreprises. Mais une jeune entreprise ne ferait jamais cela, et même, elle ne peut pas, sur un préalable d'enjeux juridiques, se lancer dans un projet d'innovation. Pour être dans ce milieu depuis longtemps, consubstantiellement, un entrepreneur lançant une nouvelle entreprise essaie des choses. Vous prenez des risques sans savoir très bien sur quoi vous allez tomber. Avec la donnée et les données massives ou *big data* en particulier, vous ne savez qu'assez rarement ce que vous allez trouver. Vous lancez des processus de traitement de données et vous pouvez trouver que des gens sont atteints de la maladie d'Alzheimer, par exemple. Dans le domaine, c'est tout à fait étonnant.

Un autre exemple m'a été donné par des chercheurs de *Bellevue Hospital*. À partir d'un traitement des flux des réseaux sociaux, assez curieusement, ils parviennent à détecter les pathologies, juste en lisant des informations non médicales. Ils pensaient qu'il était possible, sans l'avoir démontré, de voir dans les réseaux sociaux si l'on a les lobes attachés ou pas. 20 % des gens ont des lobes attachés. C'est un marqueur épigénétique fort qui est lié à des éléments de renforcement ou de faiblesse par rapport à certaines maladies. Il est donc probable que, très facilement, à travers les réseaux sociaux, on soit capable d'identifier des résistances, ou au contraire des faiblesses particulières. Vous ne les détectez pas *a priori*. Vous devez

lancer des expérimentations de tous types pour pouvoir soudainement vous rendre compte que cela fonctionne ou pas.

Cela m'importe beaucoup. Je crois que l'Europe est en train de prendre du retard. On entre dans une nouvelle ère avec des paradigmes qui sont assez différents. Je constate que **chaque révolution industrielle a amené son droit. La première a amené le code civil, la seconde le droit du travail, et celle-là amènera un droit de la donnée**. Je ne suis pas contre la régulation. Au contraire, je pense qu'on va avoir énormément de régulation à cet égard et qu'on va vers une période de surrégulation. Mais, dans la mesure où l'on n'a pas cette agilité numérique pour comprendre ce paradigme, en particulier au sein de l'ensemble des organes qui participent à la régulation de la vie de la cité, je pense que c'est assez risqué.

Encore un exemple. Aux États-Unis, les fermiers commencent à confier leurs données à des sociétés tierces qui leur disent où arroser, où mettre des engrais, etc. *Monsanto* a d'ailleurs racheté une société de traitement de *big data* dans le domaine agricole. **Les fermiers américains se sont rendu compte qu'ils allaient devenir des sous-traitants de l'industrie de la donnée**, notamment de *Monsanto* qui allait expurger de la valeur. Comme les associations de fermiers américains ont la chance d'être fédérées, elles se sont réunies et ont édicté **un code de bonnes conduites** qu'elles ont opposé à l'ensemble des sociétés en leur disant : soit vous respectez ce code, soit on demandera à nos membres de ne plus donner leurs données. Et cela a fonctionné. Le code est en discussion en permanence. Les acteurs du traitement des données consultent ces associations et il y a débat.

Je ne dis pas, qu'à terme, il ne faudra pas une régulation en la matière. Je dis simplement qu'il faut absolument faire en sorte que l'Europe ne rate pas une marche qui restera dans l'histoire. C'est mon inquiétude et c'est la raison de ma venue ici ce matin. Ce préalable d'innovation doit être, à mon avis, important.

Je vais vous donner un autre exemple qui n'est pas couvert par la régulation sur les enjeux des *machine learning*, des techniques qui trouvent des réponses à partir de signaux extrêmement variés sans avoir besoin d'identifier les gens. J'ai vu des expérimentations absolument incroyables de *machine learning*. Par exemple, je peux détecter qu'à tous les barbus qui ont une voiture rouge, sans connaître leur nom, je vais pouvoir montrer des publicités de rasoir quand ils vont passer dans la rue. C'est très efficace, je l'ai vu, et dans ce domaine, la régulation est complètement perdue.

Même si ce n'est pas dans la culture du droit continental, je pense que **le débat citoyen est un préalable indispensable à l'émergence de cette nouvelle forme de droit**. Sinon, on court le risque de laisser l'Europe durablement derrière.

Mme Anne-Yvonne Le Dain. – Voilà une discussion qui est ferme, très claire et éclairante pour nous, parlementaires et législateurs. Maintenant,

la question est de savoir comment on sort de cette situation, ce qu'on fait, ce qu'on construit, ce qu'on décide, dans quels délais et avec quelles motivations. Tout cela est sur la table. L'une et l'autre. Vous l'avez remarquablement bien exposé. En ce qui me concerne, j'ai appris des choses et découvert un mode de pensée que je ne soupçonnais pas.

Mme Isabelle Falque-Pierrotin. – Puisqu'il s'agit du débat citoyen, nous sommes bien tous d'accord sur le fait qu'il faut passer à l'échelle supérieure pour que collectivement, au plan national ou européen, on entre dans ce nouvel univers. Je partage entièrement cet objectif.

Je voudrais juste pointer ce qui a été dit sur l'expérimentation. L'expérimentation peut-elle tout justifier ? C'est un sujet très intéressant de débat collectif. Nous parlons de données. Effectivement, recenser tous les hommes barbus vêtus d'un pantalon rouge qui se présentent à tel endroit… on ne voit pas. Mais si c'est ce principe d'expérimentation qui justifie tout, je m'inquiète. Et ce n'est pas un propos conservateur. L'histoire a montré que l'expérimentation pouvait conduire à des choses épouvantables. **L'expérimentation ne peut pas s'affranchir de tout.** Sur un plan humaniste, ce n'est pas acceptable. Ce n'est pas parce qu'il n'est question que de données qu'on peut le faire. Un débat citoyen sur l'ensemble de ces questions me semble nécessaire, en particulier sur cette question de l'expérimentation, parce qu'elle cristallise beaucoup des tabous que l'on veut mettre ou ne pas mettre dans cet univers numérique.

Mme Anne-Yvonne Le Dain. – Je vous remercie tous les deux de votre venue. Je crois que nous serons appelés à nous revoir.

M. Bruno Sido. – M. Pascal Chauve, je crois savoir que la récente loi de programmation militaire et ses décrets d'application sont au cœur de vos préoccupations actuelles. Pouvez-vous dire où vous en êtes à ce sujet ? Plus largement, pouvez-vous nous apporter quelques précisions sur le degré de protection que l'on peut attendre de nouvelles dispositions législatives ou réglementaires face aux failles des réseaux numériques ?

M. Pascal Chauve, conseiller du Secrétaire général de la défense et de la sécurité nationale (SGDSN). – Je vais vous parler de *hard law*. La loi de programmation militaire a été promulguée le 18 décembre 2013. Elle fixe un cadre légal totalement novateur pour la protection des infrastructures critiques nationales contre les cyberattaques. Ce dispositif que je vais vous présenter est au cœur de nos préoccupations quotidiennes au SGDSN, où nous sommes chargés d'en élaborer les décrets d'application et toutes les mesures qui en découlent. Je vais nous éloigner de la problématique de l'espionnage des données des personnes pour parler d'un enjeu assez nouveau, celui des attaques informatiques, non pas pour espionner et capter des données, mais pour perturber les systèmes, voire les détruire.

Les mesures qui ont été prises dans la loi de programmation militaire portent sur les infrastructures critiques. En France, on parle

d'**opérateurs d'importance vitale (OIV)**. Ce champ n'est pas nouveau, il a fait l'objet d'une définition dans le code de la Défense. Il concerne tout ce qui est absolument indispensable à la vie de la nation et dont le dysfonctionnement pourrait porter des atteintes graves au fonctionnement de l'État, de ses institutions, de l'économie et à la vie des populations.

Les domaines couverts, qui vous intéressent en particulier, sont ceux de l'énergie et des télécommunications. Mais les transports, l'alimentation sont également autant de secteurs qui sont placés sous la tutelle de ministres coordonnateurs de secteurs d'activité d'importance vitale.

Le texte voté en décembre 2013 est extrêmement consensuel. Son succès est dû à la clairvoyance des parlementaires, mais aussi au talent de pédagogie des auteurs du projet. C'est également le succès d'une idée qui apparaît aujourd'hui comme une sorte d'évidence. Premièrement, **les cyberattaques sont un phénomène dont l'ampleur ne cesse de croître. Elles visent nos concitoyens, nos entreprises, mais aussi l'État et toutes les fonctions essentielles au fonctionnement de la nation**. Deuxièmement, face à cette menace**, l'État doit affirmer son rôle d'autorité de cybersécurité et de cyberdéfense** pour continuer à protéger ce qui est essentiel au pays et la loi doit lui en donner les moyens. La chose ne va pas se faire spontanément. Je pense résolument que sur ces questions d'infrastructures critiques, nous ne sommes pas du tout dans le registre de la *soft law*, du droit souple.

L'idée avait germé dès les discussions sur le Livre blanc sur la défense et la sécurité nationale. À l'été 2013, il a dressé un constat tout à fait préoccupant de l'évolution de la cybermenace depuis sa précédente édition de 2008. Nous étions tous familiers du cyberespionnage. Nous avons constaté que, depuis 2008, le cyberespionnage s'est généralisé – voir les révélations de Snowden. Aujourd'hui, on a affaire à **un pillage systématique des informations sensibles de nos industriels, de leurs offres commerciales, de leurs secrets de fabrication**. Mais, plus inquiétant, on a assisté, depuis 2008, à **l'émergence du cybersabotage** dont on a déjà quelques illustrations concrètes comme celle de la fameuse attaque informatique de 2009 sur les centrifugeuses d'uranium iraniennes de Natanz. Des automates industriels, de marque *Siemens*, ont vu leur fonctionnement perturbé par l'introduction de petits délais aléatoires qui ont conduit à des destructions ainsi qu'à un retard d'un certain temps dans la progression du programme nucléaire iranien. Il y a eu également les attaques destructrices contre la compagnie pétrolière saoudienne *Aramco* et la compagnie gazière qatarie *RasGas*.

Aujourd'hui, nos craintes, fondées sur des arguments techniques, portent sur les systèmes de supervision et de management des installations critiques. Par exemple, la régulation des cœurs de centrales nucléaires, la régulation des barrages, le contrôle du trafic aérien, du trafic ferroviaire, des feux tricolores… pourquoi pas ? Le cybersabotage, c'est-à-dire la prise de contrôle par des saboteurs, voire des terroristes, d'une

infrastructure critique, ne relève pas uniquement de l'imagination d'un scénariste de film à succès américain ou d'un fameux jeu vidéo qui vient de sortir, dont le héros peut éteindre les quartiers d'une ville en passant son pouce sur son *smartphone*. C'est une menace bien réelle contre laquelle il convient de se protéger, qui peut conduire à des catastrophes écologiques et à des pertes de vies humaines.

On a commencé à faire de la *soft law*. Au sein du SGDSN, nous avons l'ANSSI qui a déjà publié sur son site des recommandations sur la sécurité de ce qu'on appelle les *Supervisory Control and Data Acquisition (SCADA)*. Ils désignent les systèmes de contrôle industriel, c'est-à-dire ces appareils informatiques qui régulent des processus industriels dont les dysfonctionnements ont des conséquences physiques directes.

Ces recommandations relèvent du bon sens et de ce que le directeur général de l'ANSSI appelle de « *l'hygiène informatique* », comme de procéder à des authentifications fortes et à des mises à jour, ou superviser la sécurité même de ces dispositifs de contrôle industriel. **La mesure essentielle préconisée dans les guides de l'ANSSI est de déconnecter ces systèmes industriels de l'Internet**, afin de réduire le plus possible la surface d'attaque qui permet à un attaquant distant de prendre le contrôle de ces dispositifs. À elle seule, cette règle, si elle est effectivement appliquée dans les systèmes modernes et dans les systèmes futurs, s'avérera contraignante, voire très contraignante, tout simplement parce qu'elle va empêcher la télémaintenance et exiger la présence d'un administrateur sur place, depuis sa console, pour vérifier que les systèmes continuent de fonctionner correctement.

C'est une mesure d'autant plus nécessaire que **les systèmes sont de plus en plus complexes et qu'ils comportent de plus en plus de failles**. Par exemple, les systèmes d'exploitation utilisés dans ces systèmes de contrôle industriel ainsi que les protocoles qui sont mis en œuvre sont très largement répandus dans l'Internet, voire dans la bureautique. Toutes les failles de sécurité que nous connaissons avec nos ordinateurs, nous pouvons également les rencontrer dans ces systèmes de contrôle industriel.

C'est sur la base de ces recommandations que vont s'ériger désormais par la loi des règles obligatoires qui vont s'appliquer aux opérateurs d'importance vitale. La loi précise que l'État peut fixer des règles et qu'il devra en contrôler l'application. De leur côté, **les opérateurs d'importance vitale seront tenus de cartographier leurs systèmes**. Vous pouvez mettre au défit un grand industriel de vous montrer à quoi ressemblent ses systèmes d'information, notamment ses systèmes d'information industriels. En général, les industriels ne savent même pas comment est configuré leur système, où sont les interconnexions, les passerelles vers Internet. Le flou est assez abyssal. C'est également le cas des administrations. L'obligation de cartographier est donc absolument importante.

Une fois dressée cette cartographie et identifiés des sous-systèmes qui sont qualifiés de particulièrement critiques au sein de ces opérateurs d'importance vitale, la loi précise qu'il faut **mettre en place des sondes de détection d'attaque** sur ces systèmes et les faire opérer par des prestataires qualifiés.

Une autre obligation est celle de **l'information sans délai des autorités nationales en cas d'attaque**. Les opérateurs sont désormais tenus d'alerter l'ANSSI en cas d'attaque informatique sur leurs systèmes critiques. L'ANSSI aura donc un rôle centralisateur de toutes ces alertes qui lui permettra d'avoir une vue d'ensemble et peut-être de prévoir les prochaines.

Enfin, en cas de crise majeure, **la loi habilite désormais le Premier ministre à prendre des mesures d'exception**.

Les décrets d'application sont en cours de finalisation. Nous ne faisons pas ce travail dans notre tour d'ivoire administrative, éloignés des contraintes de terrain. Nous travaillons en coordination avec les ministères de tutelle, mais aussi avec les opérateurs concernés. Nous n'avons pas du tout laissé la place à l'improvisation sur ces sujets-là. Tout ce travail est issu d'un travail préalable qui avait été conduit dans un cadre de *soft law*, de recommandations qui avaient été adressées aux différents secteurs.

Je précise également que les règles de sécurité qui seront édictées et donc rendues obligatoires, puis contrôlées par des prestataires de contrôle qualifiés par l'État, seront déclinées secteur par secteur. On ne va pas *in abstracto* imposer à tout le monde des règles qui seraient inappropriées ou inapplicables.

Je souhaite mettre l'accent sur l'importance de ces prestataires de contrôle qualifiés qui vont naître dans cet écosystème de la sécurité des systèmes d'importance vitale. L'État va donner un **label à des prestataires de confiance** chargés de détecter les vulnérabilités, les manquements des opérateurs critiques au cœur de leurs systèmes. Ils seront en relation avec l'État. Il y aura des prestataires de détection qualifiés par l'État, qui seront en contact avec l'ANSSI pour échanger sur les nouvelles menaces, les nouvelles signatures techniques de comportement d'attaquant. Ce sont ces critères techniques que l'on peut introduire dans les sondes automatiques pour détecter que quelque chose d'anormal est en train de se passer et que nous sommes *a priori* victimes d'une attaque. Ces signatures sont désormais le bien le plus cher des agences de sécurité. Elles se substituent un peu à ce que, dans la cybersécurité de grand-papa, on appelait les clés cryptographiques. **Le nerf de la guerre, ce sont maintenant les signatures d'attaque informatique**, dont l'ANSSI entretient un vivier et qui seront partagées avec des prestataires de détection qualifiés.

Avec ce dispositif, **la France est pionnière en Europe**. Nos partenaires, notamment allemands, sont en train d'élaborer un cadre similaire. Nous sommes en discussion avec eux. Le projet de directive

européenne concernant la Sécurité des réseaux et de l'information (SRI) est en cours de négociation. Dans son chapitre 4, il comporte des dispositions qui ont été inspirées par la France : l'édiction de règles de sécurité, la notification obligatoire des incidents à une autorité nationale compétente disposant d'un pouvoir de contrôle et un régime de qualification de prestataires.

La France soutient depuis le départ ce projet de texte européen. S'il est adopté, il ne devrait pas nécessiter de transposition en France puisque nous avons déjà les mesures dans notre arsenal législatif.

Dans la discussion européenne, ce nouvel arsenal a soulevé quelques réticences de certains États membres, ceux qui par exemple ne disposent pas d'une autorité nationale compétente en matière de cyberdéfense, contrairement à la France. Pour nous, il est très important d'avoir des interlocuteurs qui s'érigent en autorité nationale de cyberdéfense comme l'est l'ANSSI en France.

D'autres États membres défendent un modèle plus libéral, où il n'y aurait pas de règles qui s'imposent, mais davantage de bonnes pratiques partagées dans les milieux professionnels au sein d'un partenariat public-privé qui instaurerait des règles par la discussion avec les opérateurs concernés. Je pense que ce n'est pas incompatible. C'est ce que nous sommes en train de faire pour les mesures d'application de la loi de programmation militaire.

J'espère vous avoir convaincu de la nécessité et de la pertinence de ce cadre légal. J'espère surtout que, depuis le vote de cette loi il y a six mois, nous tous, industriels, fournisseurs de sécurité, administrations, parlementaires, continuons à croire en ces dispositions qui visent à défendre les systèmes les plus critiques pour le fonctionnement de l'État, l'économie, la société et pour la vie même des populations.

M. Bruno Sido. – Vous conviendrez avec moi que les précisions apportées par M. Pascal Chauve sont de nature à éclairer notre réflexion. Elles peuvent également faire naître de nouvelles interrogations dans l'esprit des rapporteurs qui ne manqueront pas de lui adresser quelques questions et recevront avec plaisir tout document et également toute nouvelle sur l'avancement des rédactions en cours.

Nous tenons à remercier particulièrement Mme Mireille Delmas-Marty qui a accepté de nous apporter un éclairage juridique sur l'élaboration des normes aux niveaux national et international, ce qui peut nous conduire à réfléchir sur l'imbrication du public et du privé, particulièrement complexe dans le domaine de l'Internet, en nous demandant, par exemple, si le concept de souveraineté n'est pas profondément remis en cause par l'évolution du numérique, au point de pouvoir parler de révolution numérique, non plus seulement technique, mais quasiment institutionnelle.

Mme Mireille Delmas-Marty, membre de l'Institut de France (Académie des Sciences morales et politiques), professeur honoraire au Collège de France (Études juridiques comparatives et internationalisation du droit). – Je ne suis pas spécialiste de la question des réseaux numériques. Je vais donc présenter des observations assez générales sur les métamorphoses du cadre juridique dans le prolongement de cette question des réseaux numériques et de leur sécurité.

D'abord, je voudrais réagir à ce que nous venons d'entendre. Les exemples donnés me frappent parce qu'ils montrent l'impossibilité, ou l'extrême difficulté, à distinguer la sécurité intérieure de la sécurité extérieure. Peut-être y a-t-il là un effet 11 septembre 2001, non pas qu'on y ait vu naître la formule de la guerre contre le terrorisme, mais parce qu'on a vu alors se transformer cette formule qui était une sorte de métaphore – on évoquait souvent aussi « la guerre contre le crime » – en un concept nouveau : la guerre au sens plein du terme. En droit international, on sait qu'après les attentats du 11 septembre, le Conseil de sécurité a considéré qu'il y avait eu une agression justifiant, au nom d'une légitime défense préventive, l'attaque de l'Irak. Et le droit américain a explicitement reconnu l'état de guerre car la Constitution américaine ne prévoit pas l'état d'exception, seulement un état de guerre avec transfert de pouvoir au chef d'État. D'où le fameux *Patriot Act* de 2001, toujours en vigueur. Ce transfert de pouvoir va très loin, puisqu'il permet au chef de l'État de condamner à mort sans procès les suspects de terrorisme. C'est la pratique des assassinats ciblés, en riposte aux soupçons de terrorisme. À terme, on peut donc s'interroger sur la disparition progressive de la distinction entre guerre et paix, ennemis et criminels, armée et police.

Dans un tel contexte, la question des réseaux numériques est centrale du point de vue juridique. Les réseaux numériques sont en effet au cœur de mutations, de véritables métamorphoses, de l'ordre juridique, tant leur fonctionnement perturbe les différentes composantes de cet ordre que sont les normes, les formes et les dogmes.

Avec les réseaux numériques, on observe de façon extrêmement visible **la privatisation des normes** qui est liée à la diversification des acteurs, au risque de réduire peut-être l'effectivité, de diluer les responsabilités.

On observe aussi une sorte d'**assouplissement des formes**. C'est tout le débat que nous avons eu sur la *soft law* et la *hard law*, sur l'autorégulation et la régulation proprement dite. Or cet assouplissement des formes entraîne du même coup, un affaiblissement de la prévisibilité et un risque pour la sécurité juridique, c'est-à-dire un risque pour l'état de droit. La forme, longtemps considérée comme la sœur jumelle de la liberté, étant supposée garantir la sécurité juridique.

Enfin, l'**ébranlement des dogmes** affaiblit la légitimité du cadre juridique lui-même. En Occident, nous avons construit nos systèmes de droit sur le dogme de la souveraineté de l'État. C'est ce qui fonde et ce qui stabilise nos systèmes de droit. Nous avons un modèle souverainiste à l'esprit. **Or les réseaux numériques remettent assez directement en cause ce dogme de la souveraineté de l'État.** Même si les États résistent, les réseaux numériques annoncent une métamorphose.

Vers quel modèle allons-nous ? Un modèle universaliste, qui reposerait sur un nouveau dogme, le dogme de la communauté mondiale ? On en est loin, semble-t-il. Un modèle ultralibéral, qui reposerait sur le dogme du marché autorégulé ? C'est un peu le prolongement du débat que nous avons eu. Un modèle hybride aurait ma préférence.

Quelques mots sur chacune de ces trois métamorphoses.

1. D'abord la privatisation des normes. Avec les réseaux numériques, l'émission de la norme n'est plus le monopole de l'État-nation, mais elle ne relève pas pour autant d'un État-monde. Au stade actuel, un État-monde n'est sans doute pas souhaitable parce qu'il risque de devenir un État totalitaire. Il n'est pas non plus faisable, fort heureusement, parce qu'il y aurait des obstacles politiques. **Même si les experts en nouvelles technologies et les opérateurs privés semblent mener le jeu, les États, surtout les superpuissances, s'en accommodent très bien, précisément parce que la privatisation empêche l'émergence d'un État-monde.**

Certes, le constat ne se limite pas aux réseaux numériques. Il vaut plus largement à travers tous les phénomènes liés à la mondialisation du droit. Mais les réseaux ont un effet révélateur parce qu'ils mettent au grand jour un phénomène plus général de diversification des acteurs. On l'a vu pendant la première partie de cette séance. Nous avons parlé d'acteurs étatiques, qui sont encore une fois très présents à travers leurs législateurs, leurs autorités administratives indépendantes comme la CNIL et leurs juges. À l'heure actuelle, **il y a une montée en puissance du juge**, qui applique non seulement le droit national, mais aussi le droit international. **Le juge français est aussi un juge européen. Il a vocation à être juge mondial à l'occasion.** Donc les États restent des acteurs essentiels, mais ils ne sont plus les seuls.

À leurs côtés, les organisations interétatiques, voire supraétatiques, se situent à des niveaux différents. À un niveau régional, on a beaucoup parlé d'Europe à travers le projet de règlement de l'Union européenne. À propos de l'Europe, on aurait pu aussi évoquer l'impact de la Convention européenne de sauvegarde des droits de l'homme. C'est le pôle Droits de l'homme de la construction juridique européenne. Mais potentiellement, ces organisations interétatiques se situent aussi à un niveau mondial, par extension du phénomène d'internationalisation des normes.

Cela dit, le plus frappant, ce n'est pas l'internationalisation seule mais l'internationalisation accompagnant, suivant ou complétant la

privatisation des normes car elle renvoie aux acteurs privés. Les acteurs privés ne sont pas une catégorie très homogène. En réalité, on y trouve les opérateurs économiques, dont on a déjà beaucoup parlé. Ils montent en puissance et pas seulement à travers les réseaux numériques. Par exemple, dans le droit des investissements, ils peuvent mettre en cause un État au moyen de la procédure d'arbitrage du CIRDI (Centre international de règlement des différends relatifs aux investissements). De ce point de vue, le droit des investissements est un domaine comparable au droit du numérique.

Mais avec les réseaux numériques, ce qui est important, c'est que **petit à petit, il semble que les grands acteurs économiques aient centralisé l'architecture de l'Internet**, alors même que, au départ, le système était très décentralisé.

Quant aux acteurs scientifiques, aux experts dont nous avons peu parlé, ils sont pourtant très présents, à la fois aux plans national et international. Je pense au rôle des chercheurs en informatique. Il n'y a pas très longtemps, nous avons eu une rencontre entre l'Académie des sciences et l'Académie des sciences morales et politiques. Avec mon collègue du Collège de France, Gérard Berry, nous avons discuté du droit à l'oubli. Selon lui, nous n'avons pas les moyens techniques d'assurer de façon parfaitement efficace ce droit à l'oubli. On a besoin, qu'on le veuille ou non, de cette interface entre les acteurs politiques, juridiques, économiques et scientifiques. Or elle pose toute une série de problèmes liés aux conditions de l'expertise scientifique, aux risques de conflit d'intérêts, un vaste domaine.

Enfin, les acteurs non étatiques sont aussi les citoyens. Ils commencent à s'organiser en agissant de façon concertée. Leur action peut aller à la fois dans le sens d'une recherche de plus de liberté et d'une participation à plus de contraintes, à plus de contrôles. Dans les années 2000, un collègue américain posait la question : « *perfect control or perfect freedom* ? » allons-nous vers un contrôle parfait ou une liberté totale ?

Les acteurs civiques sont le reflet de ce que le Conseil constitutionnel avait très bien dit, en 2009, à propos de la loi Hadopi : l'exercice de la libre communication et de la liberté d'expression implique la liberté d'accéder à Internet. **Même si le Conseil constitutionnel ne va pas jusqu'à affirmer que l'accès à Internet serait un droit fondamental, il n'est pas loin de le dire.** Cela étant, les acteurs civiques, et cela a été rappelé par la présidente de la CNIL, participent aussi à la surveillance. Donc ils revendiquent leur liberté et, en même temps, ils participent à la surveillance : de façon passive quand ils profitent des services de l'Internet, mais aussi en acceptant d'entrer dans ce jeu de façon active lorsqu'ils participent à la surveillance, par des dénonciations par exemple.

C'est le premier point qu'il me paraissait important de souligner à travers la privatisation des normes. Mais la multiplication des acteurs que je

viens de commenter brièvement n'entraîne pas seulement cette privatisation des normes, elle entraîne aussi la complexité des jeux entre la *soft law* et la *hard law*.

2. On observe par là même un second processus, d'assouplissement des formes. Assouplissement, parce que le recours à la *soft law* accompagne généralement la privatisation et parfois l'internationalisation. Je traduirais *soft law* par droit souple. Derrière la *soft law,* nous avons à la fois un **droit flou**, ou imprécis, fait de principes généraux qui ne sont pas définis de façon rigoureuse et un **droit mou**, facultatif, non obligatoire (le droit des recommandations), enfin le **droit doux,** qui n'est pas sanctionné. Le flou, le mou et le doux peuvent aller de pair ou séparément.

L'un des enjeux de notre discussion est d'articuler la *soft law* et la *hard law,* de les faire cohabiter, fonctionner de façon non pas opposée mais complémentaire. Il peut en effet être utile de dissocier le droit flou, c'est-à-dire des principes généraux ou des principes directeurs, suffisamment précis pour indiquer une orientation mais suffisamment vagues pour permettre ensuite des applications concrètes par des régulations différentes les unes des autres. **Un droit qui n'uniformise pas, mais qui permet de pluraliser la régulation**, me paraît une perspective très intéressante. Elle irait dans le sens d'une corégulation qui ne soit pas l'uniformité de la loi, au sens traditionnel du terme.

Il est utile aussi, et on l'a déjà dit, de faire appel au **droit mou, non obligatoire, comme manière d'amorcer un processus de régulation.** Il est plus facile de commencer par des recommandations que directement par un texte de loi. Le droit mou est peut-être un moyen d'**éviter que le cadre juridique soit en retard par rapport aux innovations technologiques.** La loi est plus rigide. Pour mieux adapter le cadre juridique à cette extraordinaire accélération des vitesses de transformation technologique, on a besoin d'agir très vite et de façon souple, d'où l'utilité de passer dans un premier temps par le droit mou, qui fera ensuite l'objet d'un durcissement progressif. C'est un peu ce qui se dessinait dans la présentation de la présidente de la CNIL à propos de l'accord entre les autorités nationales de protection des données, qui appellerait peut-être par la suite une loi de blocage.

Cet assouplissement est utile, mais il pose, en termes d'éthique, le problème de la légitimité du cadre juridique. Cette légitimité est d'autant plus difficile à trouver que l'on observe l'ébranlement des dogmes. **La métamorphose des normes par leur internationalisation, par leur privatisation et l'assouplissement des formes, produisent un ébranlement qui annonce peut-être un changement de modèle.**

3. L'ébranlement des dogmes. Nous vivons encore sous le **dogme du souverainisme**. C'est un État souverain qui assure la régulation et la réglementation, sur son territoire. Ce dogme est très important puisqu'il permet de stabiliser la norme juridique et de ne pas la réduire à l'état de pur instrument au service de la force, au service du marché.

Or, **s'agissant des réseaux numériques et de leur sécurité, le territoire n'a guère de sens**. Il y a une sorte de neutralisation des frontières par la circulation de flux immatériels d'informations ou de capitaux. Au mieux, on pourrait parler de transterritorialité. Nous sommes donc obligés de renoncer, au moins en partie, au modèle souverainiste, non pas pour des raisons idéologiques, mais en raison de la déterritorialisation des pratiques.

Quel autre modèle invoquer ? Un modèle universaliste nous conduirait à un nouveau dogme, nouveau car il suppose une communauté mondiale et qu'elle soit suffisamment organisée pour émettre des normes dans un cadre juridique clair et cohérent et pour assurer une régulation qui serait non pas étatique, mais supraétatique. Apparemment, une telle voie peut sembler séduisante. On y retrouve l'idée de la démocratie par Internet. Internet au service de la liberté d'expression et favorisant l'éclosion de mouvements comme celui dit des Printemps arabes. En même temps, **ce modèle universaliste ne me paraît pas réalisable en raison de la résistance quasi certaine des États**, à commencer par les grandes puissances. Et je ne pense pas qu'il soit souhaitable parce qu'il risque de cacher le rôle hégémonique exercé par une superpuissance.

Que penser du modèle ultralibéral ou libéraliste de type transétatique ? Ce serait l'autorégulation revendiquée au nom d'un autre dogme, celui du marché autorégulé. Le risque de ce modèle, c'est qu'il reflète, lui aussi, la tendance hégémonique d'une régulation imposée par des acteurs tout puissants. **Le risque, c'est que le modèle libéral pur, ultralibéral, conduise au totalitarisme du marché.** On le voit déjà avec la commercialisation du corps humain par Internet : vente d'organes, recrutement de mères porteuses et bien d'autres pratiques. On a l'impression que dans cette perspective, les normes se resserrent dans un maillage de plus en plus dense et qui annoncerait l'avènement d'une société de contrôle ou de surveillance. Je rappelle que cet avènement avait été prophétisé dans des termes prémonitoires par Tocqueville quand il s'était posé la question de savoir à quoi ressemblerait **le despotisme en démocratie**. Il écrivait : « *Ce serait un despotisme plus étendu et plus doux qui dégraderait les hommes sans les tourmenter et qui couvrirait la société d'un réseau de petites règles compliquées, minutieuses, uniformes, mais dont on aurait un peu perdu le sens, la signification. Il tendrait à* ***retenir les humains dans l'enfance et à réduire chaque nation à n'être plus qu'un troupeau d'animaux timides et industrieux dont le Gouvernement est le berger.*** » Ce tableau n'est pas très loin de celui que l'on peut observer, avec cette nuance qu'au lieu de troupeau d'animaux timides, il faudrait plutôt parler d'une tendance à la robotisation de l'être humain. En tout cas, le modèle ultralibéral n'est pas une réponse satisfaisante.

Alors vers quoi allons-nous ? Je propose d'imaginer un nouveau modèle plus complexe, qu'on pourrait appeler modèle pluraliste, dans la mesure où il n'échappera aux risques de totalitarisme ou de

fondamentalisme juridique que s'il tient compte de la diversité des cultures et s'il réussit à anticiper sur les innovations technologiques. Il faut donc un modèle pluraliste et évolutif, ce qui pose très directement la question des valeurs de référence. Quelles sont les valeurs sur lesquelles on pourrait bâtir ce modèle à la fois commun et pluraliste, stable et évolutif ?

Nous disposons déjà des éléments : dans le droit international des droits de l'homme, avec **le droit à la dignité de la personne humaine** ; dans la justice pénale internationale avec **le crime contre l'humanité**, une sorte de noyau dur que Boutros Boutros-Ghali (à l'époque Secrétaire général de l'organisation des Nations unies) avait appelé, lors de la conférence de Vienne en 1993 « *l'irréductible humain* ». Évidemment, il faudrait donner un contenu plus précis.

Si l'on veut aller vers des valeurs communes en matière de réseaux numériques, les droits de l'homme et les crimes internationaux ne suffiront pas. Il faudrait ajouter **la notion de « bien public mondial ».** Cette notion, qui vient de l'économie, désigne des biens non exclusifs – on ne peut se les approprier, ils peuvent être utilisés par tous – et non rivaux, en ce sens que l'usage par quiconque ne compromet pas l'utilisation par autrui. Chacun en a sa part et tous l'ont en entier. **On pourrait dire cela à propos des réseaux numériques.** Les qualifier de biens publics mondiaux serait une manière de favoriser une convergence autour de valeurs qui deviendraient universelles.

En conclusion, pour assurer la sécurité dans les réseaux numériques sans aboutir à une insécurité au niveau juridique, il faut d'abord tout un arsenal juridique et technique hautement complexe. C'est ce qui sera présenté pour l'essentiel dans cette journée. J'ai voulu simplement rappeler qu'il faudra aussi une boussole pour orienter les choix éthiques et instaurer ainsi une confiance dans les réseaux autour de valeurs universalisables, aptes à devenir progressivement universelles.

M. Bruno Sido. – Merci, madame le professeur, c'est avec un vif intérêt que nous avons écouté la communication d'un membre de l'Institut sur le sujet qui nous occupe depuis plusieurs mois, ma collègue députée et moi-même. Permettez-moi à cette occasion de recommander la lecture de votre contribution à l'ouvrage collectif « *Science et Société : les normes en question* » (Actes Sud/IHEST, 2014), intitulée : « *Normes, formes et dogmes : regards d'une juriste* ».

Permettez-moi de saluer la venue de Jean-Yves Le Déaut, député, premier vice-président de l'OPECST, qui mène par ailleurs un rapport sur un sujet d'actualité lié à la loi sur la transition énergétique.

La parole est à M. Jean-Dominique Nollet, qui nous vient des Pays-Bas, puisqu'il travaille à *Europol*. Nous attendons de lui un éclairage technique. À partir de son expérience technique et internationale, pourra-t-il tracer quelques pistes de solutions pour améliorer l'avenir qui attend les entreprises, quelle que soit leur taille, et pour nous aider à mieux cerner le

risque numérique résultant directement des vulnérabilités qu'il a eu l'occasion de mieux cerner dans son activité quotidienne ?

M. Jean-Dominique Nollet, lieutenant-colonel de la Gendarmerie nationale, chef d'unité de laboratoire de recherche, Centre européen de lutte contre la cybercriminalité (*EC3*) à Europol. – Merci de nous donner l'occasion de tenter de vous éclairer dans ce cadre difficile de la cybersécurité. J'articulerai mon propos en deux points : une présentation de ce qu'est vraiment la cybercriminalité pour nous et, ensuite, la déclinaison des risques potentiels dans les pratiques actuelles dans le domaine de cybercriminalité appliquée aux entreprises.

Le Centre européen de lutte contre la cybercriminalité a été créé il y a un an et demi à la suite d'une communication de la Commission européenne et il se focalise sur les groupes criminels. Dans notre vision des choses, il y a des domaines. On a entendu parler de la cyberdéfense et de la défense contre le cyberespionnage. Pour notre part, nous travaillons à lutter contre la cybercriminalité.

Je regrette que, depuis ce matin, on ait assez peu parlé des acteurs. On a l'impression qu'on attrape un virus informatique parce qu'on se promène dans la rue. L'analogie est bonne, mais n'oublions pas que derrière des claviers d'ordinateur, ce sont des gens qui créent des virus, des *malwares*, ou qui ouvrent des portes qui sont restées ouvertes. Il ne faudrait pas déshumaniser le côté de l'attaquant malicieux. Derrière ce qui se passe, il y a de vrais gens, de vraies personnes. Il ne faut pas oublier que nous, en tant qu'organisme européen de police, souhaitons remettre ces personnes à la justice afin qu'elles soient arrêtées et que les biens qu'elles peuvent générer, souvent énormes, puissent leur être confisqués.

Le gros problème en matière de cybercriminalité, c'est l'absence de lien entre le lieu de l'infraction et son auteur. En effet, le principe d'échange de Locard ne s'applique pas à la cybercriminalité. C'est un gros changement pour les forces de l'ordre en général. L'attaquant n'est pas forcément en Europe, il a peut-être rebondi sur un site au Venezuela ou au Vietnam. Ou ce peut être une attaque entre deux personnes situées dans la même rue. La perte de ce lien géographique appelle nécessairement une coopération entre les polices internationales.

Depuis un an et demi, l'approche des policiers internationaux a considérablement changé. Ils viennent frapper à notre porte avec des dossiers complets pour collaborer avec nous. Jusqu'alors, ce n'était pas une pratique courante en matière de contre-terrorisme et de lutte contre le crime organisé. Nous sommes très satisfaits de voir le FBI et d'autres grands organes venir nous proposer des dossiers et essayer d'organiser les ripostes, principalement contre les *botnets*, des réseaux assez puissants qui demandent un gros travail.

Les priorités émises par les ministres de l'intérieur européens nous permettent de nous focaliser sur la cyberattaque pure : *botnet*, *malware*, des attaquants assez classiques du cyber, mais très avancés.

Ensuite, il y a l'abus de l'enfance en ligne. Il n'a pas été évoqué et je le regrette. C'est quand même un drame ! Je sais que la protection des infrastructures critiques est très importante. Mais n'oublions pas ce que certains appellent la « pédopornographie en ligne », un terme qui me paraît inapproprié. Des enfants se font violer pour que des gens puissent aller regarder devant des ordinateurs ces viols d'enfants ! En matière d'éthique mondiale, ce volet nous semble prioritaire.

Un troisième axe concerne la fraude aux moyens de paiement, qui est en augmentation. Il y a eu un mouvement depuis les groupes qui opéraient des fraudes classiques de manipulation d'automates ou de terminaux de paiement ou *skimming*. En termes de technologie, c'est la copie d'une bande magnétique des années 1960, ce qui n'est pas très compliqué. On a encore ce problème-là aujourd'hui. Mais toutes ces problématiques se déplacent dans le *Card-Not-Present*, c'est-à-dire le vol de numéros de cartes bleues destiné à faire des achats en ligne. Tout cela est très structuré par des groupes criminels très puissants. Un numéro de carte bleue sur Internet ne vous coûtera qu'entre vingt-cinq et trente centimes d'euros !

Sur Internet, les réseaux de « *Cybercrime as a Service* », pour faire l'analogie avec l'informatique en nuage ou *cloud computing*, vous fournissent des services vingt-quatre heures sur vingt-quatre, en cinq langues. Vous pouvez les appeler à trois heures du matin pour demander une attaque sur la société concurrente de votre choix. Vous pouvez les rappeler aussi, etc. C'est une vraie industrie qui fonctionne. On est très surpris de constater la réactivité de leur service après-vente. Techniquement, leurs services sont très bons.

Certains sites proposent une attaque dite *DDoS (Denial of Service Attack)*, c'est-à-dire une attaque par déni de service, somme toute classique, à dix euros les dix minutes ! Vous n'avez rien à connaître. Il suffit de payer pour simplement attaquer votre voisin. J'ai connu des sociétés qui se sont retrouvées en grande difficulté et qui même ont dû fermer, à la suite d'une attaque de leur concurrent au moment de Noël. La cybercriminalité est une réalité.

Mon laboratoire travaille sur un quatrième axe : les sciences légales avancées. Internet oblige les forces de l'ordre de tous les pays à se bouger en matière technologique et à suivre l'avancée technologique des malfaisants, afin d'essayer de comprendre dans un premier temps ce qui se passe, pour ensuite neutraliser, quand c'est possible, ou essayer *a posteriori* de trouver dans les *logs*. Mais je doute que s'il y a espionnage, on va trouver grand-chose dans les *logs*. Les gens doivent comprendre que la preuve informatique va évoluer. Il y a dix ans, on savait qui avait effacé son fichier.

Dans quelques années, avec l'évolution de différentes technologies, sa nature va évoluer. Elle sera peut-être plus fluide parce que les attaquants s'adaptent relativement bien.

À ce titre, les lois en France sont relativement bien faites. En tant que porte-parole européen, il me paraît important que les enquêtes sous couverture, telles qu'elles sont définies actuellement, et la possibilité pour les enquêteurs d'aller anonymement en ligne, doivent être étendues en France.

Une autre chose me paraît capitale, c'est d'**étendre la captation des données à distance**. Si l'on considère que l'écoute téléphonique doit être maintenue, c'est-à-dire la possibilité de procéder à des écoutes dans le cadre de commissions rogatoires, avec un encadrement juridique qui est relativement sain dans notre pays, il faut pouvoir avoir les moyens techniques d'avancer vers une captation à distance des données.

Pour moi, l'Internet, ce sont ces deux points et une ligne au milieu. Cette ligne va être de plus en plus cryptée et les points de départ vont être de plus en plus durcis par les criminels. C'est déjà le cas. Si vous n'êtes pas sur l'un de ces deux points, vous ne savez pas ce qui se passe. Donc il va falloir rentrer dans les machines qui sont d'un côté ou de l'autre. Là-dessus, la loi française pourrait favorablement évoluer.

Avant de parler des entreprises, je vais parler de la sensibilisation. C'est un thème à la mode. Il y a deux ans et demi, nous nous sommes livrés à un exercice très analytique et très classique dans le monde du renseignement et de la police : élaborer un scénario sur la sécurité informatique en 2020.

Nous avons réuni nos experts, des pirates informatiques, des experts du monde de l'industrie, de la vente et de la sécurité informatique, pour essayer, avec une méthodologie du scénario, de voir quelles seraient les options en 2020. Je vous invite à lire notre beau rapport de trente pages. Mais évidemment, les gens ne lisent pas ce genre de rapport, en anglais en plus. Et la société *Trend Micro*, qui était avec nous, l'a repris pour en faire un film avec des acteurs. Je vous invite à le voir sur *YouTube* (http://2020.trendmicro.com). Il permet de prendre conscience de ce que M. Gilles Babinet vient de décrire. Notre monde va évoluer.

Pour l'instant, les publicités arrivent sur le *smartphone*, mais dans quelques années, elles arriveront dans vos lunettes *Google Glass*. On a toujours tendance à se dire qu'on va essayer de réglementer un peu tout ça et que, lorsque la technologie sera mûre, on y réfléchira. Je pense que c'est une erreur de raisonnement. **Il faut réfléchir dès maintenant aux conséquences de ces évolutions sur la société.** Certes, ce scénario est fait par des policiers, des gens qui ne sont pas toujours optimistes sur la moralité. Mais cela nous paraît assez intéressant.

En ce qui concerne la sécurité des entreprises, c'est une grosse difficulté. Pour l'instant, si l'on considère les entreprises dans leur globalité, hors opérateurs d'importance vitale et *high tech*, il n'y a pas grand monde qui

y comprend quelque chose. C'est difficile de suivre, parfois très difficile, et l'on ne sent pas la volonté des gens d'y parvenir.

Je trouve surprenant qu'après un épisode aussi important que les révélations de M. Edward Snowden, les entreprises qui ont des choses à cacher, comme la R&D en biologie, n'ont pas pris en compte cette menace et se protègent. Il n'y aura pas de scandale plus fort de ce niveau-là. Malgré cet événement, des acteurs qui évoluent dans des secteurs avancés et qui peuvent se sentir vulnérables, ce qui n'est pas le cas de toutes les sociétés, n'ont pas pris en compte cette dimension-là. Il ne faut pas non plus hurler au loup, mais on pense qu'il faut que les choses avancent.

Dans les entreprises, on assiste aussi à une moralisation de la sécurité informatique. C'est un problème. Je ne suis pas contre la morale, mais croire qu'il n'y a pas de risque parce qu'on ne va surfer que sur des sites reconnus ou parce que le directeur des ressources humaines a demandé de bloquer *Facebook*, c'est faux. **Il n'existe pas de proportionnalité de risque entre les comportements des salariés sur leur ordinateur et le risque qu'ils courent.**

Pour moi, **le point clé de la sécurité dans les entreprises françaises réside dans la sensibilisation des décideurs**. Le problème se situe au niveau des décideurs. Les responsables de la sécurité des systèmes d'information (RSSI) savent ce qu'il faudrait faire et ils l'ont décrit, en s'aidant des guides de l'ANSSI ou de références internationales. Mais la perception et l'analyse du risque dans les entreprises doivent être faites au niveau de la direction et la prise de conscience par la direction n'est pas forcément proportionnée. C'est une grosse difficulté. Je rencontre des RSSI qui me disent qu'ils ont tout écrit. « *Si ça pète, j'aurai fait ce qu'il fallait !* » La seule issue ne peut venir que d'une prise de conscience dans ce domaine-là.

Pour le décideur, la grosse difficulté réside dans la disproportion entre l'investissement qui doit être fait dans la sécurité informatique et le risque qui va être couvert ou pas. Cela bénéficie à certaines entreprises du marché de la sécurité informatique qui vous vendent des grosses boîtes magiques à deux millions d'euros censées vous protéger de tout ! Ces boîtes-là n'existent pas. Et cela oblige les gens à se poser des questions pour lesquelles ils ne sont pas formés.

La sécurité informatique est une histoire de code. Qu'est-ce que le code ? Vous écrivez un rapport parlementaire et puis quelqu'un va le réécrire autrement, pour lui faire dire autre chose, en modifiant deux ou trois mots. La sécurité informatique, c'est la même chose : une histoire sans fin. **Du code sécurisé à 100 %, ce n'est pas possible.** On pourra augmenter la sécurisation, ce qui n'est pas très difficile en ce moment, mais ce code informatique est un texte écrit par un humain, et un autre humain, avec ou sans intention malicieuse, va chercher à le détourner. Cet aspect de l'**adaptation permanente** doit être pris en considération. Untel vous vantera la cryptographie comme la solution ultime, un autre le niveau des pare-feu

ou *firewall*, etc. Il faut toujours s'adapter. C'est le cadre juridique ou le cadre conceptuel de la sécurité informatique, qui doit être posé.

Je me sers souvent des analogies avec des portes à propos de la sécurité informatique. Le PDG va très bien comprendre que la porte blindée à l'entrée sera plus sécurisée que la porte vitrée. Mais, pour faire venir des clients, une porte blindée, ce n'est pas accueillant. En matière informatique, cette perception et la compréhension du décideur ne vont pas être facilitées. Toutes les sociétés qui font de l'audit de sécurité, ou *pentesting*, proposent de l'ingénierie sociale. Les entreprises n'en veulent pas. C'est un souci. Et pour ces sociétés d'audit, il s'agit aussi de garder leurs clients. Si elles ne détectent pas grand-chose, c'est mieux pour elles. Plus l'audit est avancé, plus on a de chance de trouver quelque chose. Si la sécurité informatique ne se fonde pas sur la vue que peut avoir un attaquant d'une société, elle n'est pas réelle. Certains commandent des audits de sécurité depuis l'intérieur du réseau. L'intérêt peut être technique, mais en aucun cas cela n'aura de l'efficacité en matière de réseau.

En conclusion, je dirais que nous rencontrons deux difficultés dans la lutte contre la cybercriminalité au profit des entreprises. D'un côté, **les pirates opèrent selon une technique de guérilla**, à la façon de guérilleros, et de l'autre, **on essaie souvent d'y répondre avec des chars**. C'est ainsi que, quels que soient le *hardware* et les logiciels que l'on met en œuvre, si le programmeur de logiciel a oublié de changer le mot de passe par défaut – l'erreur est humaine –, les pirates entreront. Si l'entreprise ne comprend pas que le code malicieux est apparu parce qu'on a cliqué sur un lien malveillant non protégé ou inconnu, ou si la mise à jour d'*Acrobat reader* n'a pas été faite, elle sera piratée.

M. Bruno Sido. – L'une des questions qui me vient le plus à l'esprit est celle de la nouvelle place des États face au développement, souvent inattendu, du numérique. Pourront-ils aller jusqu'à prévoir l'imprévisible alors qu'il se présente de plus en plus de manière soudaine à un rythme défiant celui des institutions ? Nous en reparlons à l'occasion du débat tout à l'heure.

Nous allons maintenant aborder la question des données massives ou *big data* avec M. Charles Huot qui préside le comité éditorial du portail *Alliance big data.* Il va nous exposer en quelques mots pourquoi la création de ce portail est nécessaire, avant de nous faire part de ses analyses et réflexions sur le thème de la présente journée d'audition.

M. Charles Huot, président d'*Aproged*, président du comité éditorial du portail *Alliance big data*. – L'objectif de la création de cette Alliance est un peu le même que celui de ma participation ce matin à votre audition. *Big data* est un terme porteur de beaucoup de fantasmes et comme pour tous les termes qui se développent rapidement ou *buzzword*, on pense que ce mot est amené à disparaître. En réalité, il va perdurer parce qu'il correspond à une réalité nouvelle, une vraie révolution.

L'objectif de cette Alliance vise à expliquer, à raconter ce qu'est le *big data* à travers toute une série d'exemples. M. Gilles Babinet en a donné quelques-uns. Et peut-être que l'explication de ces exemples va apporter des réponses aux orientations juridiques que nous devons donner au traitement de ces données.

L'*Alliance big data* est partie du constat suivant : ce terme étant issu de l'informatique, très rapidement les sociétés informatiques s'en sont emparées, notamment les grandes entreprises américaines, les *Google*, *Facebook* et autres, qui ont développé les technologies sous-jacentes au *big data* pour des raisons internes à leurs entreprises, liées à la nécessité technique d'utiliser de nouveaux systèmes d'exploitation de l'information, de façon à prendre à compte les volumes de données très importants qu'elles devaient gérer chaque jour, les millions de clients, les très gros volumes de données issus des recherches et des indexations de l'Internet.

Finalement, l'idée de cette Alliance est venue le jour où l'on s'est dit que le besoin de technologies pour traiter de gros volumes de données, ce n'était pas vraiment nouveau. C'est lié à l'histoire de l'informatique. Cela remonte au temps où l'on voulait modéliser un profilage d'un véhicule dans des systèmes de soufflerie numérique. En quoi le *big data* n'est-il pas seulement un élément technologique ? La donnée ou *data*, dans l'écosystème national et international, c'est un terme qui s'associe à d'autres termes, comme l'*open data* par exemple, qui est le fait pour les États d'ouvrir leurs espaces de données aux citoyens et aux entreprises.

Petit à petit, un consensus s'est fait entre des acteurs qui avaient des intérêts différents, des métiers différents, et qui se sont regroupés dans ce mouvement qui porte aujourd'hui le nom d'*Alliance big data*. Les associations membres sont partagées en trois grands silos : le silo lié aux données, au milieu le silo lié aux technologies, c'est le cas notamment des grands pôles de compétitivité, et, enfin, le silo lié aux usages. Quand on prend le *big data* sous l'angle technologique, on oublie souvent de se demander à quoi il sert.

Le *big data* va perdurer parce qu'il touche tout le monde. La question, ce n'est pas la technologie pour la technologie, les données pour les données, mais les usages à lui donner. Le *big data* est bien ce lien entre ces trois grands pôles, où chacun va apporter sa brique. S'agissant des données, on va s'intéresser à leur nature, à leur qualité et à leur protection, c'est-à-dire à tout l'environnement qui a déjà été décrit ce matin autour de la sécurisation des données, de la propriété des données et du rôle de la CNIL.

Ce qu'on réalise peut-être mal, c'est l'incroyable capacité des outils techniques à exploiter les données. Il y a toute une série de questions qu'on se pose aujourd'hui. On a parlé des données de santé. Je ne sais pas si on mesure bien la possibilité aujourd'hui, avec des données ouvertes, disponibles sur Internet, d'améliorer la santé publique, sans pour autant ouvrir des données de l'État sur notre consommation de médicaments ou les

feuilles de remboursement maladie. Il faut bien comprendre que si l'on bloque un certain nombre d'accès à des données, pour des raisons de protection de la vie privée et autres, ces aspects-là seront détournés, parce qu'on travaillera sur d'autres gisements de données publiques qui nous permettront *in fine* d'arriver aux mêmes résultats. C'est donc une question de temps. C'est un phénomène incroyable d'interconnexion de données. Le moindre appel téléphonique donne lieu à des centaines d'enregistrements et de captations de données qui vont des plus classiques – comme la géolocalisation ou le contenu de la conversation – aux plus pointues – les routeurs – les éléments techniques et tous les réseaux par lesquels sont passées les conversations.

De quelle technologie, de quelles données parle-t-on ? Pour visualiser la notion de données, on peut imaginer une base de données de clients qui comporte le nom, le prénom, l'adresse et tout un tas d'informations sur les produits qu'il a achetés. Aujourd'hui, avec le temps et le développement des technologies, on est capable de stocker dans cette même base de données des données dites non structurées. Autant on peut concevoir qu'un ordinateur soit capable d'analyser intelligemment des chiffres, autant c'est moins évident de comprendre qu'**aujourd'hui les ordinateurs et les technologies peuvent analyser de manière semi-automatique, voire automatique, des textes**. Cette compréhension de texte passe par le *web* sémantique, des outils de traitement automatique du langage, mais également des outils de traitement automatique des images et du son. Les technologies de reconnaissance faciale, capables de reconnaître un individu par rapport à une photo, vont être mises en exploitation par *Facebook* pour indexer les photos de vacances tout simplement. Par exemple : « *J'aimerais avoir toutes les photos de mon fils à bicyclette.* »

Tout cela a dépassé le stade de l'expérimentation. Ces systèmes sont disponibles aujourd'hui pour les entreprises et les laboratoires de recherche, en Europe et en France. Nos grands instituts de recherche les développent. Les applications sont à l'œuvre sur des ensembles de données. Dans le monde scientifique, on voit apparaître des alliances sur les données de la recherche. *Research Data Alliance*, un grand consortium paneuropéen, vise à regarder les exploitations envisageables des données scientifiques. D'un côté, on dispose de toutes les données expérimentales, avec des volumes informatiques colossaux, alors que précédemment, on avait un article de cinq pages qui décrivait l'objet de la recherche. La réécriture ou la reconstitution de l'expérience en partant de ces données *versus* ce qu'on faisait à l'époque, en partant directement de la lecture de l'article, pose question.

Ces *big data* se mettent en œuvre dans tous les secteurs des services et de l'industrie. On a parlé du compteur électrique intelligent qui permet aussi de savoir quelle chaîne de télévision est regardée, qui prend sa douche, etc. Si l'on combine toutes ces données à d'autres données, sur le transport en Île-de-France et toutes les données publiques produites par les

collectivités, par exemple, on comprend bien qu'on peut en tirer un grand usage pour la collectivité et de grandes économies. On a rappelé ce qui est envisageable pour les données de santé qui peuvent également servir au bon usage de l'argent public et c'est tout le débat qui nous touche profondément sur l'ouverture des données de l'État. La nomination récente de M. Henri Verdier, *chief data officer*, responsable des données de l'État, vient contribuer au débat sur le *big data*.

Et là on va rebondir sur toutes les questions d'actualité depuis que cette fameuse actrice américaine s'est fait opérer suite à l'analyse de son génome. Ce sujet touche aussi le monde des assurances. Doit-on rembourser les frais de maladie de quelqu'un dont on sait qu'il va tomber malade ? Dans l'assurance automobile, on peut assurer au kilomètre en plaçant un capteur dans le véhicule. Ce capteur peut également capter d'autres informations permettant de connaître le comportement de conduite. Si je suis un bon usager et que je respecte le code de la route, je vais souhaiter pouvoir en bénéficier auprès de mon assureur.

Les exemples se multiplient à l'infini. Toutes les grandes entreprises françaises, aidées par le réseau des pôles de compétitivité et tous les réseaux liés à l'innovation en France, créent aujourd'hui au sein de leurs organisations des laboratoires de recherche dédiés au *big data*. Ils créent également des collaborations avec des chaires parmi les plus grandes universités françaises, sur les thématiques de la banque, de l'assurance, de l'automobile, de la santé, etc.

Les technologies sont prêtes. On attaque le sujet. Ces technologies commencent à travailler sur des ensembles de données, avec toujours cette idée presque absurde qu'on ne sait pas en premier lieu ce qu'on va pouvoir faire de toutes ces données. Que peut-on faire d'un million d'informations concentrées sur un individu ou sur une région ? L'*Alliance big data* nous pousse à être pragmatiques. Travaillons au cas par cas et réfléchissons à cette notion d'écosystème. Le véhicule n'est plus l'apanage du constructeur automobile. Il appartient désormais à tout un écosystème de capteurs, d'assurance, de déplacements dans la ville…

Il existe d'autres thématiques. Vous avez cité en introduction le nuage numérique ou *cloud*, les objets intelligents, les villes connectées. **Le citoyen qui se déplace dans la ville est à la fois élément déclencheur de toute une série de capteurs, soit mobiles soit fixes, et en parallèle, il est porteur et émetteur de toute une série d'informations non structurées issues des réseaux sociaux.**

Mme Anne-Yvonne Le Dain. – Merci pour ce tour d'horizon très complet, qui est, comme la vie elle-même, à la fois vivifiant et inquiétant. C'est le propre de l'humanité, quasiment depuis Adam et Ève, qui ont inventé le mal, comme chacun sait. Le mal va devenir le paradis. Et là, comment arrive-t-on à construire, dans un système qui s'est fait tout seul ? L'Internet n'a pas vraiment été inventé, il est apparu d'un seul coup. Quand

on a décidé de faire les chemins de fer, quelqu'un a inventé un moteur à vapeur, il a décidé de le mettre sur une caisse en fer et il l'a fait avancer en mettant des rails dessous. L'Internet n'a pas été décidé. Les possibilités de l'Internet se sont déployées à grande vitesse et personne n'a véritablement su comment et combien.

Tout à l'heure, Mme Mireille Delmas-Marty a cité expressément l'ancienne prix Nobel d'économie, Mme Elinor Ostrom, qui a inventé le concept de « bien public mondial ». C'est apparu sur la place publique comme une sorte de révélation simple. Maintenant il appartient à tous les êtres humains vivants, scientifiques, intellectuels, industriels, associations, politiques, de construire progressivement cet espace juridique qui fera que notre avenir, espérons-le, soit meilleur et un peu moins angoissant.

Maître Christiane Féral-Schuhl, ancienne bâtonnière du Barreau de Paris, nous vous remercions d'avoir accepté de venir nous faire part de votre analyse. En tant qu'avocate spécialisée en droit de l'informatique et des technologies, vous allez faire état, de manière très synthétique, des problématiques qui résultent des sept zones de risques que vous avez identifiées, ainsi que des parades que l'on peut imaginer pour limiter tout cela. Sachant que tout est à faire et à construire, mais que tout est, en partie, déjà pensé.

Je n'oublie pas ce qu'ont dit MM. Jean-Dominique Nollet et Pascal Chauve qui nous rappellent au fait que le droit construit et détermine ce qui va être la vie des individus dans leurs forces et leurs faiblesses. Ce ne sont pas que des théories intellectuelles qui régulent des sociétés. Ce système est extrêmement concret et important.

Me Christiane Féral-Schuhl, avocat spécialisé en droit de l'informatique et des technologies, ancien bâtonnier du Barreau de Paris. – Je vais peut-être réagir à ces propos. Vous disiez que l'Internet est apparu d'un seul coup. C'était au début des années 1990. En vingt ans, les technologies nous ont obligés à repenser tous les fondamentaux de la société. Les institutions ont été bouleversées. Tous les modèles ont été confrontés à l'Internet, et, bien sûr, le cadre juridique aussi. Mais, ce que j'ai pu constater à travers les années, c'est qu'à chaque fois que se pose un problème technologique et que l'on regarde les textes existants, les principes fondateurs de notre droit apportent des réponses satisfaisantes.

On a évoqué uniquement la loi informatique et libertés. Elle pose des règles fondatrices et c'est sous forme d'avis et de recommandations que la CNIL s'est exprimée, apportant des précisions aux différents cas auxquels nous avons été confrontés. Et l'on trouve dans notre droit ces principes fondateurs sans avoir besoin de la prolifération des textes que l'on a pu voir ces dernières années.

À propos du thème particulier de la sécurité, j'ai constaté que le citoyen a toujours une attitude schizophrène. Nous avons toujours cette

recherche de la sécurité, de l'État sécuritaire, et puis, en face, cette volonté de liberté qui est revendiquée sur Internet. C'est, par exemple, tout le débat qu'a suscité le passe *Navigo* de la RATP. À sa sortie, ce passe permettait de tracer par la collecte des données le chemin parcouru dans le métro. Un tollé s'est élevé, fondé sur le principe de la liberté d'aller et de venir, liberté constitutionnelle. Dans le même temps, très spontanément le voyageur va se tourner vers la RATP pour s'indigner de son incapacité, avec tous les outils dont elle dispose, à suivre la trace des agresseurs de voyageurs.

On retrouve cette même logique avec la vidéosurveillance pudiquement appelée « vidéoprotection ». Chacun refuse qu'on surveille ses allées et venues dans son immeuble, en revanche, dès qu'il y a un cambriolage, il s'interroge sur l'utilité de tous ces systèmes.

Un dernier exemple avec les contrôles aéroportuaires. On vit comme un déshabillage numérique ces contrôles, et, dans le même temps, on ne comprendrait pas que le transporteur ne remplisse pas son obligation de sécurité renforcée.

Cette problématique est déclinable à l'infini. Suivant le moment, on va changer de positionnement et faire bouger le curseur, tantôt en voulant être protégé, tantôt en voulant revendiquer cette zone de liberté. Face au thème de la liberté d'expression, du droit à l'information, du droit de savoir selon certains, on va tout de suite voir la limite posée par la protection de la vie privée, la revendication de l'intimité de la vie privée.

Cela m'amène à dire qu'il faut peut-être définir ce qu'est la vie privée, comment elle s'appréhende aujourd'hui. Dans le modèle économique actuel qui consiste à livrer ses données personnelles, à alimenter le système de l'Internet, la conscience de l'internaute, ou en tout cas son attention, doit être attirée sur deux règles fondamentales de l'Internet : la mémoire d'éléphant – « *je donne de l'information et elle ne disparaît jamais* » – et le préjudice sur Internet qui peut être à l'échelle planétaire.

Vous m'avez demandé d'aborder plus particulièrement la problématique sous l'angle de l'entreprise. L'entreprise est partie prenante de cet univers, elle fait partie de la société numérique. Il y a cette conscience aussi à l'intérieur de l'entreprise. Le chef d'entreprise est responsable de son bateau. Dans le même temps, le numérique fait que tout s'instaure par la voie des dialogues, des échanges et des enrichissements. Beaucoup de choses ont changé dans le modèle de l'entreprise.

Une première réaction consiste à protéger le bateau en faisant attention aux voies d'eau. La première zone de risque consiste donc à identifier ce qui peut provoquer ces voies d'eau.

Et, déjà, il apparaît une première difficulté qui vient du **défaut de gestion des contrôles d'accès**. Les entreprises font de plus en plus appel à des prestataires ou à du personnel intérimaire et le problème des *badges* d'accès n'est pas réglé. Pour les grands projets informatiques, des armées de

prestataires entrent dans l'entreprise, et, lorsque le projet est terminé, on ne va pas nécessairement changer les codes à la sortie. Sur quelque chose d'aussi basique que les *badges*, on constate des défaillances.

Par ailleurs, aujourd'hui il est facile de prendre la maîtrise d'un ordinateur à distance. Cela suppose que des codes soient communiqués.

D'autre part, **certaines grandes entreprises ou administrations livrent à travers leurs appels d'offres l'intégralité de leur système d'information**. C'est pourquoi la politique informatique d'une entreprise est absolument déterminante pour éviter de livrer clé en main des informations stratégiques sans traiter le volet confidentialité. En effet, **la clause de confidentialité ne va apparaître qu'au moment où le contrat va être signé avec le prestataire**. Avant cela, une mine d'informations stratégiques relatives aux modalités d'accès et aux systèmes de traitement est ainsi livrée en pâture à des tiers.

Ensuite, il y a tout ce qui est lié à la surveillance électronique. Par exemple, **les mises à jour de pare-feu ne sont pas faites systématiquement**. Or de nouveaux virus apparaissent au quotidien et nécessitent donc une mise à jour périodique. La responsabilité de l'entreprise se joue déjà à ce simple niveau. Certes, les atteintes en provenance de l'extérieur sont réelles, mais, souvent, elles sont dues à des négligences de ce type.

Les atteintes peuvent aussi venir de l'intérieur. **85 % des risques qui se concrétisent dans l'entreprise viennent du personnel, par malveillance ou par négligence. La sécurité passe par des mesures basiques, *via* des audits, des tests d'intrusion.** L'essentiel des risques se situe déjà à ce niveau-là.

La deuxième zone de risque est liée au risque de discontinuité du service. L'entreprise fonctionne dans un dialogue permanent avec l'extérieur. **Au niveau du système d'information et du traitement d'information, il existe une vulnérabilité très forte de l'entreprise qui ne traite pas suffisamment la réversibilité ou la transférabilité d'un système.** Par exemple, si l'application de gestion des commandes s'arrête, quels sont les scénarios qui doivent être mis en place pour assurer la continuité de l'entreprise ? Cette chaîne de fabrication passe par des mesures de protection informatiques et technologiques : plan de contournement d'activité, plan de reprise d'activité, de façon à s'assurer de la continuité des logiciels et garantir la continuité de service. J'invite les entreprises à identifier toutes leurs applications sensibles afin de gérer l'incident, le risque de discontinuité de service.

La troisième zone de risque est liée à la perte des archives. Le chef d'entreprise est responsable de la conservation de la mémoire de l'entreprise. L'administration a cette même obligation. Aujourd'hui on ne raisonne plus qu'en termes d'archives numériques. **La politique d'archivage doit favoriser**

une approche hiérarchisée des archives. La CNIL propose trois niveaux de hiérarchie : les archives courantes, les archives intermédiaires et les archives définitives.

Pourquoi la CNIL ? Le volet des données personnelles est incontournable dans les archives et la durée de conservation doit être définie. Cette distinction que propose la CNIL est tout à fait pertinente. Les données concernant un client pendant l'exécution du contrat iront aux archives courantes. Les données servant un intérêt en cas de contentieux comportent un délai de prescription légale et iront aux archives intermédiaires. Enfin, les données qui présentent un intérêt scientifique, historique, doivent être conservées dans le temps et elles iront aux archives définitives pour que la mémoire de l'entreprise puisse être restituée dans un ou deux siècles.

Cela pose **la question de la lisibilité des données dans le temps par les appareils de lecture**. Les supports d'il y a dix ans sont déjà obsolètes aujourd'hui. Une politique d'archivage inclut à la fois la conservation et la mise à jour des archives afin de garantir la lisibilité, l'accessibilité, l'authenticité des informations. L'intégrité des informations, la pérennité des solutions techniques d'archivages sont importantes. Elles supposent un **travail d'indentification des données sensibles**. Nous sommes là au cœur de la problématique de la sécurité.

La quatrième zone de risque est liée à l'atteinte à la vie privée. Ces risques existent au sein de l'entreprise, notamment *via* la messagerie. Comment s'articulent les sphères privée et professionnelle au moment où elles ne recouvrent plus les mêmes unités de temps et de lieu de travail ? J'ai tendance à dire que le code du travail est dépassé sur ce point. Pour toute une catégorie de salariés, les trente-cinq heures n'ont plus beaucoup de sens, quand on sait que leur temps de travail se prolonge chez eux et que, sur leur lieu de travail, des démarches personnelles sont faites. Tout cela pose le problème de l'atteinte à la vie privée par les réseaux sur le lieu de travail.

Peut-on interdire l'usage de l'Internet dans l'entreprise ? Non, mais en même temps, **le chef d'entreprise est responsable de tout ce qui est transféré par le réseau, notamment des téléchargements effectués par ses salariés dans son entreprise par la voie des accès Internet**, de la même manière qu'il serait responsable d'un réseau de trafic de drogue ou de prostitution qui se mettrait en place dans son entreprise.

Des dispositifs de contrôle doivent donc être prévus. Le chef d'entreprise en a le droit, à condition de respecter deux règles : la règle de la transparence et la règle de la proportionnalité. Dès lors il faut se demander comment donner une place à la sphère privée de l'employé, comment gérer intelligemment toutes ces relations et ces modifications qui se mettent en place au sein de l'entreprise.

La cinquième zone de risque est liée à l'atteinte à la liberté d'expression, une liberté fondamentale que beaucoup revendiquent. Mais, au sein de l'entreprise, beaucoup de choses changent. *Quid* de la liberté syndicale ? Va-t-on pouvoir utiliser la messagerie ? Peut-on utiliser le site de l'entreprise ? Que peut-on divulguer quand on sait que les syndicats peuvent avoir accès à des informations couvertes par le secret ? La diffusion de certaines informations pose des problèmes de risque. Si la liberté d'opinion est garantie, notamment aux fonctionnaires, des règles sont à rappeler : le secret professionnel, la discrétion professionnelle, le devoir de réserve, pas d'utilisation à des fins politiques, pas d'information à des fins syndicales… Tout cela fait partie des zones de prise de conscience par les entreprises.

La sixième zone de risque est liée au non-respect de la loi informatique et libertés. Je ne vais pas revenir sur les éléments apportés par Mme Falque-Pierrotin, sinon pour rappeler que les entreprises sont amenées à contribuer à la sécurité, notamment par **l'obligation de conservation des données de connexion pendant une année**. Dans certaines entreprises qui ouvrent des possibilités d'accès en *Wi-Fi* pour leurs clients par exemple, ou pour les visiteurs, des garanties sont à prendre en matière de sécurité. Cela s'inscrit dans le plan de lutte contre la cybercriminalité qui a été évoquée.

La mise en place des **accès biométriques** est de plus en plus généralisée dans les entreprises. Elle soulève cette recherche d'un juste équilibre entre la vie privée et le besoin de sécurité au sein de l'entreprise.

La septième zone de risque est liée au non-respect du code de la propriété intellectuelle. Parmi les problèmes les plus courants, figure l'utilisation de logiciels sans licence et la conformité des sites *web*, de l'Intranet et des bases de données.

D'une part, je voudrais insister encore une fois sur le problème du téléchargement au sein de l'entreprise et de la responsabilité particulière du chef d'entreprise, lorsqu'une infraction a été commise et alors qu'il est responsable du réseau.

D'autre part, j'attire l'attention sur l'utilisation de l'*open data* et des biens communs. Il faut être conscient que cela peut fragiliser l'entreprise. Dans une démarche visant à favoriser l'*open data* et le logiciel libre, il faut connaître les contraintes du dispositif. Le concept même du logiciel libre est l'inversion du raisonnement du droit d'auteur. Le droit d'auteur dit : « *Je ne veux pas qu'on puisse s'approprier le logiciel dont je suis l'auteur.* » En contrepartie, tous ceux qui l'utilisent partagent les évolutions et l'enrichissement. Et certaines entreprises peuvent être obligées de communiquer et de partager des informations qui viennent sur ce terrain-là mettre en difficulté leur politique de sécurité.

Pour finir, je vais vous faire part d'une préoccupation. Aujourd'hui la sécurité est omniprésente et, à chaque fois que la liberté avance, les libertés fondamentales peuvent reculer. La question est de trouver le juste

équilibre. Je suis frappée de voir que notre système judiciaire et juridique de manière générale, a mis en place un certain nombre de protections, notamment les prescriptions. Je vais prendre l'exemple des **prescriptions de la presse**, où les diffamations et injures sont limitées à trois mois. Pour moi, **elles n'ont pas de sens sur Internet parce que le préjudice perdure**. Les entreprises peuvent en être victimes. Aujourd'hui, la guerre économique se fait aussi sur le terrain de la diffamation pour les entreprises et pour les chefs d'entreprise. En règle générale, cette durée de prescription est toujours limitée à trois mois. Et, même si elle a été prolongée à une durée de trois ans pour certains délits aggravés, dans certains cas comme la pédopornographie, la prescription est limitée à trois mois en règle générale. Cette durée me paraît aberrante par rapport à la réalité de ce que l'on constate sur Internet.

À l'inverse, il y a une possibilité d'effacement des peines, pour un chef d'entreprise par exemple, et les casiers judiciaires ne sont pas partagés à l'échelle de l'Internet. Nous avons une faculté d'effacement dans la vie de tous les jours, ce qui n'est pas le cas de l'Internet. En tant qu'avocate, je vois des drames, des chefs d'entreprise dans l'incapacité de se reconstruire et de reconstruire leur entreprise à cause de diffamations, d'injures, voire de situations où ils ont été largement médiatisés suite à des gardes à vue ou à des actions qui ont pu être engagées. Parfois elles ont conduit à des relaxes, parfois à des peines, mais en tout cas elles perdurent sur Internet. De ce point de vue, la décision qui a été rendue par la Cour de justice de l'Union européenne est extrêmement intéressante. Pour la première fois, on est dans un droit de déréférencement à travers la possibilité de déréférencer certains liens sur certains contenus.

C'est différent du droit à l'oubli qui est la faculté de pouvoir effacer complètement une information, ne plus la faire exister sur Internet. C'est, par exemple, le souhait d'un jeune qui s'est ridiculisé dans une vidéo en fêtant l'obtention de son baccalauréat et qui en est pénalisé dans sa vie professionnelle ou sentimentale pendant des années. On peut imaginer quand même ne pas être lié *ad vitam aeternam* à certains comportements qu'on a pu avoir à un moment donné. Donc oui au droit à l'oubli dans ce cas-là. En revanche, les opposants au droit à l'oubli disent une chose très importante : est-ce que chacun va pouvoir réécrire son histoire telle qu'il a envie de l'écrire ? C'est le problème de la mémoire. Aujourd'hui, l'archivage va s'écrire à travers le numérique. La sécurisation de l'histoire, le devoir de mémoire, va s'écrire et se décliner partout. Il faut donc faire attention à cette faculté.

La Cour de justice de l'Union européenne ouvre une porte. Peut-être faut-il en profiter. C'est extrêmement intéressant. L'information ne disparaît pas d'Internet, mais c'est le référencement qui disparaît. **Il faudrait arriver à faire respecter sur Internet la présomption d'innocence, le respect du contradictoire et le respect des prescriptions** qui sont des protections et qui sont inscrits dans ces principes fondateurs que j'évoquais au début.

Mme Anne-Yvonne Le Dain. – Nous vous remercions de ces ouvertures et en même temps du rappel de ces inquiétudes constantes. Le droit construit la vie, vous en avez fait une démonstration magistrale.

Avant d'ouvrir le débat général, je voudrais passer la parole à notre collègue député, Jean-Yves Le Déaut, premier vice-président de l'OPECST. Pourriez-vous regrouper vos interrogations en une seule ?

Jean-Yves Le Déaut, député, premier vice-président de l'OPECST. - Les débats de ce matin sont passionnants. Nous avons déjà suivi cette question avec le sénateur Bruno Sido et cela a donné lieu à une audition publique de l'OPECST en 2013 sur « *Le risque numérique : en prendre conscience pour mieux le maîtriser* ». Nous y avions examiné les risques pour la défense et pour la société civile. D'autre part, je suis rapporteur général de l'Assemblée parlementaire du Conseil de l'Europe pour la science et la technologie, et, à ce titre, on vient de travailler sur ces sujets au Conseil de l'Europe.

En vingt ans, tout a bougé. Non seulement le citoyen a compris l'intérêt d'utiliser l'Internet et ses applications, mais, en même temps, il souhaite une protection, une sécurité et il ne comprend pas les ressorts techniques de ce qu'il utilise. L'élu encore moins. L'élu est déboussolé devant ces avancées scientifiques et techniques. Le rôle de l'OPECST, c'est finalement de rendre compréhensible les questionnements pour que l'élu puisse décider. C'est de vous donner la parole et c'est ce que nous faisons aujourd'hui.

Vous avez très largement indiqué les dévoiements du système. Ils ne sont pas de même nature selon qu'on exploite des données disponibles, gigantesques, qu'on est capable d'aller puiser par des outils informatiques puissants. Cela donne des renseignements, y compris commerciaux.

Les données frauduleuses ne sont pas de même nature. Et là, ce que demandent globalement le Conseil de l'Europe, l'Union européenne et la communauté internationale, c'est une sorte de régulation. D'abord en affirmant, comme l'ont dit les Nations unies, lors de l'assemblée générale du 18 décembre 2013, le droit à la vie privée à l'ère du numérique ; ensuite, en travaillant de plus en plus sur la gouvernance de l'Internet, car il faut progresser sur cette question – une réunion à Istanbul aura lieu sur ce thème du 2 au 4 septembre 2014 ; et, enfin, en complétant un certain nombre de textes internationaux qui existent déjà, et c'est le rôle du Conseil de l'Europe.

Dans ses recommandations, le Conseil de l'Europe propose des avancées pour améliorer le cadre juridique au niveau international, aussi bien sur l'entraide judiciaire en matière de cybercriminalité que sur la protection des personnes.

Le Conseil de l'Europe a recommandé de veiller à la protection de la vie privée et la sécurité de l'utilisateur. Celui-ci doit être protégé en ligne, notamment face à l'interception, la surveillance, le profilage et

l'archivage des données. Il faut que cela soit clair et que le consommateur le sache.

Parmi toutes ces recommandations, je voudrais attirer l'attention sur le fournisseur de services en ligne, commercial ou institutionnel. **Il faut qu'il soit identifiable et transparent et qu'il affiche clairement sa politique**, et ce n'est pas le cas aujourd'hui. Nous ne savons pas d'où viennent ces services. C'est comme si on achetait des produits sans savoir qui nous les vend. Ce fournisseur de services collecte énormément de données qui lui sont fournies par l'utilisateur et qu'il peut utiliser sans que, de manière transparente, l'utilisateur en soit averti. Sur ce point, nous devons progresser.

Deuxièmement, je souhaiterais vous interroger sur l'obligation de mettre en place pour ces questions un médiateur du citoyen. Celui-ci pourrait être désigné par chaque fournisseur, être facilement joignable et avoir obligation de répondre. Certains fournisseurs en ont un.

Troisièmement, je souhaiterais qu'un travail soit accompli sur le recours à l'identification réelle en ligne, que ce soit par des outils d'authentification, et certains existent déjà **– la signature électronique par exemple, mais on pourrait en développer d'autres, notamment le recours à des tiers de confiance**, ce qui n'a pas toujours été fait.

Quatrièmement, le droit à l'oubli me paraît important. Même si parfois, de manière schizophrénique, ce sont les utilisateurs eux-mêmes qui ont émis ces données, la possibilité de retirer des données, des contenus et des informations doit exister. Et ce, malgré le point que vous avez indiqué, Maître Christiane Féral-Schuhl, à savoir que tout fait partie de la mémoire. Je ne suis pas sûr que lorsqu'on a multiplié par mille les données en ligne sur un seul individu, il y ait un intérêt historique à toutes les conserver. L'individu doit pouvoir demander à un fournisseur de retirer les données le concernant.

Cinquièmement, les fournisseurs doivent s'interdire de fournir les identifiants des utilisateurs, les « *user ID* », sauf avec leur autorisation.

Sixièmement, les *cookies* existent, on le sait, et certains servent tout simplement à mesurer un certain nombre de besoins de l'utilisateur de l'ordinateur. Les *cookies* devraient à mon sens avoir une **durée de vie limitée**, sauf si les utilisateurs les acceptent. C'est possible techniquement. Rien que cette limitation de la durée de vie des *cookies* ferait changer les choses.

Tant que nous aurons des réglementations nationales sur des sujets qui ont des conséquences internationales, nous n'y arriverons pas. Quel est le système juridique qui va s'imposer ? Celui du pays de l'utilisateur ? Celui du consommateur final ? Celui du constructeur ? Pour le consommateur, le droit applicable serait le plus favorable entre celui du pays d'origine et celui du pays de service.

Il faudrait également travailler sur la gouvernance mondiale de l'Internet. Sans vouloir une révolution, on peut espérer avoir une charte de l'Internet signée par tous les pays, traitant notamment de l'attribution des **noms de domaine** et d'un certain nombre de sujets. Ces idées ont peu évolué depuis Tunis, je crois, il y a une dizaine d'années, et, comme on l'a vu lors de la dernière réunion à Montevideo**.**

Voilà quelques points, monsieur le président, que je souhaitais livrer à votre réflexion. Je suis très heureux que nos deux rapporteurs aient choisi ce sujet d'investigation. Actuellement, l'Office traite aussi d'un autre sujet relatif au numérique sur les données médicales, « *Le numérique au service de la santé* », dont les rapporteurs sont M. Gérard Bapt, député, et Mme Catherine Procaccia, sénateur.

Débat

M. Bruno Sido. – Nous allons profiter des minutes qui nous restent pour échanger.

Me Christiane Féral-Schuhl. – Merci pour votre intervention. Il me semble qu'**aujourd'hui on n'a pas besoin de légiférer**. Deux points me paraissent les plus critiques. Premièrement la sensibilisation à l'information avec obligation pour les fournisseurs de bien renseigner le consommateur. Informer l'internaute, que lorsqu'il choisit la page privée de *Facebook*, cela ne veut pas dire que cette page est confidentielle. **Tout un travail de sensibilisation est à faire pour que les consommateurs arrêtent de fournir tous azimuts des données personnelles.**

Le deuxième élément à consolider aux plans national, européen et international, est lié aux chargés d'enquête, de façon à appréhender les auteurs d'infraction. Depuis la loi Godfrain, l'arsenal est extrêmement riche, en tout cas, je n'ai jamais eu de difficultés à l'appliquer. En dehors du domaine pénal, on a tout ce qu'il faut en termes de textes, et même parfois trop, puisque nous avons des hésitations. En matière pénale, je sais, comme vous, qu'il faut un texte pour que l'infraction puisse exister. On y arrive à 95 %. Le délit d'usurpation numérique a été rajouté. Je me permets d'insister là-dessus. Les cadres juridiques se juxtaposent et je crains que cela finisse par susciter une difficulté. L'ensemble des juristes vous diront qu'il y a une prolifération de textes qui s'emboîtent, compte tenu du travail européen qui se fait.

Je voudrais également faire une observation sur la charte Internet dont vous avez souligné l'intérêt. Aujourd'hui, les acteurs sont transversaux, en particulier les moteurs de recherche, qui forment un État quasiment à eux

seuls. En ce qui concerne les données personnelles, nous sommes arrivés à faire adhérer les entreprises américaines au *Safe Harbor*. L'idée que les grands acteurs soient tenus d'adhérer à ce que vous appelez la charte informatique est absolument à encourager et à imposer.

Enfin, je suis frappée par les ravages provoqués par les propos anonymes, cette possibilité sur Internet d'avoir des pseudonymes. La liberté d'expression, qui est une liberté fondamentale, ne prévoit nulle part qu'elle s'applique à des personnes anonymes. Rien n'empêcherait, dans l'élaboration d'une charte constitutionnelle numérique, si on devait aller dans cette direction, de rappeler l'obligation d'identification. Aujourd'hui, lorsqu'un journaliste utilise un pseudonyme, on peut le retrouver grâce au rédacteur en chef et à la responsabilité en cascade qui s'applique en matière de propriété littéraire et artistique. Mais, avec le pseudonyme, on se heurte à l'obstacle de l'anonymat. Ce problème doit être surmonté, ce qui règlerait déjà une partie non négligeable des problèmes, puisqu'un certain nombre de personnes aiment bien s'exprimer avec violence sur Internet, en général sous couvert d'anonymat.

Mme Mireille Delmas-Marty. – Je vais continuer la discussion sur la gouvernance mondiale d'Internet. Si je comprends bien, une charte signée par tous les pays du monde est un objectif lointain. Pourquoi est-elle bloquée ? Si l'on n'y arrive pas tout de suite, peut-on considérer que les organisations régionales comme celles que nous avons en Europe puissent fonctionner comme un laboratoire d'expérimentation ?

Cela m'amène à une autre question concernant le représentant d'Europol, M. Jean-Dominique Nollet. Pensez-vous que le parquet européen, prévu par le traité de Lisbonne, pourrait jouer un rôle dans le domaine de la cybercriminalité ? Même si ce n'est pas évident sur le plan du montage juridique, serait-ce souhaitable ?

M. Jean-Dominique Nollet. – Ce parquet européen est une entreprise qui se bâtit doucement, avec un intérêt qui est clair. **En matière de cybercriminalité, nous n'en voyons pas le manque.** Dans mon travail de tous les jours, quand on monte des opérations pour démonter des réseaux de robots informatiques ou *botnets*, on a tous les outils juridiques pour travailler.

Là où l'on a des besoins, c'est pour travailler plus vite et plus en profondeur. Pourquoi plus vite ? Parce que pendant que nous démontons les infrastructures des groupes criminels, ces groupes nous attaquent. Dans le monde physique, on arrête physiquement les gens et ils « gigotent » plus ou moins. Sur Internet, ils se livrent à des attaques par déni de service (*DDoS*). C'est très dynamique, très rapide, et donc il faudrait pouvoir adapter notre structure de démantèlement à cette vitesse.

M. Bruno Sido. – Mais disposez-vous de tous les outils juridiques quand vos attaquants sont en Chine, en Russie ou ailleurs ?

M. Jean-Dominique Nollet. – Ce n'est pas un problème juridique. Nous devons avoir les moyens pour mener notre opération à bien. Démanteler les centres de contrôle et de serveurs ou désinfecter les machines.

Je vais rebondir sur votre question. La vision que nous avons autour de cette table est très centrée sur la France et un peu sur l'Europe. **Vous pourrez faire une charte, mais techniquement l'anonymat est possible sur Internet**, en vous connectant au logiciel *Tor* par exemple. Entre 800 000 et un million de personnes utilisent *Tor*. Ces utilisateurs sont parfois bienveillants, ce sont des journalistes par exemple, parce qu'ils souhaitent entrer en contact avec des personnes qui sont en souffrance dans leur pays ou parce qu'ils sont exposés et que, si un État saisit leurs serveurs de messagerie, l'anonymat de leurs sources disparaît.

Donc l'anonymat est techniquement possible sur Internet. Même si vous faites signer une charte par les opérateurs Internet, cela ne changera absolument rien. Et je renverse la question : n'est-il pas fondé, pour les forces de l'ordre de l'Union européenne, d'essayer de lever cet anonymat de façon proportionnée, quand l'infraction le justifie ?

Mme Anne-Yvonne Le Dain. – La question de l'anonymat est fondamentale. Cette question n'est pas si simple parce qu'on touche à des questions assez délicates. Si l'on pense à une loi, encore faut-il qu'elle soit votée par une majorité. De plus, une loi est nationale. Mais c'est une question, effectivement. Une charte me semble une étape pertinente, qui aura le mérite d'être partagée par plusieurs pays européens et au-delà. C'est quelque chose qu'on est obligé de construire. Maintenant, j'entends votre urgence.

M. Jean-Dominique Nollet. – Je me suis mal exprimé. Je ne dis pas qu'il ne faut pas de loi en la matière. Je dis juste que **la loi peut être contournée par la technologie en quinze secondes**.

Mme Anne-Yvonne Le Dain. – Que faire alors ?

M. Jean-Dominique Nollet. – Sur l'anonymat, ma proposition est de dire la chose suivante. Je me promène dans la rue en tant que citoyen. Si un policier me contrôle, je vais lever mon anonymat puisqu'il existe un cadre juridique pour ce contrôle. Essayons aussi de maintenir sur la planète la capacité pour les forces de l'ordre de lever l'anonymat pour des gens qui portent une cagoule sur Internet.

M. Bruno Sido. – Disposez-vous actuellement de tous les outils juridiques nécessaires ?

M. Jean-Dominique Nollet. – Actuellement, il faut des outils avancés pour pouvoir lever cet anonymat. C'est ce que j'évoquais dans mon introduction à propos de la captation de données à distance.

Me Christiane Féral-Schuhl. – Cela m'évoque le problème des cybercafés. À un moment donné, on a dit que c'est de là que venaient la plupart des contenus illicites. J'ai constaté que certains cafés affichent au moment de la connexion une page du cybercafé qui dit : « *Pour nous conformer à la loi, nous vous demandons votre identité* ». Vous donnez votre nom et un certain nombre d'informations. Cela signifie que nous ne pouvons créer une identité virtuelle, le café se réservant même parfois le droit de demander la pièce d'identité à son client. Je ne dis pas que c'est la solution mais c'est le signe d'une prise de conscience.

À noter, à propos de liberté, que lorsque je m'installe dans un cybercafé, j'utilise la connexion *Wi-Fi* du café ; quand je suis chez moi, j'utilise ma connexion. C'est le responsable de ma connexion qui doit rendre compte à la justice de ce qui se passe. Il peut donc y avoir une justification dans le fait que, oui, je vous autorise à vous connecter, mais ce qui va circuler par ce réseau est de ma responsabilité de cybercafé, donc je vous demande des informations.

Mme Anne-Yvonne Le Dain. – Cela renvoie à la question de l'anonymat. Dans le droit français, on n'a pas le droit de se promener dans la rue avec le visage couvert.

M. Bruno Sido. – Pas en tchador par exemple.

Mme Anne-Yvonne Le Dain. – C'est une particularité du droit français, mais c'est dans notre loi. Et donc la question est d'une nature extrêmement délicate et complexe. Le sénateur Bruno Sido et moi-même ne partageons pas forcément la même analyse.

Dans un monde où l'individu devient le nœud de tout et peut se connecter à tout, dans des communautés variées, improbables, introuvables, pertinentes, éventuellement profitables, je crois qu'on est véritablement dans une nouvelle dimension économique. Le XXIe siècle, c'est l'ère du numérique, de l'Internet, d'une liberté individuelle qu'il faut corréler avec les libertés sociales, avec la sécurité individuelle et sociale.

Seconde table ronde

M. Pierre Lasbordes, ancien député, ancien membre de l'OPECST. – Cette table ronde est très riche, puisqu'elle invite des philosophes, des représentants des consommateurs, des techniciens, des avocats, une responsable d'un office étatique de la police et un psychopathologue.

À 16 heures, nous aurons la chance d'écouter Mme Axelle Lemaire, secrétaire d'État chargée du numérique, puis les débats reprendront.

Je vais tout de suite donner la parole à M. Bernard Stiegler qui va nous donner sa vision d'un thème ayant déjà fait l'objet d'un rapport de l'OPECST, dont j'ai été membre pendant dix ans : la sécurité des réseaux numériques.

M. Bernard Stiegler, philosophe, directeur de l'Institut de recherche et d'innovation du Centre Georges Pompidou (IRI), membre du Conseil national du numérique. – Je vais commencer par un mot axiomatique qui va être à la base de tous mes propos. Je soutiens, avec la communauté des philosophes du XXIe siècle, une thèse qui est à l'origine de la philosophie, une thèse de Socrate selon laquelle toute technique est ce que les Grecs appellent un *pharmakon*. Comme le disait Claude François, un marteau sert à construire sa maison, mais aussi à assassiner son voisin. Toute technique a cette double dimension, plus ou moins visiblement, et plus ou moins sensiblement. Par exemple, une technique comme le biface a mis près d'un million d'années à se constituer, en passant du *chopper* (il y a 2,8 millions d'années) au biface (il y a deux millions d'années). Le temps d'appropriation de cette technique a été relativement long.

Le numérique commence avec le *web* qui est apparu le 30 avril 1993. En l'espace de vingt-et-un ans, il a bouleversé absolument tout : la fiscalité, le commerce, l'enseignement, les pratiques scientifiques, la vie politique. Cette sorte d'éclair foudroyant pose **un problème d'une difficulté colossale à savoir la capacité de la société à transformer la toxicité potentielle du *pharmakon* Internet en un système thérapeutique, curatif**. En vingt-et-un ans, une communauté de sept milliards d'individus doit arriver à reconstruire des modèles, là où, autrefois, encore pratiquement jusqu'à la révolution industrielle, vers 1780, on avait encore deux ou trois siècles pour s'approprier une mutation technologique. Au début de l'humanité, c'était incomparablement plus long.

Nous avons donc affaire à un problème de pharmacologie, au sens large de Socrate, absolument exceptionnel. D'une manière ou d'une autre, l'OPECST est toujours confronté à ces problématiques. C'est pourquoi il faut faire des choix technologiques. Une enceinte politique doit arbitrer de tels choix qui ne sauraient être laissés au seul marché car ce dernier a la faiblesse de ne représenter que des intérêts particuliers. Je sais bien que certaines

théories du marché posent que la sommation de ces intérêts particuliers produit un intérêt général, mais c'est un autre sujet dans lequel je ne vais pas m'engager.

En tant que membre du Conseil national du numérique (CNNum), je signale la récente parution du rapport sur la neutralité des plates-formes, publié par le CNNum et pour lequel M. Francis Jutand, son principal rédacteur, a accompli un travail exceptionnel d'analyse sur les **dangers portés par les logiques de plates-formes qui sont actuellement mises en œuvre**.

Alors qu'est-ce qu'une plate-forme ? Le *web* en est une d'une certaine manière. Mais à cette plate-forme sont venues s'ajouter des plates-formes de type *Apple* ou *Facebook*, lesquelles distordent les logiques initiales de la plate-forme qu'était le *web*.

Vous aurez noté aussi que le patron de *Springer* a adressé une lettre ouverte à M. Éric Schmidt, en avril 2014, intitulée : « *Nous avons peur de Google.* » C'est une première dans l'histoire du capitalisme industriel qu'un PDG d'une entreprise d'une telle ampleur déclare qu'il a peur de quelque chose. Normalement, un PDG n'a peur de rien. Cette rhétorique indique qu'un malaise s'est installé autour du numérique et qu'il faut absolument l'analyser en détail.

Ce malaise s'est installé depuis environ un an, depuis l'affaire Snowden en particulier et même avant, puisque, il y a trois ans, l'Institut de la culture des réseaux à Amsterdam, que dirige M. Geert Lovink, un activiste très pronumérique, a changé de ton et a engendré ce que j'ai appelé dans une conférence « *le blues du* Net ». **Le doute s'est installé dans la communauté des activistes qui sont des militants du numérique.**

Ce malaise profond, on le retrouve aussi dans le rapport sur la fiscalité de l'économie numérique, remis par Pierre Collin et Nicolas Colin, un problème qui avait déjà été souligné par M. Philippe Marini, sénateur. La fiscalité à l'époque de l'économie des données est littéralement en voie de désintégration avec les plates-formes que j'ai évoquées et toutes sortes de modèles qui sont liés au numérique.

Ce *blues* du *Net* se produit maintenant dans le champ scientifique, par exemple autour des données massives ou *big data*. M. Chris Anderson, qui fut un prescripteur en tant que rédacteur en chef de *Wired*, la revue de référence de la *Silicon Valley*, a publié, en juin 2008, un article intitulé : « *The end of theory : data deluge makes the scientific method obsolete* ». Dans cet article, il prenait *Google* comme un exemple caractéristique. Premièrement, ***Google*, en faisant évoluer la pratique des langues à travers son moteur de recherche, les *AdWords*, l'autocomplétion, la traduction automatisée et bien d'autres services, a totalement transformé le rapport au langage et l'évolution des langues**. Or, constatait Chris Anderson, il n'y a pas de linguiste chez *Google*, si ce n'est pour traiter des problèmes d'interface.

Ce qui a permis tout cela, ce n'est pas la linguistique, ce sont les mathématiques appliquées mettant en œuvre des chaînes de Markov à l'échelle de ce qu'il appelle le « *déluge de données* » (*data deluge*), c'est-à-dire ce qu'on appelle aujourd'hui le *big data*.

M. Chris Anderson ajoute que l'OMS n'a pas su anticiper l'évolution de l'épidémie de grippe, mais que *Google* l'a fait très bien, sans médecin. Donc **on n'a plus besoin de ces savoirs théoriques, avec des modèles, des hypothèses, des causalités. On n'a plus besoin que de corrélations.** C'est M. Viktor Mayer-Schönberger, de l'Institut Internet de l'université d'Oxford, qui le dit. M. Chris Anderson ne le dit pas, mais il décrit déjà cela.

Quatre mois plus tard, M. Alan Greenspan, président de la Réserve fédérale américaine, est auditionné devant le Congrès à la suite de la crise des *subprimes*. Ses explications consistent à dire que le *trading* automatique, la délégation aux automates – ce qui a fait dire aux prix Nobel d'économie, qu'il n'y avait plus besoin de modèles théoriques, d'hypothèses –, et que tout cela, par la sommation automatisée, ne pouvait que marcher très bien, alors que cela ne marche pas du tout ! Et il a refusé que lui soit reproché d'avoir mis en œuvre cela parce que toute la théorie économique avait en fait renoncé à la théorie économique en disant qu'il fallait remplacer la prise de décision des humains par des systèmes automatisés. Cette audition du 23 octobre 2008 est en ligne sur *YouTube*.

Le numérique est un *pharmakon* d'un genre spécial qui engendre toutes sortes de risques : des **risques civiques**, par exemple avec la perte de contrôle des données personnelles, des **risques politiques**, des **risques économiques** – fiscalité ou plates-formes telles que Francis Jutand a montré qu'aux États-Unis d'Amérique elles permettaient aujourd'hui d'imposer des modèles hégémoniques et des distorsions de concurrence absolument drastiques –, des **risques culturels**, des **risques diplomatiques** aussi.

Le *web* et plus généralement l'Internet et le numérique, n'est pas l'informatique, qui est la science des ordinateurs. **Le numérique est la science** de ce que Mme Clarisse Herrenschmidt appelle **« l'écriture réticulaire », c'est-à-dire que tout le monde est relié à travers des réseaux et produit des traces.**

Depuis deux ans et demi, l'université de Stanford fait la promotion des *MOOCs*, une vitrine un peu tapageuse qui cache beaucoup d'autres choses que l'on regroupe sous le terme de *smart power*. Mme Clinton porte un grand discours sur le *smart power* qui viendrait remplacer le *soft power*. Le *soft power* est venu de l'usine à rêves Hollywood qui permettait aux États-Unis d'envoyer plutôt *Mickey* que les *GIs*. Comme le disent certains spécialistes de l'histoire américaine, *Mickey* rapporte de l'argent et de l'estime, les *GIs* coûtent de l'argent et produisent des ennemis. Il vaut mieux avoir un *soft power*, s'appuyant sur toute une technologie et des industries culturelles et qui va être à la base du modèle économique puisque ce sera aussi à l'origine de l'*american way of life*, c'est-à-dire le consumérisme capitaliste américain.

Aujourd'hui, nous allons vers le *smart power*, c'est-à-dire la prise de contrôle de la constitution des concepts, de la formation des élites, de tout ce qui consiste d'une façon générale à exploiter les possibilités des technologies dites intelligentes reposant sur l'automatisation, le calcul, les corrélations, etc.

Dans ce contexte géopolitique tout à fait fascinant, je pense que **l'Europe est extrêmement mal partie**. C'est le risque principal dont je veux vous parler. Cela peut sembler incroyable, puisqu'elle avait un avantage à la fin des années 1980. **La télématique, qui est à l'origine du concept du *web*, a été conçue en France** grâce à deux hauts fonctionnaires, respectivement inspecteur des finances et directeur de l'ENA, M. Simon Nora et M. Alain Minc. À la demande du Président de la République française, ils ont prescrit la nécessité de développer des réseaux télématiques.

Pour rappel, c'est dans le cadre de l'informatisation de la société, qui est à l'origine de la CNIL, qu'a été recommandée à la Direction générale des télécommunications (DGT) la mise en œuvre d'une politique nationale française de télématique. Celle-ci a donné le Minitel qui n'était qu'une première phase. **Le *web* est une deuxième phase, française et européenne, qui a été développé à Genève, au CERN.** Ce développement a duré quatre ans, de 1989 à 1993, date à laquelle les responsables du CERN, dont M. Tim Berners-Lee, directeur du *World Wide web Consortium (W3C)*, ont décidé de le verser dans le domaine public. Ils estimaient que parce qu'ils étaient des fonctionnaires payés par l'Union européenne, il n'y avait aucune raison qu'ils s'approprient ces résultats. Il se trouve que c'est M. Al Gore qui a récupéré ce travail pour en faire le cœur d'une stratégie de développement et de rebond des États-Unis, qui, faut-il le rappeler à cette époque, ne se portaient pas très bien.

J'insiste sur ce point pour affirmer que l'Europe peut parfaitement rebondir aujourd'hui. L'Europe a développé énormément de concepts qui sont aujourd'hui mis en œuvre stratégiquement par le Gouvernement fédéral américain. **L'Europe doit repenser le *web* et l'élaborer de fond en comble. Elle en a absolument les moyens.**

Que s'est-il passé entre 1993 et aujourd'hui ? En 1993, M. Tim Berners-Lee, M. Robert Cailliau et quelques autres ont constitué cette plate-forme qui s'appelle le *web*, basée sur *html*, les *URL* et un certain nombre d'autres technologies, dans une optique tout à fait précise : développer une plate-forme d'échanges entre scientifiques, ou porteurs d'hypothèses de savoir, afin que ces hypothèses soient livrées à la controverse publique. Ce public, ce sont d'abord les physiciens, les informaticiens, les mathématiciens, etc., mais le but était que tout cela puisse s'ouvrir au débat public sous toutes ses formes, politique, économique et autres. C'est de cette manière que le *web* s'est développé initialement.

Mais l'Amérique du Nord a très vite tiré parti de ce développement, dans une logique contributive qui était d'ailleurs celle du *web*.

Les Américains sont entrés massivement auprès du consortium *W3C* pour prescrire les évolutions du *web*. Comme vous le savez, le *W3C* est une instance de recommandation où l'on n'impose rien, mais où l'on recommande très fortement. La recommandation a un tel effet d'autoréalisation et de performativité que tout le monde est obligé de s'y soumettre, non pas par la force de la loi, mais par la force du fait technologique.

En conséquence, **le *web* a évolué depuis vingt-et-un ans dans une direction complètement différente de celle qui était initialement prévue. Le *web* est devenu essentiellement une machine à prendre tout le marché publicitaire** qui était dans les médias de masse, pour le transférer vers les plates-formes et au passage, défiscaliser les actions, créer de nouveaux modes intégrés de logistique, de production, etc. Aujourd'hui, *Amazon* s'apprête à prendre les marchés de *Promodès*. Je n'ai jamais trouvé personne pour me contredire sur ce point. *Amazon* vous livre déjà des livres et des balances électroniques à la fois. Si la question est à poser en ces termes-là, en toute logique, on peut s'attendre à ce qu'*Amazon* vous livre bientôt de la lessive et des petits pois.

Si vraiment on en est là, alors une question majeure se pose. Le Gouvernement français a récemment prévu d'investir treize milliards d'euros dans les infrastructures à très haut débit en France. **C'est une très bonne chose, si et seulement si l'on crée les conditions pour que ces réseaux à très haut débit servent plutôt à des activités européennes.** Ces réseaux à très haut débit ne doivent pas devenir les ambassadeurs d'*Amazon*, de *Google*, de *Facebook*, pour détruire la fiscalité nationale et l'activité privée européenne. C'est pourtant ce qui est en train de se préparer en ce moment.

Dès lors, je pense qu'il faut poser les problèmes avec une certaine radicalité. On considère que c'est la population française qui contribue le plus sur les réseaux. Que signifie contribuer et qu'est-ce qu'un réseau numérique aujourd'hui ? **Un réseau numérique ne vit que de la contribution des utilisateurs. Ce qui veut dire que ce ne sont pas des consommateurs.** Le consommateur ne contribue pas, il consomme. Le modèle d'un réseau numérique n'est absolument pas consumériste. C'est un modèle contributif. L'association *Ars industrialis*, que je préside, plaide depuis neuf ans pour la mise en œuvre d'une politique et d'une économie contributives fondées sur le numérique, qui rompt avec les modèles classiques du consumérisme issus du XX^{e} siècle.

Il est fondamental que l'Europe reconstitue une stratégie numérique, la France en particulier, à mon avis avec l'Allemagne. Un groupe parlementaire s'est constitué en France, et, côté allemand, Mme Merkel a encouragé un groupe parlementaire l'an dernier au Bundestag, qui a remis ses conclusions tout récemment à Berlin. Cette stratégie numérique doit avoir une ampleur mondiale et reposer sur la formation d'un troisième *web*.

Le *web* des années 1990 conçu par Tim Berners-Lee reposait sur les liens hypertextes et les *URL*. Ce *web* a été remplacé à la fin des années 1990 par les technologies collaboratives qui reposent sur les métadonnées, etc., et qui évoluent en ce moment même vers le *web* sémantique. Aujourd'hui **il faut constituer un nouveau *web***, que j'appelle **le « *web herméneutique* » et qui repose sur la possibilité pour les individus de reconstituer des controverses et de refaire du *web* un outil d'intelligence collective** et pas simplement un outil de captation du marché publicitaire par les plates-formes américaines. L'Europe en a les moyens. Cela suppose de repenser les industries éditoriales européennes et aussi l'enseignement supérieur, qu'il faut absolument mobiliser pour cela.

Je vous recommande la lecture d'un article de M. Hubert Guillaud, publié il y a deux jours dans *Internet Actu*. Il reprend des idées que j'ai présentées au Centre Pompidou en décembre 2013 lors des Entretiens du nouveau monde industriel, dont les travaux portaient sur l'automatisation (« *Le nouvel âge de l'automatisation, algorithmes, données, individuations* »). Le numérique est une technologie qui permet d'articuler très étroitement et fonctionnellement toutes sortes d'automatismes. C'est l'hypothèse de M. Michel Volle en France, ou de M. Marc Giget (CNAM).

Il y a un mois, M. Bill Gates a annoncé que **la technologie algorithmique allait détruire l'emploi dans les vingt ans qui viennent**. D'innombrables rapports sortent en ce moment, surtout aux États-Unis, qui montrent que **le modèle fondé sur l'emploi est terminé**. Ce modèle est basé sur la redistribution de la plus-value *via* le salaire et donc la constitution d'un pouvoir d'achat permettant au système de fonctionner sur les bases de ce que Roosevelt avait mis au point en 1933, vingt-cinq ans après les débuts d'Henry Ford, en institutionnalisant le modèle keynesien. Ces travaux montrent que le modèle fordo-keynesien est terminé. L'automatisation sonne la fin de l'époque de l'emploi.

Dans un tel contexte, on doit prendre en compte tous les facteurs que je viens d'évoquer, et bien d'autres, notamment la nécessité de **constituer une citoyenneté numérique**. Lors de mon intervention au Conseil d'État sur l'impact du numérique sur le droit, j'ai soutenu que **le droit devait être repensé au niveau constitutionnel dans le contexte du numérique. C'est une nouvelle Constitution qu'il faut mettre en place, de A à Z**, de l'ampleur de ce que les révolutionnaires ont posé en 1789. Dans le contexte de Condorcet, c'était la République des Lettres créée par l'imprimerie. Aujourd'hui, c'est la publication numérique automatisée à l'échelle planétaire qui pose un problème de Constitution.

D'ailleurs, M. Tim Berners-Lee encourage actuellement l'écriture d'une constitution du *web* à l'échelle internationale. Je pense qu'il faut poser ces problèmes-là dans toutes leurs dimensions et les articuler dans un point de vue synthétique et non pas d'une façon sectorisée. Par exemple, **pour développer une alternative au *web* tel qu'il est passé sous le contrôle**

californien, il faut mobiliser toutes les disciplines, en faisant travailler ensemble l'INRIA, le CNRS, les grandes universités, et pas seulement en France mais aussi en Allemagne avec le Fraunhofer, l'Université de Berlin, etc.

Questions à M. Bernard Stiegler

Mme Anne-Yvonne Le Dain. – Êtes-vous dans l'inquiétude, dans l'urgence, dans le désir, dans l'angoisse ou dans la nécessité ?

M. Bernard Stiegler. – Rien de tout cela. Je suis dans la pensée. Selon Hegel, l'inquiétude, c'est ce qui fait penser. Pour certains, je suis un indécrottable optimiste, un technophile qui ne raisonne qu'en étant persuadé de trouver une solution à tout. Pour d'autres, je suis un Cassandre qui annonce la fin des haricots. Je ne suis ni optimiste ni pessimiste. Le pessimisme est une façon d'empêcher de penser puisque tout est fait d'avance et il n'y a plus rien à faire. L'optimisme, c'est l'inverse, il n'y a rien à faire parce que tout s'arrangera. Je récuse ces attitudes-là. La responsabilité consiste à refuser l'une ou l'autre de ces positions. Par contre, il faut être lucide.

Quant à l'affaire Snowden, il faut souligner que tous ceux qui ont un petit peu réfléchi au numérique avaient connaissance de ces problèmes. Ils ne le disaient pas pour ne pas créer de panique. Mais, à un moment donné, il faut poser les problèmes. **La toxicité du numérique est extrêmement grande et très protéiforme. Le potentiel de réponse à cette toxicité par le numérique est encore plus grande**, selon moi. Je pense qu'il y a beaucoup de choses à faire et qu'elles sont possibles, mais cela suppose de penser, c'est-à-dire d'élaborer des points de vue vérifiés, à partir de données, etc.

Vous m'avez parlé d'urgence. Il ne faut pas penser pour les six mois qui viennent. C'est très important. En 1989, j'ai été chargé par l'Université de technologie de Compiègne et ensuite par le Premier ministre, Alain Juppé, quand j'étais directeur de l'Institut national de l'audiovisuel (INA), d'observer la stratégie industrielle américaine dans le champ de l'audiovisuel et de l'informatique. **Dès les années 1980, les États-Unis avaient une stratégie d'engagement dans le numérique**, à travers la loi de Moore, à travers *Intel* pour être précis, pour conquérir tout le marché des produits bruns.

Pourquoi ? En 1979, les États-Unis avaient perdu le marché de l'électronique grand public puisque *JVC* avait sorti le premier magnétoscope. Ils avaient également perdu le contrôle du marché automobile puisque *Toyota* était en train de supplanter *General Motors*. Bref, c'était le début de la

désindustrialisation des États-Unis. Détroit commençait à s'écrouler. **L'Amérique du Nord a construit une alternative industrielle avec l'armée, les grandes universités, les grands industriels, la société civile et les administrations fédérales, en l'occurrence avec la Commission fédérale des communications (FCC).**

Lorsque j'ai organisé, en 1989, à la Cité des sciences et de l'industrie un séminaire sur le *D2 Mac Paquets*, la TVHD, etc., tout le monde était là, sauf les Américains. M. Lionel Levasseur, économiste, qui travaille toujours à *France Télécom*, m'a expliqué que les États-Unis avaient fait un autre choix, celui du multimédia, c'est-à-dire que c'est par les microprocesseurs qu'ils allaient prendre le contrôle de la télévision.

En 1997, j'étais directeur général de l'INA, j'ai reçu M. Craig Mundie, vice-président de *Microsoft*. Il arrivait juste après une décision de la *FCC*, le 3 avril 1997, déclarant que, en 2006, il n'y aurait plus aucune fréquence analogique, en invitant les 3 500 stations de radio et de télévision américaines à passer au tout numérique dès 2003.

Vous comprenez comment marchent les États-Unis. On dit qu'ils ne fonctionnent que sur le marché à très court terme. C'est absolument faux. **Ils ont un pilotage stratégique qui est fait par l'armée américaine.** J'ai moi-même fait des travaux de développement de réseaux sociaux alternatifs dans mon institut à l'Institut de recherche et d'innovation (IRI) et j'ai eu la tristesse d'être financé par l'*US Navy* et non pas par les Français ou les Européens. L'*US Navy* s'est d'ailleurs déplacée exprès de Californie pour venir voir les résultats de ces travaux.

Il y a une intelligence techno-scientifique dans la puissance publique américaine, qui ne travaille pas pour elle-même, mais bien pour le marché américain, sachant très bien que le marché n'aura jamais intérêt à développer une technologie de rupture. Il faut l'obliger à la développer. Donc **il faut reconstruire une politique européenne à long terme**.

M. Parfait Nangmo, ingénieur en sécurité informatique, représentant d'*Altran technologies*. – J'ai apprécié l'intervention très riche de M. Bernard Stiegler. Vous avez dit que le *web* a été créé comme une plate-forme d'échanges et par la suite, il s'est dénaturé et a été monopolisé par des géants comme *Google*. Comme solution, vous proposez la création d'un troisième *web* comme une plate-forme d'échanges collective. Ne va-t-on pas retomber dans le même engrenage que pour le premier *web* ? En d'autres termes, quelles sont les pratiques actuelles qui vous font penser que le troisième *web* pourrait avoir le succès qui a été pensé au départ ?

M. Bernard Stiegler. – Merci pour cette très bonne question. C'est la question qui se pose après mon intervention. Je crois que l'Europe est très menacée en ce moment par la stratégie du *smart power*. D'abord parce que ses universités risquent d'être extrêmement pénalisées par cette démarche ainsi que ses grands éditeurs, *Springer* par exemple, comme le dit son *CEO*, ou

Gallimard en France, qui est ni plus ni moins que l'image de la France partout dans le monde, parce qu'il incarne une histoire (Voltaire…) et les scientifiques français (Évariste Galois, Pasteur…). Si la France est aujourd'hui encore extrêmement respectée dans le monde et l'Europe plus généralement, comme étant les pays des grands penseurs, des grands artistes, des grands scientifiques, etc., c'est parce que **la France et l'Europe ont des industries éditoriales. Si vous perdez les industries éditoriales, tout cela va disparaître en très peu de temps.** Je vous recommande un excellent article sur le rôle de la bibliométrie américaine et la manière dont l'Amérique du Nord a pris le contrôle de l'évaluation scientifique à travers les technologies de bibliométrie (revue Réseaux, printemps 2013). *Google* est un produit direct de cela.

Il faut que l'Europe reconstitue un schéma de priorités européennes et de solvabilisation d'une technologie de rupture. Pour illustrer mon propos, je vais vous dire un mot sur Jules Ferry. C'est un homme qui se réfère à Condorcet, pensant que l'Occident a une mission planétaire à travers une politique coloniale. C'est aussi quelqu'un qui récupère un État qui s'est développé à partir de 1830 avec Louis Hachette. Très connu comme le fondateur des éditions *Hachette*, Louis Hachette au départ voulait être professeur et il a fait l'École normale. Au moment de la Restauration, il a été remercié et s'est retrouvé au chômage. Un ami lui a prêté de l'argent pour qu'il achète une librairie. À cette époque, une librairie, c'est aussi une maison d'édition. Louis Hachette devient donc éditeur, et comme, par ailleurs, il a été formé, c'est un professeur, il se met à publier des manuels scolaires. Un ami à lui, qui s'est retrouvé ministre de l'éducation nationale, lui ouvre des marchés. Et cela a été le début, non pas de l'éducation nationale à la façon de Jules Ferry, mais d'une instruction portée par la puissance publique, bien qu'elle n'ait pas encore été obligatoire. En 1880, quand Jules Ferry arrive, il y a eu l'apparition de *Hachette*, le premier à fabriquer des manuels scolaires et l'arrivée de la presse à journaux, qui permettait au *Petit Journal* par exemple de tirer à un million d'exemplaires en 1870. Cela a permis que les manuels scolaires de *Hachette* descendent à un sou, permettant à une petite commune de trois cents habitants de les acheter pour la bibliothèque et donc de créer une école communale. Le génie incroyable de Jules Ferry, en 1880, c'est d'avoir consacré un budget absolument colossal à l'éducation de tout le monde. C'était inimaginable à cette époque-là. Oui pour mettre 20 % du budget national dans l'armée, mais dans l'instruction des paysans, non ! Et d'abord, on disait que les paysans ne pouvaient pas être formés… Jules Ferry l'a fait parce qu'une technologie a permis de le faire : c'était la technologie de production des manuels scolaires.

Aujourd'hui, nous devons réinventer un système de publication numérique qui permette de créer un nouveau système académique. Cette publication académique doit être produite selon des formes contributives. Au CNNum, j'ai proposé au Gouvernement que l'État français investisse

treize milliards d'euros sur vingt ans dans une infrastructure, à une condition : financer tous les ans **cinq cents thèses sur le numérique pour penser la mutation numérique de manière transdisciplinaire, avec des technologies de contribution et d'éditorialisation d'un nouveau genre**.

J'ai proposé à *France Télévisions*, membre de l'IRI, qui a accepté de s'associer à cette démarche. Nous réfléchissons actuellement à la manière dont *France Télévisions* pourrait devenir éditeur de savoir dans une démarche de recherche contributive.

Le numérique évoluant extrêmement vite, vous devez mettre en œuvre des méthodes de transfert vers la société, des travaux de recherche qui accélèrent la transmission de l'intelligence collective et qui collent à la réalité numérique. En effet, quand les travaux de thèse sont finis, ils sont magnifiques, mais ils parlent de choses qui ont disparu. Le numérique offre des technologies de transfert de concept, et, en plus, il permet d'y associer les populations. *Wikipédia* en est un exemple. Le numérique a développé des espaces communautaires de production de savoir, qui parfois sont de très bonne qualité et produits par des gens qui ne sont pas issus du monde académique. Il y a aussi des choses de très mauvaise qualité. Mais la démarche contributive engendrée par le numérique est extrêmement intéressante.

L'Europe doit donc développer une stratégie contributive en mobilisant toutes ces intelligences. Tant qu'à payer des thésards, payons-les à faire quelque chose de vraiment intéressant pour que nous inventions ce nouveau *web*. À partir du moment où nous aurons fait cela, **nous allons solvabiliser le système parce que nous aurons créé une industrie éditoriale d'un nouveau genre** qui va elle-même être au service d'une production d'intelligence collective à l'échelle européenne.

Depuis vingt-cinq ans, on nous dit que nous entrons dans la société de la connaissance. C'est vrai, mais de son côté, quelqu'un comme M. Alan Greenspan estime que nous sommes entrés dans la société de la bêtise. **Il faut que nous allions vers la connaissance mais nous n'y sommes pas encore. Et je crois qu'on peut le faire avec une vraie stratégie industrielle de recherche et d'enseignement supérieur**, en mobilisant les ressources spécifiques du numérique dans ce sens et dans le sens de nos intérêts et non pas ceux de la Californie ou d'*Amazon* en Virginie.

M. Pierre Lasbordes. – Je vais donner la parole à un représentant des consommateurs qui est apparemment sensible à tout ce qui tourne autour de la fraude au niveau des cartes de paiement. Dans mon rapport au Premier ministre, en 2006, j'avais constaté que, aux États-Unis, les entreprises n'étaient pas gênées pour dire qu'elles avaient été piratées, y compris les banques. En France, ce n'est pas imaginable pour l'instant. Il est vrai que si une banque déclare à ses clients qu'elle a fait l'objet de dix attaques de *phishing* par jour, peut-être risque-t-elle de perdre des clients. Comment voyez-vous votre rôle au niveau de l'association *UFC-Que Choisir*

pour sensibiliser les consommateurs à ces problèmes qui sont de plus en plus nombreux ?

M. Maxime Chipoy, responsable des études, *UFC-Que Choisir*. – Je vous remercie pour cette introduction qui fait référence à l'un des cœurs de sujets sur lesquels je travaille. Je supervise toutes les études économiques effectuée par l'*UFC-Que Choisir* et je m'attache en particulier à toutes les problématiques financières (banque, finances, assurance), dont la fraude à la carte bancaire et aux autres moyens de paiement qui constitue vraiment une importante problématique.

Aujourd'hui, je peux vous dire que **le risque sur la sécurité du numérique est avéré pour les consommateurs et même supporté**. Pour ne parler que de la fraude à la carte bancaire, **les montants fraudés sont de l'ordre de 450 millions d'euros par an, dont 60 % ont été fraudés par la voie numérique. Ce sont principalement des données de cartes bancaires volées sur Internet** lors d'un achat effectué par un consommateur, qui sont ensuite réutilisées par des fraudeurs pour effectuer d'autres paiements. Les taux sont en forte croissance depuis 2007, avec la croissance des achats sur Internet, mais la part des montants fraudés sur les montants facturés a progressé beaucoup plus vite que la montée en charge du commerce électronique.

Il y a deux problématiques principales. La première est géographique. Au fur et à mesure des années et parfois de manière assez douloureuse, les commerçants français ont peu à peu amélioré leur site Internet pour qu'on ne puisse pas capturer de données bancaires. Mais, auparavant en Europe et aujourd'hui à l'international, **tous les pays n'atteignent pas le même niveau de sécurité**. On aura beau élaborer des réglementations contraignantes au niveau français, pousser les acteurs à sécuriser leur site Internet et pousser les consommateurs à adopter de bonnes pratiques, si, à l'échelle européenne voire internationale, on n'a pas le même degré de sécurité, il est fort à parier que **les fraudeurs vont agir sur le maillon de la chaîne qui est le plus faible**. Ce maillon peut être géographique ou technologique ou tout simplement un type de moyen de paiement.

En France, et même en Europe, on commence à faire des efforts sur la carte bancaire. On sait que **les Européens commencent peu à peu à convaincre les Américains de l'utilité de la mise en place d'une carte à puce pour leurs paiements et de l'utilité d'une meilleure sécurisation des sites Internet américains** pour éviter que les fraudeurs qui ont récupéré des numéros de cartes bancaires françaises les réutilisent aux États-Unis.

Je voulais dépasser le cadre de la carte bancaire car nous avons une nouvelle préoccupation à l'*UFC-Que Choisir*. La carte bancaire commençant à être sécurisée, les fraudeurs se reportent sur les moyens de paiement les plus faibles et malheureusement aujourd'hui, nous avons de grosses craintes sur les virements et les prélèvements. En effet, le règlement européen *SEPA* (Espace unique de paiement en euros) prévoit, dans un but louable

d'harmonisation du marché européen, de créer des processus uniques pour les prélèvements et les virements. Son entrée en application prévue en janvier 2014 a été reportée à août 2014 parce que la plupart des établissements français et des professionnels n'étaient pas prêts. En janvier 2014, seuls 40 % des commerçants étaient prêts. Jusqu'à présent, les prélèvements français fonctionnaient selon un modèle franco-français. Demain, les prélèvements seront communs à l'Espace économique européen (EEE), la Suisse et Monaco.

Cela va provoquer un problème. Précédemment, quand les consommateurs français mettaient en place un prélèvement, ils devaient donner leur mandat de prélèvement, d'une part au commerçant pour qu'il puisse retirer de l'argent sur leur compte et, d'autre part, à la banque pour qu'elle puisse vérifier que le professionnel qui effectue une opération fût bien reconnu par le consommateur. Aujourd'hui, le nouveau mandat de prélèvement européen ne prévoit plus qu'un seul mandat. Ce mandat est donné au professionnel et c'est le professionnel qui va fournir le mandat auprès du banquier pour retirer de l'argent sur le compte du consommateur. Cela pose un gros problème. **Désormais, la banque est totalement aveugle. Elle ignore si, oui ou non, le consommateur a accepté le prélèvement.**

Alors que le prélèvement *SEPA* vient à peine d'être mis en œuvre, nous avons déjà des cas de fraude. Le fraudeur a réussi à capturer les données d'identité du consommateur (nom, prénom, adresse, etc.) et ses coordonnées bancaires, ce qui n'est pas vraiment difficile en France, où on les donne très souvent. Par exemple, des fraudeurs s'abonnent à *Orange* et font payer la facture par un prélèvement automatique sur le compte d'autrui. Si le consommateur n'est pas extrêmement vigilant, vous pouvez être sûr que, dans les années à venir, vous aurez des prélèvements *SEPA* de un ou deux euros montés par des fraudeurs sur des centaines de milliers de comptes.

Nous souhaitons dénoncer une seconde chose au sujet du *SEPA*. Le législateur européen, sachant que ce système de mandat unique est bien moins sécurisé que le système de double mandat que l'on avait en France, a prévu des mécanismes de sécurité. Théoriquement, le consommateur a le droit de mettre en place auprès de sa banque ce qu'à l'*UFC-Que Choisir* nous avons appelé des « listes noires » ou des « listes blanches ». Concrètement, vous demandez à votre banquier de refuser tout prélèvement qui viendrait d'un autre organisme qu'*Orange*, *GDF* ou *EDF*, par exemple. C'est la liste blanche. Seuls sont autorisés les paiements des prestataires identifiés. Dans l'autre cas, la liste noire vise à interdire les prélèvements à un ou plusieurs prestataires.

Ces outils très utiles sont censés sécuriser le prélèvement européen et éviter les fraudes. Or notre enquête, menée en janvier 2014, a montré que sur les cent trente banques que nous avons étudiées, **une seule banque communique avec ses clients sur la possibilité de mettre en place des listes**

noires ou des listes blanches pour éviter les prélèvements non acceptés. Ce manque d'information du client nous paraît assez irresponsable, d'autant plus que **le règlement européen oblige les banques à communiquer sur la mise en place de ces listes noires et blanches**.

Voilà pour le cadre, un peu apocalyptique, du sujet numérique sur l'aspect bancaire à l'*UFC-Que Choisir*.

Je vais revenir sur des sujets plus larges. En ce qui concerne la sécurité des serveurs contenant des données personnelles, nous sommes en faveur de la mise en place d'une normalisation la plus large possible, au moins au niveau européen, voire au niveau mondial. Cela suppose **la mise en place d'une autorité mondiale ayant éventuellement des pouvoirs de sanction**, ce qui ne va pas sans poser de gros problèmes vis-à-vis des prérogatives de chaque État. Malgré tout, cela nous paraît indispensable dans un monde globalisé. Si l'on en reste au niveau franco-français, et on le voit déjà avec les moyens de paiement, une normalisation ne servira à rien. **Il est très facile, dès aujourd'hui, de voler des données de cartes bancaires pour s'en servir en Chine ou ailleurs. Les autorités de police sont totalement impuissants**, ou en tout cas, ils peuvent agir mais cela prend des années et donc ne sert pas concrètement au consommateur à limiter le coût de la fraude. Il faudrait une normalisation mondiale avec des pouvoirs de sanction au même niveau. C'est au politique de prendre le relais.

Que faire en cas d'attaque informatique sur les serveurs ? À l'*UFC-Que Choisir*, nous estimons qu'il y a beaucoup plus d'attaques informatiques réussies que ce que l'on veut bien nous dire. Théoriquement, les professionnels ont une obligation de moyens quant à la déclaration aux consommateurs lorsqu'ils ont été dérobés et ils ont une obligation de résultats quand il s'agit de données personnelles sensibles. À l'*UFC-Que Choisir*, nous pensons que la plupart des professionnels en France font passer leurs intérêts propres avant tout et le risque d'atteinte à leur image lié à la fraude avant de penser à l'intérêt de leurs clients.

C'est pourquoi nous plaidons fortement pour la **mise en place d'une obligation de déclaration au client dès lors qu'une attaque informatique réussie a eu lieu**. Peu importe le nombre de comptes qui ont été dérobés. Cette règle d'or doit être applicable à l'ensemble des professionnels agissant dans le secteur numérique.

Nous considérons qu'il est meilleur pour l'image d'une entreprise qu'elle dise honnêtement à ses clients qu'elle a été victime d'une attaque informatique. Les progrès de la fraude étant ce qu'ils sont et les progrès de la sécurité informatique ne pouvant que suivre, hélas, les progrès de la fraude, on sait très bien que le risque zéro n'existe pas et qu'il y aura toujours des attaques informatiques. Dès lors, il n'y a pas d'acteurs meilleurs que d'autres à partir du moment où ils ont respecté une normalisation de base. Il faut que les consommateurs soient avertis de l'attaque du compte de leur prestataire pour qu'ils puissent prendre les précautions qui s'imposent. Si l'un de mes

prestataires possède mes numéros de carte bancaire et qu'il s'est fait attaquer, je préférerais largement faire opposition à ma carte bancaire et en commander une nouvelle plutôt que de découvrir trois semaines plus tard que j'ai été fraudé de deux cents euros.

Cependant, il faut reconnaître que la loi issue des directives européennes est très protectrice en matière de fraudes à la carte bancaire. Théoriquement**, pour tout ce qui concerne le numérique, le consommateur est entièrement couvert**. Et même s'il peut y avoir des problèmes au cas par cas puisque des banques peuvent rechigner à rembourser le préjudice subi, et cela peut prendre certains délais, aujourd'hui les consommateurs sont bien couverts par la loi à titre individuel. Mais cela a un coût. **Plus il y aura de fraude, plus cette fraude sera répercutée sur les tarifs bancaires**, et donc, *in fine*, sera assumée par l'ensemble des consommateurs.

C'est pourquoi nous sommes en faveur d'une politique de prévention très large. **Il faut une normalisation, une sécurité maximale, et cette normalisation doit être mise à jour de manière régulière. Il faut également qu'un système d'alerte permette au consommateur de prendre des précautions minimales**, comme de surveiller son compte en banque ou faire opposition à ses moyens de paiement si une attaque informatique a été détectée.

Pour terminer sur la question des données personnelles au sens large, nous déplorons la tendance des consommateurs à donner leurs données personnelles à n'importe qui, notamment parce qu'une bonne partie de l'économie de l'Internet est fondée sur le principe de la gratuité du service contre la fourniture de données personnelles. Hélas, les consommateurs ne savent pas encore que la gratuité n'existe pas et que les données personnelles qu'ils fournissent à leurs prestataires sont forcément réutilisées et revendues quelque part. Toutefois, on note une prise de conscience de la part des consommateurs. On l'a vu avec l'affaire *Instagram* qui a révélé que les photos des consommateurs devenaient plus ou moins la propriété d'*Instagram* et qu'elles pouvaient être réutilisées.

Néanmoins, il faut aussi les aider à gérer leurs données personnelles. À l'*UFC-Que Choisir*, nous plaidons très fortement pour la mise en place de *dashboard* par l'ensemble des acteurs du monde numérique. Dans cet espace personnel, le consommateur peut savoir quelles données le professionnel possède sur lui mais également à qui le professionnel a revendu ses données personnelles. Ce *dashboard* irait dans le sens d'une plus grande clarté. À partir du moment où le consommateur reçoit ces informations, il peut commencer à faire des demandes d'effacement, des demandes auprès de la CNIL, etc.

Je vais terminer sur la problématique du droit à l'oubli. À l'*UFC-Que Choisir*, nous considérons que **le droit à l'oubli est une chimère totale**. Vous aurez beau demander à un professionnel de retirer des photos ou des renseignements qui vous concernent, même s'il le fait, rien n'indique qu'un

tiers n'aura pas déjà récupéré les données personnelles et qu'il sera en capacité de les réutiliser. Ce droit à l'oubli est donc très provisoire.

Concernant le droit au déréférencement, on l'a vu récemment avec l'affaire *Google*, la problématique est double. Premièrement, *Google* peut encore s'arroger le titre du juge puisqu'il est en droit d'estimer de la légitimité de la demande effectuée par le consommateur. **Il est très gênant qu'une personnalité privée, de sensibilité anglo-saxonne, soit en capacité de juger de la pertinence et de la légitimité de la demande des consommateurs.** Au-delà de cet aspect, le fait de déréférencer sur *Google France* ne va pas automatiquement déréférencer sur *Google monde*. Enfin, si vous êtes déréférencé sur *Google*, rien n'indique que vos données ne soient pas retrouvables sur *Bing* ou sur d'autres moteurs de recherche. En conséquence, nous pensons que le droit au déréférencement est une bonne chose, mais il ne peut être que partiel et ne doit pas se substituer au droit à l'effacement des données personnelles.

M. Pierre Lasbordes. – Nous comptons sur vous pour être l'aiguillon qui sensibilisera les gens à être prudents. Personne ne peut dire qu'il n'a pas été l'objet d'une fraude.

M. Maxime Chipoy. – On constate que le montant moyen des fraudes diminue tandis que le nombre de personnes touchées s'accroît. Les consommateurs se rendent compte des fraudes d'un montant élevé puisque cela touche directement l'équilibre de leur budget chaque mois. À l'avenir, il est à craindre que les fraudeurs fassent des dizaines ou des centaines de milliers de prélèvements d'un euro qui passeront inaperçus pendant des années.

Mme Anne-Yvonne Le Dain. – Ce matin, Me Christiane Féral-Schuhl a considéré que le droit à l'oubli pourrait être une manière de réécrire sa biographie et que, au contraire, le droit au déréférencement permettrait de continuer à construire du droit et une histoire sur laquelle pourrait se construire le droit futur, y compris de tiers. Votre position est assez différente.

M. Maxime Chipoy. – Nous considérons que **le droit à l'oubli n'a pas vraiment d'application** puisque vous ne savez pas qui a utilisé vos données personnelles, qui les a vues, qui les a capturées.

Mme Anne-Yvonne Le Dain. – Vous souhaitez qu'on puisse faire appel au droit à l'oubli, c'est-à-dire disparaître de la Toile mais pas au détriment du droit au déréférencement. Me Christiane Féral-Schuhl a souligné que le droit à l'oubli, c'est-à-dire le fait de supprimer sa trace sur Internet, permettrait de contribuer à la réécriture de son propre historique, ce qui pourrait mettre en danger, moral ou juridique, des tiers. Vos deux points de vue sont-ils si différents ?

M. Maxime Chipoy. – Je vais être plus clair. Nous ne sommes pas contre le droit à l'oubli en tant que tel. Mais nous considérons qu'il ne faut

pas que la création d'un droit à l'oubli serve de prétexte pour oublier les autres droits qui seront sans doute plus effectifs. Effectivement, nous pensons au droit au déréférencement, même s'il trouve très largement ses limites, mais également au droit à l'effacement qui nous semble beaucoup plus important. Mais pour qu'il y ait droit à l'effacement, il faut aussi une prise de conscience et la mise à disposition des consommateurs d'outils adaptés pour qu'ils sachent avant tout quelles sont les données possédées par l'ensemble des prestataires ou des services par lesquels ils passent.

M. Pierre Lasbordes. – Monsieur Jean-Pierre Quémard, en tant que chef de la délégation française à l'ISO/IEC JTC 1/SC 27, vous jouez un rôle assez important en matière de normalisation. En France, nous avons la réputation d'être en retard sur ce sujet, par rapport aux Américains en particulier. Pouvez-vous nous rassurer et nous dire que la France n'est pas en retard, que les Américains ou des Européens plus puissants que nous ne vont pas nous imposer des normes et quelles sont pour vous les étapes importantes dans cette normalisation ?

M. Jean-Pierre Quémard, président de la commission de normalisation SSI et chef de délégation française à l'ISO/IEC JTC 1/SC 27. – Je voudrais d'abord réagir sur ce que j'ai entendu. On dit que l'industriel se préoccupe de ses intérêts plutôt que de sécurité et de ses produits. Chez *Airbus*, nous avons mis en place un *Product Security Office* parce que nous considérons que la sécurité de nos solutions et de nos produits est très importante pour notre réputation et que l'on ne peut plus se permettre aujourd'hui de traiter la sécurité comme un mal nécessaire. Je suis d'ailleurs en charge de ces activités chez *Airbus Défense & Sécurité*.

Au sujet de la normalisation, il faut identifier un premier point qui est le triangle magique. Actuellement la biométrie fait débat. Mais il n'y a pas de technologie bonne ou mauvaise en soi. Un marteau peut enfoncer un clou tout comme vous écraser un doigt. Ce qui est très important, c'est d'**entourer la technologie des trois sommets d'un triangle que sont la réglementation, la normalisation et l'évaluation**.

Une réglementation va définir un cadre juridique, technique, politique parfois. La normalisation va permettre de garantir un niveau de standardisation, d'homogénéité, d'interopérabilité. L'évaluation consiste à vérifier que l'on est conforme à des standards et que ces standards respectent la réglementation. Cela permet de recadrer la standardisation comme étant indispensable pour garantir de nombreuses choses, aussi bien l'interopérabilité des boulons que la sécurité des réseaux numériques.

Je vais me concentrer sur l'aspect normalisation de la sécurité des systèmes d'information. En tant que président de la délégation française à l'*ISO* du SC 27 qui traite des systèmes d'information, je dirais qu'**en France nous ne sommes pas en retard**. Dans la délégation que j'ai conduite il y a un mois à Hong Kong, il y avait dix-huit délégués français sur deux cents délégués du monde entier et nous étions la troisième délégation en nombre

derrière les Américains et les Japonais. C'est loin d'être ridicule. Je pense qu'on a réussi à motiver dans ce domaine un certain nombre d'intervenants, aussi bien des grands groupes que des PME, des experts dans le domaine.

Les travaux du SC 27 se partagent en cinq activités : la gestion des systèmes d'information (*ISMS*) ; le groupe 2 définit tous les mécanismes crypto ; le groupe 3 s'occupe de tout ce qui est évaluation comme, par exemple, les critères communs, l'évaluation d'algorithmes cryptographiques… tout un ensemble de normes et de standards qui permettent de vérifier la conformité ; ensuite il y a la sécurité des applications ; et finalement la sécurité des identités et de la biométrie. Ces travaux couvrent l'ensemble des briques nécessaires à la mise en place d'un système sécurisé performant.

En France, nous sommes tout à fait bien placés. Je suis personnellement éditeur de cinq standards internationaux plutôt dans le domaine de l'évaluation de la crypto. Nous avons des compétences très fortes en France. En revanche, nous avons aussi quelques faiblesses sur lesquelles je reviendrai.

M. Pierre Lasbordes a parlé de normes mondiales, c'est bien, mais en fait, il y a trois niveaux dans la sécurité. Le premier niveau est national, régalien, c'est le « confidentiel défense » ou le régalien pur qu'on ne va pas trop partager. Ensuite il y a le monde européen dans lequel on est capable de mettre en place des règlements. Enfin il y a la norme mondiale, où, là, c'est un combat politique. Je ne parlerai pas de Snowden, mais on se sent plus à l'aise à travailler avec nos partenaires européens plutôt que se faire imposer des standards qui viennent soit de Chine soit des États-Unis. Pourquoi j'engage beaucoup l'industrie française à aller dans le sens de la standardisation ? Parce que c'est un avantage compétitif. Quand on est conforme aux standards, *a priori* on a un avantage commercial mais nous serons encore meilleurs si c'est nous qui avons contribué à la définition du standard.

La cohérence et l'homogénéité sont très importantes. J'anime aussi ces réflexions au niveau européen, au sein du *Cyber Security Coordination Group (CSCG)* dont je suis vice-président. Et je suis aussi vice-président du *Technical Committee on Cyber Security* à l'*ETSI*.

Je vous ai décrit une situation merveilleuse, mais ce n'est pas aussi simple. Au sein du Comité de filière des industries de la sécurité, j'anime aussi les réflexions sur les aspects « *Export, Normes, Intelligence économique* ». C'est vrai qu'il n'existe pas de position partagée par tous. Souvent, des interlocuteurs me disent que ça coûte cher. **En France, on souffre d'un problème de gouvernance de la normalisation.**

Un exemple : l'AFNOR est le *national body*, c'est-à-dire le référent mandaté au niveau de l'*ISO*. **La normalisation française est faite de telle sorte que ceux qui y contribuent paient trois fois.** Une fois pour adhérer à

l'AFNOR, une deuxième fois, si vous êtes très motivé, pour envoyer des experts, des gens qui vont faire des contributions, des commentaires…, une troisième fois pour acheter la norme parce qu'elle n'est pas gratuite.

Au Japon, les choses se passent différemment. Lorsque le Japon a considéré qu'un domaine était prioritaire, il paie ses experts pour constituer un groupe miroir. C'est pourquoi dans une délégation japonaise on trouve quarante experts quand celle de la France compte quinze volontaires.

Donc face aux atouts, nous avons un vrai problème de gouvernance. Je travaille sur ce problème-là avec la Direction générale de la compétitivité, de l'industrie et des services (DGCIS) en charge de la coordination de la normalisation, pour essayer d'avancer sur ce sujet. Les freins et les limitations sont plutôt à rechercher de ce côté-là. Pour accepter de payer trois fois, il faut être très motivé.

M. Pierre Lasbordes. – J'avais écrit, en 2006, que la France devait absolument être à l'avant-garde dans le domaine des normes de la sécurité informatique. Vous me rassurez. C'est déjà une bonne chose.

M. Philippe Wolf, ingénieur général de l'armement, auteur de nombreux articles et ouvrages sur le numérique. – Je connais bien les critères communs. C'est effectivement devenu un gros mot pour les Américains qui cherchent à remplacer ces critères un peu rigoureux par des choses moins rigoureuses. Est-ce toujours la tentation aujourd'hui d'aller plus vers l'auto-évaluation ?

M. Jean-Pierre Quémard. – Évidemment, c'est un sujet sensible sur lequel je travaille. Je viens de faire ce matin un *input paper* pour la prochaine réunion du *Cyber Security Coordination Group* disant que le label européen repose sur les critères communs. Les critères communs sont d'origine européenne, c'est une base d'évaluation internationale. Les Américains, qui veulent un peu rejeter les critères communs, avancent l'argument suivant : même les Chinois sont capables d'évaluer et d'avoir des laboratoires de certification. Nous pensons qu'il faut renforcer et avoir une évaluation tripartite, par celui qui réalise l'équipement, celui qui prononce la certification et le laboratoire d'évaluation. Ce modèle à trois tiers est sain. Je récuse complètement l'auto-évaluation, sinon tout le monde va être standard. Certes, dans certains cas, pour des problèmes de coûts sur des systèmes de moindre risque, on peut avoir ce genre de choses pour des niveaux d'évaluation d'assurance qualité n1 ou n2. Mais pour des niveaux au-dessus de 3, il faut absolument passer par des laboratoires.

Me Éric Caprioli, docteur en droit, avocat à la Cour d'appel de Paris, vice-président du Club des experts de la sécurité de l'information et du numérique (CESIN). – Vous avez parlé de dix-huit délégués experts qui sont envoyés pour œuvrer à la normalisation et à la défense des intérêts français au niveau international. Ces dix-huit experts sont-ils financés par leur entreprise ?

M. Jean-Pierre Quémard. – Pas tout à fait. Une convention entre l'ANSSI et l'AFNOR permet d'aider une PME à chaque fois en lui payant ses frais de déplacements, sinon l'essentiel est financé par les entreprises. D'où la difficulté. C'est l'un des trois paiements pour accéder à la normalisation.

Me Éric Caprioli. – Nous participons à des travaux sur certains sujets, *via* la Fédération nationale des tiers de confiance (FNTC), et ce sont les cotisations des membres qui financent les personnes que l'on envoie, par groupe d'une, deux ou trois personnes, qui viennent défendre les intérêts français sur l'archivage ou des sujets liés à la dématérialisation. Je constate que **l'État est relativement absent**. De la même manière, quand on doit faire des travaux et les financer au niveau de l'AFNOR, je constate que nous sommes rackettés. On nous a vendu des concepts politiques. Travailler plus pour gagner plus ou travailler plus pour gagner moins mais, dans ce cas, c'est travailler plus à vos frais ! Cette approche est assez surréaliste, d'autant plus que nous envoyons de l'expertise, et donc envoyer de la matière grise qui elle-même paie pour travailler, cela fait un peu beaucoup en termes de charges.

M. Jean-Pierre Quémard. – Nous sommes en phase, c'est tout à fait ce que j'ai dit. C'est pourquoi j'insiste sur cet aspect de la gouvernance de la normalisation. C'est un sujet stratégique. Si l'on ne veut pas être en retard, il y a urgence de mettre en place des modèles différents. C'est vrai de ce que vous faites à la FNTC, dont je connais bien le président, ou de ce que l'on fait à la Fédération des industries électriques, électroniques et de communication (FIEEC) vis-à-vis de l'Union technique de l'électricité (UTE), ou de certaines fédérations professionnelles qui prennent en charge les coûts d'expert. On pallie les défauts du modèle. C'est un emplâtre sur une jambe de bois. Je ne dis pas qu'il faut tout payer. Au sein du comité de filière des industries de la sécurité, on essaie de définir les sujets stratégiques sur lesquels on doit être présent, soit parce qu'il y a une menace sur notre industrie soit parce que nous avons des avantages à défendre et travaillons sur ces sujets-là. On ne peut pas tout embrasser.

M. Philippe Wolf. – **Les normes à l'AFNOR sont payantes parce que l'AFNOR se finance avec la vente des normes, ce qui fait que toutes les PME n'ont pas accès à des normes aussi simples que des normes de bonnes pratiques**, par exemple l'*ISO* 2702, qu'il faut payer à des prix hallucinants. Heureusement, on trouve des versions pirates sur Internet mais je trouve que la situation n'est pas très satisfaisante. **Que peut-on faire pour avoir des normes gratuites**, sachant que **les normes du *National Institute of Standards and Technology (NIST)* sont partout, qu'elles sont gratuites** et que vous les trouvez très facilement sur le site de cet institut ?

M. Jean-Pierre Quémard. – Je suis complètement d'accord. En tant qu'industriels, nous nous battons pour demander à l'*ISO* un certain nombre de normes gratuites. En revanche, l'*ISO* 2700 est gratuite, mais pas les 2701,

2702, 2703, 2704, 2705… **Il y a un palliatif, c'est de passer par l'*ETSI*, dont toutes les normes sont gratuites.** Là encore, vous soulevez le problème de la gouvernance. L'AFNOR est un vrai modèle commercial et il y a un autre effet pervers. Dès qu'on a une petite idée, on crée un nouveau groupe parce qu'un nouveau groupe, c'est une nouvelle adhésion, donc c'est de l'argent qui rentre dans les caisses. **Le modèle de l'AFNOR est complètement pervers.** C'est un modèle à tuer ! En Allemagne, l'Institut allemand de normalisation (*Deutsches Institut für Normung*, *DIN*), ne fonctionne pas comme cela. Ni l'*ANSI* aux États-Unis. Nous sommes les seuls au monde ! C'est l'exception culturelle française.

M. Pierre Lasbordes. – Petite question naïve : Que peuvent faire les politiques par rapport à cela ?

M. Jean-Pierre Quémard. – Simplement changer le modèle en disant que la participation aux groupes de normalisation est gratuite et que l'AFNOR se débrouille autrement. À la limite, je n'ai pas besoin de l'AFNOR pour faire fonctionner mon groupe. C'est simplement un point de passage obligé. Qu'est-ce que m'apporte l'AFNOR ? Rien. Je fais les comptes rendus, c'est moi qui y vais, j'anime les réunions. Ça ne sert à rien.

Me Éric Caprioli. – Vous avez parlé de l'*ETSI* qui, aujourd'hui, travaille sur plusieurs dizaines de normes dans le cadre du règlement sur l'identification électronique et les services de confiance (*eIDAS*). Quand on contribue, dans le cadre de ces groupes de travail, **les enjeux sont fondamentaux puisqu'ils concernent toute la sécurité dans les échanges**, et en plus, certains modèles sur l'identité. Heureusement qu'on a l'ANSSI en tout cas pour toute une partie des travaux avec l'Allemagne qui vont certainement nous aider. Mais les participations sont gratuites et la plupart des personnes qui travaillent en tant que Français sont payés par leur entreprise pour aller à Sophia Antipolis ou ailleurs. Ce sont des enjeux stratégiques pour la nation en termes de sécurité. Toutes les entreprises, par exemple les prestataires de services de confiance qui ne sont pas de grosses entreprises, *Open Trust*, *Dictao*… ne sont pas *Airbus* ou *Thales*. Elles mobilisent beaucoup d'énergie pour être présentes sur ces marchés. Que faut-il faire par rapport à cela ?

M. Jean-Pierre Quémard. – Je vais répondre sur l'*eIDAS* que je connais très bien. C'est un exemple qui a très bien marché. Certains pays européens, poussés par certains États, avaient couru le risque d'avoir une identité au rabais. La France s'est mobilisée avec l'ANSSI, l'Agence nationale des titres sécurisés (ANTS), les industriels, on a exercé les pressions qui conviennent auprès de Bruxelles et l'on a réussi à obtenir un règlement qui nous va bien. **L'*eIDAS* est un succès** et je pense qu'à la FNTC ils le savent aussi. C'est une bonne base réglementaire qui permet de garantir une identité de bonne valeur. C'est vrai que des sociétés comme *Dictao* ou *Keynectis* y participent et que cela leur coûte un peu d'argent. **Je milite pour la mise en place d'un vrai crédit d'impôt normalisation.** C'est ce que je

propose. Mais, par les temps qui courent, dès qu'on parle de crédit d'impôt, on est crucifié. Or, je veux sortir vivant de cette noble arène.

Mme Anne-Yvonne Le Dain. – On ne peut pas non plus en permanence compter sur la puissance publique dès qu'il y a une dépense imprévue.

M. Jean-Pierre Quémard. – Je suis d'accord avec vous. Il ne s'agit pas de demander à l'État de tout gérer à la place des industriels. L'envoi des experts est de la responsabilité des industriels. Je dis simplement : payons une fois, mais pas trois, ce serait déjà pas mal.

Mme Anne-Yvonne Le Dain. – Certes. Mais on sent que le sujet est délicat, compliqué, difficile, et que les avis sont partagés au sein de l'Union européenne. Du côté de la Commission européenne, c'est très éparpillé au niveau des services qui sont concernés par ces questions-là. Il n'y a pas véritablement encore de posture. Elle se construit. L'affaire Snowden y a un peu contribué. Il ne faut pas sous-estimer non plus l'intérêt de l'opération. On sait bien qu'un certain nombre de gens avertis depuis longtemps se posaient ces questions-là. Mais il y a une opportunité qu'on tente de saisir. On sent bien que la position en Europe, par rapport à la détermination américaine, n'est pas stabilisée, en tout cas elle n'est pas claire. Les États-Unis ont une politique, elle s'exprime, elle s'affirme, elle ne se construit pas, elle est là. Et nous, nous essayons en permanence de trouver notre place.

M. Jean-Pierre Quémard. – Je vais reprendre l'exemple de l'*eIDAS*. On a travaillé en synergie complète avec les Allemands et cela s'est extrêmement bien passé. En Europe, il y a trois niveaux. Sur les problèmes de *privacy*, je travaille beaucoup avec la CNIL, de façon très étroite, pour définir les normes qui vont bien. Mme Isabelle Falque-Pierrotin a été élue à la présidence du G29. **C'est la France qui montre le chemin**, clairement. Nos experts sont bons, on sait faire. Le problème, c'est qu'on se met des semelles de plomb là où il faudrait avoir des chaussures un petit peu plus légères. Et les alliances, on les trouve en Europe. Le chef de la délégation allemande au SC 27 est un copain. Dans 95 % des cas, on est en phase.

Mme Anne-Yvonne Le Dain. – Les grandes entreprises qui utilisent l'Internet pour créer du travail, de l'emploi et du profit ne sont pas européennes. *Google*, *Amazon* ou *Apple* ne sont pas européennes. En tant que parlementaires, nous essayons de construire une pensée. Je ne suis pas dans un débat scientifique, intellectuel ou moral. On vous demande de nous aider à construire notre pensée. Elle n'est pas formée. C'est notre interrogation. Nous sommes face à ces *GAFA*.

M. Jean-Pierre Quémard. – *GAFA*, ça fait peur, mais j'ai toujours eu pour principe de ne jamais être victime.

Mme Anne-Yvonne Le Dain. – N'interprétez pas mes propos. Je n'ai pas dit que j'avais peur. Je constate un fait.

M. Jean-Pierre Quémard. – Les faits sont comme ça et je vous assure que dans les instances de normalisation que je pratique, on ne voit pas ces sociétés. Je n'ai jamais vu *Google*, *Amazon*, *Apple*, *YouTube*.

Mme Anne-Yvonne Le Dain. – Pour les noms de domaine, ils ont leur système auto-organisé qui s'impose à tout le monde, avec beaucoup de brio, et qui est en train de s'installer, avec notre accord, en Suisse. En a-t-on envie ou pas ? Est-ce bien ou pas ? Je ne sais pas. D'un système auto-organisé, doit-on passer à un système supraétatique qui s'organise et qui fait force de loi ? Ce sont de vraies questions.

M. Jean-Pierre Quémard. – Ce sont de vraies questions et je pense que la réponse sur ce genre de problème va être européenne et non française.

Mme Anne-Yvonne Le Dain. – On est bien d'accord.

M. Jean-Pierre Quémard. – Si vous voulez, avançons, émettons des propositions, discutons avec nos partenaires. Ce qui s'est passé au niveau du G29 sur les libertés individuelles, c'est un très bon exemple parce que ça s'applique à tout le monde. Et dans nos groupes de normalisation, on compte parmi nos experts une ou deux personnes de la CNIL qui se défendent. Et on voit les Allemands qui marchent avec, les Espagnols aussi, etc. Il faut créer le mouvement. Il faut y aller !

M. Philippe Wolf, ingénieur général de l'armement, auteur de nombreux articles et ouvrages sur le numérique. – Je vais partager avec vous ma vision d'ingénieur sur le *big data* et la sécurité. Certains ajoutent la sécurité aux quatre piliers du futur cyberespace que sont le *cloud*, la mobilité, les réseaux sociaux et le *big data*. M. Ross Anderson (Université de Cambridge, *Computer Laboratory*) résume ainsi la situation : « *Les vainqueurs sont ceux qui, dans un premier temps, ignorent la sécurité au profit de la facilité, puis, dans un second temps, verrouillent leur écosystème numérique plutôt que de nous protéger des méchants.* »

Les enjeux de sécurité des traitements de masse ne concernent pas principalement le secret, le fameux patrimoine scientifique et technique, mais surtout la vie privée et le libre arbitre qui sont les fondements de nos droits de l'homme. Un rapport de mai 2014 de la Maison Blanche sur le *big data* pointe le risque, je cite : « *Les grandes analyses de données ont le potentiel d'éclipser pour longtemps la protection des droits civils dans la façon dont les renseignements personnels sont utilisés dans le logement, le crédit, l'emploi, la santé, l'éducation et le marché.* » Je vais donc essayer de vous convaincre de la nécessité de sécuriser ce *big data* non seulement par de nouvelles régulations, mais surtout par des réponses techniques qui sont à inventer pour que ces régulations ne restent pas vaines.

Je vais essayer de chiffrer mes exemples sur le *big data*. L'octet étant la grandeur élémentaire pour coder un caractère, 1 téraoctet (10^{12}), c'est un disque dur, 1 pétaoctet quand on a 1 000 de ces objets, l'exaoctet c'est 1 million de fois, le zettaoctet 1 milliard de fois, le yottaoctet 1 trilliard de

fois cette capacité. En 2012, 4 exaoctets de données ont été générées, soit plus que dans les 5 000 années précédentes. Cela va croître d'un facteur 70 d'ici 2020. Un humain va absorber au plus 40 pétaoctets dans sa vie. C'est à rapporter aux 200 yottaoctets qui seront manipulés par Internet durant 60 ans. Le rapport est ici d'1 milliard. Mais ce n'est que le début du *big data*. **Avec le *big data*, il y a aura mille fois plus d'objets connectés que d'humains. Des voitures, des caméras, des machines industrielles, des équipements médicaux, etc., seront connectés et généreront en temps réel des données bien plus massives que celles disponibles aujourd'hui.**

Dans le champ scientifique, le philosophe Bernard Stiegler a dit tout à l'heure que notre vieille démarche de l'induction est morte ou va mourir par le *big data*. Dans le passé, il s'agissait de confronter les théories imaginées aux observations. Aujourd'hui, avec des téraoctets de données, on ne peut plus effectuer cette confrontation à la main. Il faut donc exprimer la théorie sous une forme prédictive, c'est-à-dire algorithmique. Si l'on veut se servir des observations pour imaginer des théories, il faut un traitement informatique que l'on appelle l'apprentissage automatique. **La nouvelle science qu'on nous annonce consiste donc à concevoir des algorithmes permettant de construire des théories à partir des observations. On pourra même se passer des hommes au profit des robots.**

Deux exemples dans le champ ouvert des sciences fondamentales. D'abord, le nouveau collisionneur du CERN produit 15 pétaoctets de données chaque année. La découverte du boson de Higgs va illustrer la recherche d'une aiguille dans une botte de foin. Cette recherche a nécessité une grille de 200 centres de calcul, soit 500 000 ordinateurs et 200 pétaoctets de stockage sur disque.

Si l'on prend l'humain, le séquençage d'un génome est égal à 3,4 milliards de paires de base, soit 1 gigaoctet. Vous pouvez mettre 1 000 ADN dans cet objet. Par manque de moyens financiers, les trois banques publiques ne permettent plus l'exhaustivité d'accès qui était l'idée de base. Une multitude de banques privées se mettent en place avec la création de 178 banques privées en 2013. **Une première crainte est une marchandisation du vivant** qui va réapparaître très vite à travers ces banques privées.

Dans le champ du renseignement, je vais utiliser un seul élément des révélations de Snowden. C'est le programme d'écoute de fibre optique *Dancing Oasis* de la *NSA*. Il effectue 57 milliards d'enregistrements par mois, soit 684 milliards par an. Le programme chargé de trier ces données s'appelle *Cissor*. Un câble de fibre optique transporte 25 pétaoctets de données par jour. Après un premier tri protocolaire, environ 3 à 6 pétaoctets sont traités par les calculateurs de la *NSA* tous les jours. Après traitement et analyse, il reste à la fin 50 téraoctets par an, ce qui n'est pas grand-chose, c'est vraiment la substantifique moelle de ce qui a traversé cet ensemble de fibre optique (celle-ci équipait le Moyen-Orient vers des pays intéressant les États-Unis).

On peut noter l'efficacité réductrice des traitements de la *NSA*. Le nouveau centre de stockage de la *NSA* dans l'Utah aurait une capacité de stockage entre 3 et 12 exaoctets, c'est-à-dire des millions de téraoctets. Avec l'aide de 10 000 *RAM* de serveurs, la *NSA* a les moyens de stocker toutes les communications.

Dans le champ de la mercatique, c'est « *big data is big value* ». Savez-vous par exemple que **chaque publicité ciblée fait l'objet d'un marchandage mondial en moins d'une demi-seconde** ? C'est *Google* qui est au cœur de ce système. Il a donné naissance à de nouveaux métiers : les *data brokers* ou courtiers en données, qui vont rafler et analyser toutes les données personnelles que nous éparpillons sur la Toile et ailleurs.

Un récent rapport de la *Federal Trade Commission* de mai 2014 s'inquiète de la non-régulation de ces courtiers. Ils ont quatre cibles de métiers : la première, c'est bien sûr la mercatique, la publicité ; la deuxième, c'est la vérification d'identité ; la troisième, c'est la détection de fraude ; et la quatrième, c'est la recherche de personnes. Celle-ci marche bien aux États-Unis puisque c'est un pays sans état civil.

Dans le champ de la finance, je vais vous donner des chiffres sur le *high-frequency trading* ou boursicottage de très haute fréquence. En bourse, aujourd'hui, le temps moyen d'exécution d'un ordre, c'est une seconde. **Dans le *high-frequency trading*, une transaction, c'est cinq microsecondes. Le record actuel est à 740 nanosecondes.** En 2012, plus de la moitié des ordres transitaient par les robots du *high-frequency trading*. Cela a encore augmenté aujourd'hui et va aller vers les 95 % très vite. On dit que dans le *high-frequency trading,* **une milliseconde gagnée, c'est 100 millions de dollars gagnés**. Le délit d'initié, c'est-à-dire avoir une information avant les autres, ça se monnaie, ça se joue à la seconde pour des clients *premium* qui paient un peu plus. Parfois, une information donnée deux secondes avant suffit pour ces robots. Des physiciens mettent en équation « l'éconophysique », une nouvelle branche de la physique qui vise à localiser physiquement ces machines et routeurs au plus près des salles de marché qui sont virtuelles aujourd'hui.

Le champ sociétal est sûrement le plus prometteur. Voici un exemple d'analyse des données urbaines dans une ville intelligente à partir du cas des pompiers de New York. Sur le million d'immeubles que compte New York, environ 3 000 prennent feu chaque année. Depuis juillet 2013, les pompiers de la ville ont mis en place un algorithme qui analyse 60 facteurs de risques d'incendie. Les 341 unités de pompiers de la ville doivent inspecter au total 50 000 immeubles par an. Leur algorithme établit un score de risques pour les 330 000 immeubles de New York et cela fournit aujourd'hui la feuille de route des priorités pour leurs visites hebdomadaires. L'an prochain, ou dans deux ans, on aura le retour sur l'efficacité de traitement de ces données massives.

Un dernier exemple sociétal, c'est la cartographie des épidémies de grippe. Des études très sérieuses ont montré que *Wikipédia* est plus efficace pour faire de la cartographie que *Google*. Il s'agit simplement de prendre en compte le nombre de gens qui font des recherches autour de la grippe. Et il a été prouvé scientifiquement que c'est beaucoup plus efficace pour prévoir les épidémies de grippe que les données produites par les organismes spécialisés en recherche médicale ou en santé publique. Dans le domaine de la santé, le *big data* aura un effet majeur.

Le risque, c'est de prendre pour des oracles des prédictions produites par des ordinateurs à partir de théories trop complexes pour être comprises. Et donc il faut faire très attention aux biais cognitifs qui sont produits par l'exploitation des données massives.

Je vois trois paradoxes dans le *big data*. Premièrement, le paradoxe de la transparence. On annonce partout que la protection des données personnelles est morte. M. Vint Cerf, l'un des créateurs d'Internet employé par *Google*, l'a dit : « *privacy is dead* ». Nos données personnelles deviennent transparentes. Et donc les traitements opérés par le *big data* devraient aussi l'être. Mais ce sont des écosystèmes numériques fermés qui vont manipuler avec le secret le plus absolu ces données personnelles. Et les décisions prises par les robots de surveillance sont totalement opaques.

Je vais illustrer ce paradoxe de la transparence avec les *GAFA*, même s'il ne faut jamais oublier ces vieux acteurs comme *Microsoft* et *IBM*. *Google* s'appuie sur la recherche en psychologie cognitive pour mieux atteindre son but qui est d'amener les gens à utiliser leur ordinateur avec plus d'efficacité. **Cette société ne sera pas satisfaite tant qu'elle ne disposera pas de 100 % des données de ses utilisateurs.** Je cite là quelqu'un qui travaille chez *Google*.

Deuxièmement, le paradoxe de l'identité. Le droit à l'identité nécessite le libre arbitre. Mais **les robots-programmes du *big data*, qui fonctionnent déjà, vont chercher à identifier qui nous devons être**, qui nous devons aimer, ce que nous devons consommer, ce qui nous est interdit, **jusqu'à influencer nos choix intellectuels et nous faire perdre notre identité**. Les robots produisent ces résultats-là. Par exemple, dans les révélations de Snowden, on apprend que le programme *Synapse* de la *NSA* vise à stocker, pour chaque internaute, 94 critères d'identité : numéro de téléphone, *emails*, adresse *IP*, etc. ; on n'a pas toute la liste. Ils vont permettre d'y corréler 164 types de relations : profilage par les réseaux sociaux, paiements électroniques, profils d'intérêt, déplacements, géolocalisation, etc. C'est l'identité au sens de la *NSA*.

Troisièmement, le paradoxe du pouvoir. **Le *big data* est censé nous fournir une boîte à outils pour mieux comprendre le monde. Mais ces robots ne sont pas entre les mains des individus mais d'institutions intermédiaires qui ont le pouvoir de manipulation.** Le *big data* va donc créer des vainqueurs et des vaincus. Par exemple, dans le *high-frequency*

trading, les vainqueurs sont déjà connus. Les vaincus, ce sont les petits porteurs, ils n'ont plus aucune chance dans ce monde-là, dans cette bataille de robots. Les techniques utilisées par les robots ont des noms évocateurs. Pour la plupart, elles sont offensives et bientôt destructives. Dans le *high-frequency trading*, la dérégulation se fait presque exclusivement au niveau des acteurs. Plus personne n'arrive à comprendre ce qui s'y passe.

Je vais prendre un exemple de ce qu'on appelle un feu de brousse médiatique. C'est un faux *tweet* de l'*AFP* qui a été reçu par les 2,5 millions abonnés de l'*AFP* le 23 avril 2013, à 13 h 07 et 50 secondes, qui annonce un attentat à la Maison Blanche, dix jours après les attentats de Boston. Le piratage sera d'ailleurs revendiqué par l'armée électronique syrienne. Entre 13 h 08 et 13 h 10, le *Dow Jones* va perdre 147 points, soit 136 milliards de dollars de capitalisation. 105 milliards d'euros. À la fin de la journée, le *Dow Jones* finit en hausse de 1,5 %. L'argent a donc changé de main, il n'a pas été détruit. Une enquête a été ouverte par le *FBI* et la *Securities and Exchange Commission (SEC)* pour essayer d'éclaircir un doute sur vingt-huit contrats à terme. Je n'ai pas vu encore les résultats de cette enquête. Il y a deux hypothèses. Soit il s'agit d'un emballement algorithmique autonome soit c'est une des prises de décision humaine sous la peur pendant les 17 secondes avant la réaction des robots logiciels qui a amplifié la peur.

Après l'intervention de la ministre en charge du numérique, nous verrons les solutions pour sécuriser le *big data*. Pour en savoir plus sur le *high-frequency trading*, je vous invite à lire *Le nouveau capitalisme criminel*, de Jean-François Gayraud, commissaire divisionnaire de la police nationale. Il donne l'équation suivante : très grande vitesse multipliée par très grands volumes égale invisibilité. Dans le jargon populaire, on dirait : plus c'est gros, plus ça passe.

M. Bruno Sido. – Nous sommes ravis d'accueillir Mme la ministre en charge du numérique. Je précise que Mme Anne-Yvonne Le Dain et moi-même préparons un rapport sur la sécurité numérique, une question importante que nous découvrons audition après audition depuis presque un an. Nous nous limiterons à une analyse des données générales sur la sécurité numérique et à deux applications, l'une relative aux entreprises du secteur l'énergie, et l'autre à celles du secteur des télécommunications. Notre rapport devrait sortir à l'automne prochain.

Je ne doute pas que ces sujets intéresseront nos collègues tant il est vrai que l'OPECST est chargé de les éclairer sur un certain nombre de sujets scientifiques et technologiques qui vont de la biotechnologie à la sécurité numérique, en passant par le nucléaire et bien d'autres encore. À l'occasion des projets et propositions de lois qui peuvent venir en discussion, nos rapports constituent déjà une bonne base de réflexion. Même s'ils ne sont pas forcément à jour, parfois ils datent déjà de un an ou deux, c'est le rôle des commissions et des rapporteurs de les actualiser. Les dix-huit députés et

dix-huit sénateurs qui composent l'Office travaillent d'une façon apolitique sur ces sujets très importants.

Mme Anne-Yvonne Le Dain. – Je souligne que, ce matin, le travail a été accompli avec une grande liberté de ton, dans des perspectives à la fois techniques, juridiques, intellectuelles, morales, philosophiques, sur la manière dont l'Union européenne se positionne sur ces questions-là. Non seulement nous voulons conduire une analyse de risques mais également envisager que cela puisse être une opportunité, un chemin sur lequel nous devons nous positionner de manière élégante et vive, y compris en termes de vocabulaire.

Le recours à la loi peut être une solution, une opportunité, dans la mesure où il s'agit de se ménager des possibilités d'ouvrir des portes, tout en précisant les conditions des retraits, des difficultés et des recours. C'est délicat, complexe, mais c'est important, parce que, en ce début du XXIe siècle, nous sentons bien que nous nous trouvons au cœur d'une révolution considérable, touchant à la fois à la démocratie mais aussi au modèle économique et social, avec la manifestation d'une grande inquiétude : la puissance des machines, la puissance du *soft*, la puissance du *hard*, et, derrière, le grand néant de l'oisiveté.

Mme Axelle Lemaire, secrétaire d'État chargée du numérique, auprès du ministre de l'économie, du redressement productif et du numérique. – Je remercie Mme la députée Le Dain et M. le sénateur Sido pour cette invitation. J'ai bousculé mon agenda ministériel pour être parmi vous pour deux raisons.

D'abord pour témoigner de l'importance que j'attache aux travaux de l'OPECST. Je trouve très important que le Parlement se penche sur les évolutions technologiques avec l'approche qui est la sienne, qui n'est pas forcément celle d'une expertise technique authentique, mais qui consiste à recontextualiser les débats qui traversent à l'heure actuelle notre société, avec l'œil du législateur et l'œil du politique, de façon à opérer cette traduction entre la technique, le monde scientifique d'une part, et le grand public d'autre part. C'est donc une mission très importante que vous conduisez.

La deuxième raison de ma présence est liée au sujet que vous avez choisi de traiter. J'attends avec impatience les conclusions qui paraîtront dans votre rapport à l'automne prochain. Il est vrai que, pour traiter de la sécurité des réseaux numériques, on aborde classiquement ce sujet technique par technique, secteur par secteur, en oubliant d'avoir une approche globale et une vision politique et stratégique sur ces thématiques.

Ma venue a été organisée en dernière minute. Vous me pardonnerez donc le caractère peu structuré mon propos – ce qui est contraire à la manière dont j'aime opérer d'habitude.

Je voudrais aborder ce sujet sous deux angles : le premier, c'est la sécurité en tant que telle et surtout la sécurité des systèmes d'information ; le second, c'est la question de la confiance numérique de manière plus globale.

La sécurité des systèmes d'information, notamment celle des réseaux des opérateurs d'importance vitale (OIV), est **une obligation qui pèse désormais sur les infrastructures en France** puisque le cadre réglementaire a été récemment rénové. Auparavant, les opérateurs télécoms devaient garantir la sécurité des systèmes d'information utilisés par les entreprises selon des normes définies par les autorités françaises à un niveau élevé de sécurité. Cette obligation a été étendue à tous types d'infrastructures relevant des OIV, à savoir dans les secteurs de l'énergie, des transports et de l'eau. On dépasse le champ de départ des télécoms pour couvrir un champ plus vaste d'infrastructures, le cœur de cible restant les grandes entreprises privées qui travaillent dans les réseaux, avec une idée : **lorsque ce réseau tombe en panne ou s'il fait l'objet d'une attaque et qu'il est mis en danger, il est primordial que l'État, en lien avec l'acteur concerné, puisse réagir rapidement et protéger le système d'information pour des raisons économiques et de sécurité nationale.**

Cette obligation a été l'objet, entre autres, de **la loi de programmation militaire** qui **étend à un ensemble d'OIV les exigences de sécurité qui étaient initialement applicables aux télécoms**. Ces OIV ont l'obligation de notifier toutes les attaques à l'ANSSI, et, **si le cas se présente, l'ANSSI a alors la capacité de prendre la main sur les systèmes d'information**. L'État devient en quelque sorte gestionnaire d'un système, ce qu'il ne faut surtout pas confondre avec un État qui utiliserait des données.

Sur ce point, on sent une certaine confusion dans les esprits par moment. Nous ne sommes pas dans l'hypothèse d'un État qui utiliserait des données transmises, par exemple par des opérateurs de téléphonie mobile, et qui peuvent concerner des citoyens, pour des raisons de sécurité nationale. Non, lorsqu'on parle de la sécurité des réseaux des OIV, on parle bien des systèmes d'information. **En cas de problème avéré, l'État se substitue à l'opérateur pour garantir l'intégrité des systèmes d'information sans pour autant regarder le contenu de l'information détenue par l'opérateur.**

Cette évolution est la plus récente au niveau national. Au niveau européen, une directive importante est en cours de négociation. Elle a d'ailleurs fait l'objet de discussions lors du dernier Conseil européen consacré aux télécoms qui réunissait l'ensemble de mes homologues à Bruxelles. Le Gouvernement français a une demande concernant cette directive européenne sur la sécurité des systèmes d'information. En effet, les *Over-The-Top (OTT)*, c'est-à-dire les grandes plates-formes numériques, ont aujourd'hui, de par leur couverture économique et le nombre d'utilisateurs concernés par les services offerts, un rôle stratégique tout aussi important pour l'économie et la sécurité de notre pays que celui des OIV dans leur définition plus classique.

Très concrètement, **si les serveurs de *Google* venaient à être attaqués ou à tomber en panne, les conséquences seraient tout aussi dramatiques que pour des OIV plus historiquement classiques**. Et donc, sur cette question, **l'une des revendications du Gouvernement français est de passer d'une approche traditionnelle d'infrastructure à une approche étendue aux services**.

Cette approche se décline aussi dans d'autres domaines. Plus largement, l'enjeu est celui d'une reterritorialisation des problématiques. À partir du moment où l'on veut imposer un niveau élevé de sécurité, de protection des données, imposer sur le territoire la valeur créée par les usages numériques, il y a toute une série de problématiques qui font que, de manière générale, dans les négociations au niveau européen, le Gouvernement français cherche à inclure de plus en plus les *Over-The-Top* dans les négociations.

Le Gouvernement agit aussi sur l'offre industrielle en la matière. Cela ne concerne peut-être pas directement la manière dont vous avez conçu le sujet mais vous serez sans doute intéressés, puisque j'ai récemment piloté le plan industriel qui, parmi les trente-quatre plans de la Nouvelle France industrielle, est consacré à la cybersécurité. Ce plan vise à la fois à développer une filière de l'offre industrielle française en matière de sécurité et à aider à articuler la demande sur ce marché. J'aimerais vous en présenter rapidement les contours.

Il s'appuie sur une réalité souvent méconnue, **la présence sur notre territoire d'acteurs industriels d'envergure mondiale et des PME très performantes dans des secteurs très pointus de la sécurité des systèmes d'information**. Ce plan réunissait ces acteurs qui ont travaillé en bonne concertation avec l'administration et les responsables politiques pour faire des propositions assez concrètes. De ce plan est né l'idée d'un label France, qui permettrait aux acteurs français de recevoir une reconnaissance et une visibilité, qui est demandée, et qui pourrait les aider à les accompagner y compris en dehors de nos frontières.

La piste d'une meilleure orientation de la recherche et du développement a également été évoquée, qu'elle soit privée ou publique, pour faciliter l'industrialisation et pour permettre aux acteurs du secteur de conserver une réelle avance technologique.

Enfin, à l'autre bout de la chaîne, nos entreprises comme nos administrations doivent aussi être sensibilisées aux enjeux de la cybersécurité. Et là, nous nous situons plutôt du côté de la demande. Or, ce que l'on constate, c'est que l'offre industrielle reste souvent très pointue, assez chère, et qu'elle répond à des demandes et des besoins spécifiques, quasiment à la commande. De ce fait, elle est accessible aux grandes entreprises. Certaines en font usage avec raison, comme *Thales*, *Airbus*, *Capgemini* par exemple. Et puis, à l'opposé du spectre, **nos PME ont besoin d'être en capacité d'accéder aux services offerts par les entreprises**

spécialisées dans la cybersécurité. Mais ce n'est pas une priorité pour elles parce que souvent elles méconnaissent les risques liés à l'utilisation des outils numériques. Un gros effort de pédagogie est à faire sur ce sujet. Pour cela, il faut, à l'échelle de la demande industrielle, améliorer la qualité et la fiabilité des services qui peuvent être rendus aux petites entreprises.

J'en viens maintenant au sujet plus large de la confiance dans le numérique puisque, dans le cadre de mon intervention, on m'a demandé de parler du risque. Il est vrai que le numérique est souvent approché sous l'angle du risque de manière un peu anxiogène. C'est un lieu commun de dire que le numérique est partout, qu'il occupe une place croissante dans nos vies, dans le fonctionnement de nos économies, dans la société de manière générale, et que ce nouveau monde est une source d'inquiétudes bien réelles dans le ressenti des citoyens. Un sondage récent indique que **77 % des Français sont inquiets de l'usage qui pourrait être fait de leurs données personnelles**.

Face à des technologies très réactives, en évolution constante et rapide, face à ce monde des données, des protocoles et des flux, qui peut être perçu comme une sorte de boîte noire qui avale nos données, **quel niveau de confiance l'État peut-il garantir**, notamment lorsque cela concerne des informations dites sensibles ou personnelles, sachant que les flux d'informations échangées sont de plus en plus importants ?

Il faut rappeler que, dans ce nouveau monde, nous ne sommes ni des victimes ni des témoins passifs de ces changements technologiques rapides. **Il revient à l'État, aux pouvoirs publics, d'être vigilants, de sanctionner les abus mais aussi d'apporter tous les outils qui permettront d'instaurer la confiance dans le numérique.** Elle est essentielle pour les citoyens, pour s'éloigner de ce sentiment de dépossession qui est réel. Elle est aussi nécessaire pour l'économie, et ce, pour deux raisons. Par exemple, pour acheter sur Internet, il faut avoir un niveau de confiance suffisant dans les outils. Le franchissement de l'achat sur Internet semble avoir été une étape réussie en France puisque 80 % des Français ont fait au moins une fois dans leur vie un achat sur Internet. Cela a pu se faire parce qu'il y a plus de dix ans, l'État a mis en place les outils nécessaires à la construction d'une confiance économique.

Aujourd'hui, la donne a de nouveau changé et, de nouveau, il faut se donner les outils pour créer cette confiance. Ces outils existent. Ils sont connus. Je suppose que les experts que vous avez auditionnés vous ont parlé de l'arsenal législatif et réglementaire qui existe en France, notamment pour protéger les données personnelles. **Cet arsenal devra faire l'objet d'une actualisation du fait des technologies qui sont rapidement apparues.** J'ai entendu quelqu'un citer les objets connectés. Effectivement, ils vont se multiplier. Dans quelques années, les objets pourront utiliser les flux de milliards de données. C'est également vrai avec l'industrie du *big data*, une

industrie qui intéresse beaucoup de nos entreprises en France. Nous avons, dans certains secteurs du *big data*, une réelle avancée technologique.

Il faut à la fois construire la confiance pour que les citoyens se sentent protégés, mais aussi parce que **la France et l'Union européenne ont une carte à jouer dans la compétition internationale actuelle au sein de l'industrie numérique**. Je crois que c'est ce que sous-entendait Mme Le Dain. Il se trouve que nous avons des entreprises qui ont su développer des solutions technologiques qui offrent des outils protecteurs et des outils promoteurs de la confiance grâce à un cadre réglementaire sécurisé.

Tout l'enjeu du projet de loi numérique consistera à actualiser le régime juridique de la protection des données pour que l'innovation qui se fait en France autour de la donnée ne soit pas freinée, tout en conservant un haut niveau de protection des données de nos concitoyens, en réponse à une demande très forte de la population.

Dans ce domaine, l'Union européenne a un rôle très important à jouer. Certes, je parle de la France mais les flux de données sont internationaux. Internet, par définition, est universel et sans frontières. On sent bien que **la France, si elle agissait seule en ce domaine, aurait du mal à s'imposer vis-à-vis d'acteurs géants** qui ont une stratégie économique et politique et une force de frappe supérieure.

D'où l'importance des négociations, en particulier autour du partenariat transatlantique, où **la question des données est diffuse mais omniprésente** dans les chapitres de la négociation. D'où l'importance des négociations en cours sur le projet de règlement communautaire sur les données personnelles, par exemple. Là aussi, il y a une spécificité française qui consiste à offrir un cadre élevé de protection des données personnelles. **Tout l'enjeu consiste à convaincre nos partenaires européens que ce cadre protecteur n'est pas un handicap dans la compétition internationale mais que, au contraire, il peut être un atout.**

Voilà les enjeux qui sont les nôtres. J'ai essayé de poser dans des termes assez globaux la question qui m'avait été transmise.

Mme Anne-Yvonne Le Dain. – Mme la ministre a été particulièrement claire, précise et ouverte. Je crois que cela nous convient bien. Probablement que, dans le corps des textes que nous serons amenés à écrire, nous devrons affiner et préciser certains éléments. Émanant de l'Assemblée nationale ou du Sénat, ces textes ont une valeur bien plus que symbolique. Quelqu'un a-t-il une question à poser ?

M. Jean-Pierre Quémard. – Vous avez fait allusion, madame la ministre, au plan 33 et à l'Alliance pour la confiance numérique (ACN). Il s'avère que je préside l'ACN et que j'ai largement contribué au plan 33 de la Nouvelle France industrielle. Je voudrais simplement attirer votre attention sur un point que vous n'avez pas mentionné, mais dont on a parlé dans ce groupe. Il s'agit du recours à la normalisation et à la standardisation.

C'est quelque chose de très important dont nous aurons probablement l'occasion de reparler.

Je voudrais également attirer votre attention sur l'évaluation de la certification et de l'utilisation des technologies. Comme j'ai déjà eu l'occasion de le dire, **une technologie n'est pas bonne ou mauvaise, elle doit reposer sur un modèle à trois composantes : une réglementation, une normalisation et une évaluation**. Ces principes-là s'adressent aussi bien au *Security by design* qu'au *Privacy by design.* Ce sont des choses extrêmement importantes pour pouvoir développer une activité française exportatrice.

Dernier point, il faut faire attention dans le domaine de l'usage des technologies. En ce moment, nous avons quelques doutes sur des projets de loi relatif à la biométrie, etc., qui auraient tendance à nous mettre dans un coin en imposant des réglementations françaises bien plus dures que ce qu'on peut trouver partout ailleurs dans le monde. Par exemple, **interdire complètement la biométrie, pour nous, c'est extrêmement dangereux, cela bride toute la recherche et toute innovation**. Il faut donc faire extrêmement attention. C'est le rôle des industriels de tirer la sonnette d'alarme sur ces sujets, mais je suis sûr que vous en êtes tout à fait consciente.

Mme Axelle Lemaire. – Vous avez raison de souligner l'enjeu de la normalisation. C'est effectivement une attente forte de la part de la filière de la cybersécurité en France. J'espère qu'elle pourra être entendue parce que là aussi, **la bataille des normes se joue chez nous mais elle se joue surtout au niveau international**. La reconnaissance par la normalisation et par le respect de normes est tout à fait importante. Elles sont négociées dans un cadre européen dans lequel la France peut être entendue.

Quant à la biométrie, là aussi, nous avons **quelques champions français** en ce domaine. Alors, oui, des initiatives parlementaires visent à préciser par la voie législative un cadre qui jusqu'à présent a été surtout élaboré par la CNIL. L'usage de la donnée biométrique est potentiellement contesté par le grand public, lequel n'est pas toujours au fait du niveau d'intrusion, existant ou non d'ailleurs. Souvent nous sommes dans une perception un peu irrationnelle. Mais le rôle du législateur est aussi d'identifier les réticences du grand public. Et **j'ai noté certaines réticences, notamment lorsque l'usage des données concerne les enfants**. Il y a eu un débat sur la possibilité qui devra être laissée, ou pas, aux enfants par exemple, de payer leur repas dans les cantines en utilisant la paume de la main comme lecteur de leurs données pour identification. C'est un exemple de déclinaison d'usage de données biométriques qui heurte une certaine partie de la population. À mon sens, le législateur a toute légitimité à l'entendre.

Là encore, un équilibre est à trouver. L'innovation est absolument essentielle en ce domaine, je pense notamment aux moyens de paiement, où, là aussi, la France a des atouts certains. Je pense à l'accès aux bâtiments. Les déclinaisons possibles de l'usage des données biométriques sont

aujourd'hui nombreuses, elles le seront demain bien plus encore. **Il est important de ne pas s'exclure de la course internationale du fait d'un régime législatif qui serait trop rigide.**

Je crois que les parlementaires ont compris ces enjeux. Un groupe de travail a d'ailleurs été mis en place sous l'égide du ministère de l'économie, du redressement productif et du numérique, avec les parlementaires et avec la CNIL, pour voir comment les préoccupations citoyennes peuvent être entendues, comme celles des acteurs économiques.

M. Bruno Sido. – Je vous remercie, madame la ministre, d'avoir apporté votre éclairage sur nos travaux et sur la politique du Gouvernement en la matière. Nous revenons maintenant à la suite de l'intervention de M. Philippe Wolf.

M. Philippe Wolf. – Comment essayer de sécuriser l'exploitation des données massives ou *big data* ? Il y a deux écoles. L'une considère qu'il n'y a rien de neuf, qu'il s'agit de sécurité des systèmes d'information classique avec un effet volume. Je vais essayer de vous prouver qu'il existe une autre façon d'aborder ces choses qui réclament une toute nouvelle manière de sécuriser les systèmes d'information.

Je vais vous parler d'un certain nombre de technologies où tout un ensemble de très petites entreprises ou de très petites structures sont très dynamiques en France. Aujourd'hui, on a beaucoup d'inventivité, le seul problème étant de mettre toutes ces briques-là ensemble pour aboutir à des offres plus globales.

Les problèmes de sécurité liés au *big data* sont multiformes. Ils dépendent de l'origine des données (on a parlé de l'*open data*, de données privées, mixtes), de la loyauté de leur recueil (c'est souvent un problème), de la présence ou non, directe ou indirecte, de données personnelles (c'est plus facile quand il n'y en a pas), de l'objectif poursuivi (dans le cas du bien commun scientifique, on met tout en ligne, dans le cas de l'avantage concurrentiel, il faut tout protéger), de la transparence ou de l'opacité des buts poursuivis (dans le *high-frequency trading*, on est plutôt dans l'opacité), des infrastructures publiques, privées, mixtes, de stockage et de calcul, et du caractère, ouvert ou fermé, des traitements algorithmiques.

Les attaques contre le *big data* sont multiples. Ce sont toutes les attaques classiques, les atteintes contre les infrastructures, mais aussi, et c'est nouveau, les usages détournés de calculs, des clonages de masse frauduleux, des falsifications, parfois partielles, des données, de la manipulation de l'information ou désinformation.

Dans le *big data* se joue une nouvelle algorithmique, les modèles *no-SQL*. On appelle cela le modèle du sujet - verbe - complément. Ils sont plus souples que les modèles figés d'une base de données et cela va être très intéressant pour les **moteurs de recherche sémantique**. On est très fort

en France sur ce type de moteurs. Par exemple, la société *Pertimm* fait le logiciel *e-Dating* du site *Meetic*, qui marche bien.

Derrière ces données, derrière cette algorithmique, on met souvent quatre V : Volume - Variété - Vélocité - Véracité. Ils obéissent aux limitations de deux théorèmes qui ont été démontrés en 2002. On peut les rapprocher d'un vieux théorème que j'enseigne souvent, le « théorème du virus » de 1986, selon lequel **la malveillance d'un code informatique est indécidable**, et donc on va traîner ce problème jusqu'à la fin des temps.

Ces théorèmes sont intéressants parce qu'ils rendent nécessaires la présence de l'homme dans les algorithmes utilisés par le *big data*. On aurait pu penser qu'il n'y a plus d'homme dans la boucle, mais il va falloir régler certains paramètres.

Derrière ce *big data*, on a de nouveaux dangers. **Les protections périmétriques et la surveillance interne des traces ou des comportements sont nécessaires mais ne suffisent plus. J'appelle cela le mythe des lignes Maginot**. La virtualisation et l'ubiquité sont constitutives des architectures massives. Cela va augmenter les surfaces d'attaques, les délocaliser. Le *big data* s'attaquera partout dans le monde. **Les efforts et les budgets de sécurisation devront se concentrer sur les données les plus sensibles**. Le nomadisme, ou le fait que les salariés ont tout sur leur *smartphone* dans les entreprises, va obliger toutes les autres données à une transparence forcée. Les vieux modèles de sécurité statique ont quarante ans. Ils sont obsolètes aujourd'hui.

Alors que faire ? Innover. Et **il faut innover dans les trois fonctions classiques de la sécurité des systèmes informatiques (SSI) que sont la disponibilité, l'intégrité et la confidentialité**. Je vais les prendre un peu systématiquement.

La condition de base, c'est de sécuriser les infrastructures qui traitent le *big data*. En majorité, le *big data* va se faire dans le nuage numérique ou *cloud*. On a déjà beaucoup parlé du *cloud* maîtrisé – je n'ose plus parler du *cloud* souverain. Cette sécurité obéit à quatre conditions : faire appel à des **prestataires de confiance** ; être capable d'**auditer réellement la solution dans un temps court** ; avoir la **garantie de réversibilité** (en pouvant changer de prestataire sans perte et en récupérant ses données) ; et surtout rédiger les **contrats sous la protection du droit national**. C'est la chose importante et la seule à retenir sinon on ne pourra jamais gérer le risque juridique.

La deuxième condition, c'est de marquer les données. Je vous donne l'exemple d'*Accumulo*, un système de gestion de base de données qui a été créé par la *NSA* et qui a été légué à la fondation libre *Apache* en 2011. Ce logiciel utilise le système de fichier *Hadoop* qui définit des mécanismes de sécurité au niveau des cellules. Si vous ne marquez pas les données, vous ne pourrez jamais sécuriser le *big data*. Autrefois, on appelait cela la labellisation

des données. J'ai déjà trouvé des sociétés américaines, pas encore des sociétés européennes, qui offrent des solutions intégrées de cryptographie du *big data* autour de ce système de marquage des données.

La troisième condition, c'est de protéger les données dites sensibles. Dans le cas du *big data* non ouvert, privé, la confidentialité des données stockées ne pose pas de problème particulier, c'est-à-dire qu'on peut aller les stocker n'importe où dans le monde et il n'y a pas de problème par rapport au fait de devoir les localiser en Europe**.** Il faut cependant **garder la capacité de gérer ses propres clés de chiffrement ou de signature**, de préférence dans un coffre-fort numérique labellisé, ou en confier la gestion à des tiers réellement de confiance.

En revanche, pour rendre confidentiels les calculs, il manque aujourd'hui un ingrédient essentiel qui serait une implémentation pratique du chiffrement dit « homomorphe », qui donnerait le moyen de réaliser diverses opérations sur le chiffré sans recourir à l'opération de déchiffrement complète. En 2009, il y a eu une avancée considérable dans le domaine de la cryptographie malléable, après vingt-cinq ans de recherche. De temps en temps, un verrou saute. On a une rupture. Depuis, les choses vont très vite et des solutions apparaissent déjà. J'ai vu par exemple au *CEA* fonctionner les premiers logiciels homomorphes. Cela va nécessiter de reconcevoir toute une algorithmique adaptée, comme pour les hypothétiques calculateurs quantiques ou ADN.

Le seul problème du chiffrement homomorphe, c'est qu'il est tellement compliqué que le public ne comprendra jamais rien. Il y a un problème de compréhension des usages. Je ne peux plaider que pour **la formation au numérique depuis la maternelle**. C'est essentiel et je le répéterai toujours. Si on ne le fait pas, on est perdu. L'Académie des sciences s'en est ému, tout le monde s'en est ému. L'Angleterre et les États-Unis bougent, il faut que ça bouge en France aussi.

Ces nouvelles techniques cryptographiques vont permettre de réinventer la notion d'intégrité. **L'intégrité stricte n'est plus nécessaire** quand il s'agit de manipuler des données non structurées, parfois faussées ou incomplètes, ou de travailler principalement par échantillonnage. J'appelle cela une tolérance au flou, au calcul approché et aux mutations, qui va rompre le clonage binaire parfait. Ils sont les ingrédients porteurs d'une meilleure adéquation du *big data* au monde réel. Le monde réel n'est pas un clonage parfait. Et le *big data* est censé nous aider à mieux comprendre le monde.

Cette nouvelle intégrité devrait nous aider à vérifier les divers paramètres d'une donnée : attributs, granularité fixée initialement, accessibilité, authenticité, contrôle des finalités, dont la dissémination.

Parmi les applications, on a parlé de la biométrie. Le stockage sûr et centralisé des données biométriques est déjà proposé au Japon. **On sait**

aujourd'hui constituer une base biométrique centralisée, protégée, dont la perte n'a pas de conséquences. C'est une grande nouveauté qui va changer la donne.

À partir de ces briques de base, on va pouvoir construire de nouvelles fonctions de sécurité. Un pan croissant du *big data* touche aux données personnelles qui sont souvent son carburant premier. Les progrès des moteurs de recherche intelligents permettent d'identifier facilement une personne à partir d'un nombre très réduit de caractères, cela d'autant plus que notre intimité est mise à nu dans les réseaux sociaux. Les croisements de données permettent des attaques sémantiques qui ne visent pas que les protections théoriques mais leur implantation pratique.

Pour répondre à ce risque, les critères communs dont on a parlé tout à l'heure ont introduit, dès 1999, **quatre fonctions de sécurité pour la protection des données personnelles : l'anonymat, le pseudonymat, l'impossibilité d'établir un lien et la non-observabilité.** Le pseudonymat par exemple est impératif dans tous les traitements massifs concernant la santé humaine.

Ces fonctions font l'objet de travaux algorithmiques novateurs principalement en Europe mais elles tardent à s'implanter dans les traitements *big data*. Je réfute les faux débats sur des fonctions de sécurité comme l'anonymat qui servent à la fois l'honnête homme et le criminel. Il y a plus d'honnêtes hommes que de criminels. Ce sont donc des fonctions impératives.

Il y a une autre piste avec la renaissance d'une nouvelle forme de signature dite anonyme. La signature non anonyme n'a jamais marché et ne marchera jamais. La signature anonyme ne révèle que les attributs nécessaires. En plus, la possibilité de lever l'anonymat existe, ce qui va rassurer la cyberpolice.

La protection des informations nécessite une résistance au mirage du *big data* simpliste. On ne peut pas totalement éliminer le rôle du sujet dans la production de l'information ou de la connaissance par le *big data*. Vous savez que **la signification d'une information est toujours relative. Il s'agit donc de mesurer l'intelligibilité, la vérifiabilité, la traçabilité, d'estimer la responsabilité contractuelle, de gérer les conflits d'influence, de repérer les fausses nouvelles**. Des amendes record touchent aujourd'hui des institutions financières. Elles sanctionnent des infractions à répétition (*subprimes*, *Libor*, *Euribor*, taux de change, marché pétrolier) qui n'auraient pas été possibles sans l'obscurcissement numérique.

De plus, la capacité de l'absorption humaine est limitée. Un écart de plus en plus grand va se créer entre les capacités des robots-programmes et l'homme. Quand les résultats espérés ne seront pas là, on aura une tendance naturelle à complexifier les traitements, par une massification encore plus grande des données et par l'ajout de paramètres automates, alors qu'il

faudrait au contraire modéliser, analyser, expliquer et mieux cibler les données. Cette tendance à l'entropie porte en elle le germe de ce que l'essayiste Paul Virilio appelle « *l'accident des connaissances* ».

Le *big data* offre également des possibilités pour la défense des systèmes d'information, mais je crois que j'ai dépassé le temps qui m'est attribué.

Je voudrais dire un mot sur la cyberdiversité. La défense des systèmes d'information ne se réduit pas aux architectures des systèmes. **L'assemblage de composants sécurisés ne garantit pas la solidité du tout. La complexité va faciliter le travail de l'attaquant** parce qu'il va chercher un chemin d'attaque et il trouvera une porte d'entrée. ***A contrario*, la monoculture technologique à la fois favorise et fragilise le contrôle centralisé. Il faut donc protéger la cyberdiversité** qui est malmenée par beaucoup d'écosystèmes numériques fermés, dont aucun n'est européen. Par analogie avec la diversité des espèces, qui est le plus grand rempart immunitaire contre la perte d'un écosystème, **la cyberdiversité reste le constituant principal d'une véritable défense en profondeur**.

En conclusion, il s'agit de faire du *big data* un outil de progrès sociétal, par exemple pour les *smart cities*. Il faut donc en maîtriser les dérives. Mais la France ou l'Union européenne voudront-elles revenir dans le champ technologique ? C'est une condition préalable. Je propose une opportunité, c'est le remplacement du silicium par du graphène. C'est du carbone. Ce remplacement va survenir dans les dix années qui viennent. Va-t-on monter un grand programme européen pour être en tête dans l'électronique graphène ?

Quoi qu'il en soit, il faudra faire du *big data* avec un certain nombre de règles d'éthique qui sont celles de la vieille Europe : **dignité, réserve, droiture**. Je souhaite que la maîtrise et la domestication des robots logiciels du *big data* s'engagent sur une régulation qui va s'inspirer de ces principes d'Epictète.

Finalement, **deux approches économiques s'opposent. L'économie responsable – en France, on dit souvent sociale et solidaire – *versus* l'économie du chaos. Derrière le numérique de masse se joue un choix de société**.

M. Pierre Lasbordes. – Je vais maintenant me tourner vers Me Éric Caprioli. Pour vous, la sécurité numérique, c'est d'abord une culture, cela nécessite une sensibilisation de chaque instant mais aussi l'élaboration d'instruments tels que des chartes et la nécessité d'avoir des normes européennes, voire internationales. Pouvez-vous nous en dire un peu plus ?

Me Éric Caprioli, docteur en droit, avocat à la Cour d'appel de Paris, vice-président du Club des experts de la sécurité de l'information et du numérique (CESIN). – Je vais aborder cette question du risque et de la sécurité numérique du point de vue du praticien, en tant qu'avocat qui travaille sur le sujet avec des responsables de la sécurité des systèmes d'information (RSSI) et des directeurs des systèmes d'information.

Je partage beaucoup des analyses évoquées, comme **la sensibilisation et l'éducation au numérique à la maternelle**. Les risques créés par le numérique bouleversent nos sociétés, c'est une porte ouverte que j'enfonce volontiers. Les données constituent aujourd'hui le principal gisement de valeurs de nos sociétés, que ces données soient personnelles, techniques ou économiques, puisque cela permet de faire le lien avec l'intelligence économique et la sécurité. Quand on parle de patrimoine informationnel, c'est très lié à cette valorisation de la donnée, M. Bernard Stiegler nous l'a rappelé. Il faut souligner que le plan Al Gore-Clinton, en 1993, relatif aux autoroutes de l'information, n'avait pas pour objectif de développer la planète et les pays en voie de développement mais visait à conquérir le monde nouveau. Le génie américain avait créé une nouvelle frontière. Et nous, Français et Européens, ne l'avons pas perçue comme tel.

Alors, aujourd'hui on a des risques, on a de la sécurité, une révolution est en marche et on n'en est qu'au commencement. Quand j'écrivais sur ces sujets il y a plus de vingt ans, notamment dans ma thèse de doctorat, je disais que le bouleversement serait fondamental et sociétal puisque, à l'époque, on parlait de bribes de bouleversement. Or, aujourd'hui, on voit des menaces nouvelles. Que ce soient les forces de police, de gendarmerie ou les entreprises, les institutions et les opérateurs économiques doivent tous y faire face. Avec l'Internet, les multiplications des attaques sont sérieusement et considérablement développées avec de l'ingénierie sociale, de l'informatique. Si vous avez lu l'œuvre de M. Kevin Mitnick, vous vous rappellerez que dès les années 1980, il s'agissait d'ingénierie sociale *via* le téléphone et on récupérait des données. Par ce biais-là, on pénétrait des systèmes qui n'étaient pas connectés. Le numérique n'a donc pas commencé avec l'interconnexion puisque dès cette époque, on pouvait déjà pénétrer des systèmes. On volait des heures de téléphones et toutes autres choses mais ce n'est pas très différent. Le « mal » s'adapte et se déplace.

Aujourd'hui, les dommages sont plus dévastateurs, tant pour les organisations que pour les individus. Pour les entreprises mais aussi les collectivités publiques, les enjeux sont majeurs et elles doivent protéger leur patrimoine informationnel. Les individus doivent protéger leurs données qui sont majoritairement liées à leurs données personnelles.

En termes de sécurité, de manière très binaire, les risques et les menaces sont de deux ordres : des risques internes à l'organisation et des risques externes. On peut dresser un inventaire desdits risques en participant

à des travaux sur le *Security Information and Event Management (SIEM)*, de l'analyse quantitative des incidents. Par exemple, au club R2GS (Club de réflexion et de recherche en gestion opérationnelle de la sécurité) ou autres, on a identifié **74 indicateurs de risque** sur lesquels la menace porte. Et l'on fait des travaux de normalisation à l'*ETSI*, auxquels les Américains participent. En pratique, on se rend compte que les grands comptes bancaires nationaux, les opérateurs nationaux, prennent en considération les 74 et ils disent : maintenant je vais regarder d'un point de vue quantitatif, en termes de récurrence, d'occurrence et de dommage, sur quoi je vais porter mes efforts. En règle générale, ils ne retiennent pas tous les indicateurs, ils n'en gardent qu'entre 18 et 24, parce qu'on concentre la ressource sur ceux-là. Et ça suffit puisque les autres sont epsiloniques ou très réduits. Il n'empêche que si on voulait couvrir tout le spectre, on devrait tendre vers les 74 indicateurs.

Ces travaux nous montrent que les risques sont internes et externes. **Le premier des risques, c'est l'homme.** Dans un État démocratique, l'homme a des droits et des libertés.

Je n'aborderai pas la question des données personnelles, même si la grande révolution, avec la proposition de règlement communautaire, c'est que la sécurité porte également sur la donnée à caractère personnel puisque les deux s'interpénètrent. Le RSSI doit travailler avec le délégué à la protection des données. Abandonnons ce terme de correspondant informatique et libertés (CIL), qui n'est qu'un terme commercial utilisé par la CNIL et qui ne figure ni dans la loi ni dans les propositions de règlement. En tout cas, le RSSI et le délégué à la protection des données doivent travailler plus que jamais ensemble car la donnée est essentielle. Qu'elle soit personnelle ou pas, on doit la protéger. De toutes manières, en protégeant le système, on protège aussi le contenu puisque c'est lui qui va être affecté.

Ce risque humain se traduit par des menaces concrètes. Je commente régulièrement la jurisprudence de droit pénal en matière de cybersécurité, d'attaques informatiques, à savoir celles concernant les articles 323-1 et suivants du code pénal, pour aller vite. Quand on regarde cette jurisprudence, on est terriblement déçu. Je ne parle même pas des articles 226-16 et suivants en matière de protection des données à caractère personnel. Les textes existent, les sanctions sont là : deux ans, cinq ans d'emprisonnement, 30 000 €, 75 000 €, 300 000 € d'amende…

Examinons la jurisprudence. De modestes sanctions, voire quelques amendes à peine et quelques sursis. Rappelez-vous cette affaire *Valeo*, un industriel qu'il fallait peut-être protéger ou **Mlle Li li Whuang** qui a fait un mois de détention préventive et qui a été condamnée à un an avec sursis.

Elle avait pénétré dans une entreprise comme stagiaire, détourné des quantités de données, peut-être stratégiques, qui ne concernaient pas son sujet de travail et de recherche : plan d'assurance qualité, organisation

marketing, alors qu'elle faisait de l'analyse sur les tensioactifs en matière de résistance des matériaux. Rien à voir avec le marketing et la qualité. Il existe donc un arsenal en droit pénal, la police fait son travail, on poursuit et, en fin de compte, quelle déception !

Le citoyen que je suis, l'avocat que je suis, défenseur des « cibles », puisque je ne défends pas les attaquants – je suis en défense pour les entreprises ou les administrations qui se font attaquer –, est profondément choqué. **L'arsenal répressif existe, appliquons-le.** C'est un point d'attention très important, la prise de conscience. Malheureusement, tous les procureurs de la République ne sont pas comme Mme Myriam Quéméner. J'en vois un et il me dit à propos du numérique : « *Mon cher ami, n'a-t-on pas suffisamment à faire dans nos rues ? Il n'y a pas de sang qui coule.* » Mais le critère est bien curieux. Faut-il que le sang coule pour que justice soit faite ? Le numérique, c'est très volatil. Pour autant, compte tenu des enjeux pour chacun d'entre nous, les tribunaux devraient appliquer le quantum des peines avec des délits qui existent.

Un autre élément est important : certains délits ne sont pas encore qualifiés. L'affaire Bluetouff (5 février 2014 - Cour d'appel de Paris) avait pour objet une attaque contre l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (ANSES), une agence OIV, mais non assujettie à des règles et donc vulnérable en termes de sécurité. Mais ce n'est pas le problème. En revanche, ce qu'on a lu dans la presse et sur le Net est choquant. On nous a dit : « *Qui sont nos juges et de quel droit nous jugent-ils ? Ils n'emploient même pas le bon jargon. Ils disent des âneries, ne comprennent rien, parlent de "glogue, de bogue"… On s'est moqué d'eux ! De quel droit jugent-ils ?* » Ils jugent au nom de la Nation. Il y a des textes à appliquer, les juges assurent leurs fonctions de juge et ils punissent modestement par une petite amende. Et maintenant cette affaire va aller devant la Cour de cassation.

Je plaide pour que le vol soit reconnu, non pas le vol soustraction, mais ce qu'on appelle en droit le « vol reproduction ». C'est une vieille distinction que j'ai commentée en doctrine. Elle fait suite à la loi Godfrain de 1988 relative à la fraude informatique. Dans le numérique, on reproduit de la donnée. Évidemment, on ne l'a pas soustraite. On peut l'altérer, la détruire, on peut bloquer le système. Mais, la plupart du temps, on va la télécharger, la dupliquer. De petites notions, de petites évolutions permettent aussi de contribuer à prévenir le risque numérique, comme le vol reproduction par voie de téléchargement ou de reproduction.

En matière de sécurité, il faut aussi faire une grande distinction entre, d'une part, les grandes entreprises et les administrations et, d'autre part, les TPE, les PME, les PMI et les petites collectivités locales qui sont la majorité de nos communes. Dans mon village de 1 000 habitants, la secrétaire de mairie doit tout faire. La commune n'a pas les moyens d'avoir un directeur informatique.

En ce qui concerne les premiers, les grandes entreprises et les administrations, ils ont des moyens à peu près corrects en termes humains et financiers pour lutter contre ces risques. Les seconds n'en ont pas.

Ne parlons pas des individus ou des entreprises quand ils font surtout confiance à des entreprises américaines. On ne reviendra pas sur certaines affaires récentes, notamment devant la Cour fédérale de New York qui a condamné *Microsoft* à transférer des données hébergées en Irlande – c'est en Europe, me semble-t-il – aux services new-yorkais qui les lui demandaient. C'est une manifestation non pas du *Patriot Act* mais de nombreuses législations qui permettent d'avoir accès à ces données.

Alors quelle est la parade ? Au niveau des OIV et des administrations, Mme la ministre a évoqué la loi de programmation militaire. On attend le décret d'application avec impatience. L'article 22 m'intéresse, en rapport avec l'ANSSI. À quelle sauce seront-ils mangés ?

Mais il existe aussi des avancées, notamment par rapport à la prise de conscience par les dirigeants d'entreprises et par les dirigeants de PME. Dans les grandes entreprises, on va avoir la notification des failles et bientôt d'autres notifications en matière de prestataires de services de confiance électroniques. Le règlement *eIDAS* devrait être publié au cours de l'été[1]. Tous ceux qui émettent des certificats de signature, des certificats de serveur, des jetons d'horodatage et tous ces éléments liés à des moyens cryptographiques, seront assujettis. Il y aura des notifications de violation de données personnelles pour les opérateurs. Il y aura des notifications bientôt, dans le futur règlement, en tout cas si l'on arrive au bout, grâce aux Américains. On oublie souvent **l'action des groupes de pression à Bruxelles qui est le fait de groupes d'influences hautement partisans qui ne nous veulent que du bien** ! Souvent ils contrecarrent toutes les avancées de nos gouvernements et autres.

Alors, nous disposons de la mise en place de normes *ISO* 27001 et suivantes, de la prise de conscience des directions générales, de la détection et du contrôle par l'ANSSI avec la loi de programmation militaire, des chartes informatiques, de la sensibilisation des personnels. Mais les entreprises n'ont pas tout cela. Éventuellement, elles ont la charte. Il faut leur **proposer des chartes types et peu coûteuses** parce qu'elles n'ont pas les moyens de payer pour avoir un vrai service. De plus, une entreprise entre vingt et cent cinquante salariés n'a pas la complexité d'une grande entreprise. En tout cas, il faut sensibiliser les entreprises à la sécurité numérique et les inciter fortement à notifier les violations de données à caractère personnel.

Quelles évolutions doit-on attendre ? D'abord on peut faire évoluer quelques notions comme le vol, j'en ai parlé. La directive sur les attaques

[1] *Il l'a été le 28 août 2014.*

informatiques, adoptée récemment, comportait une notion très intéressante à l'origine qui revenait à dire la chose suivante : « *Vous pouvez dire, vous législateur qui transposez, que l'entreprise n'est pas protégée si elle n'a pas mis en place de la sécurité.* » En d'autres termes, si elle agit sur le plan pénal, il n'y aura pas de sanction. Allons encore plus loin, autant lui dire : « *Vous n'êtes pas protégée parce que vous ne vous êtes pas protégée. Alors l'État ne vous protègera pas.* » C'est ce que dit le juge : « *Si vous ne vous êtes pas protégé, vous avez dit* open bar*, et tant pis pour vous. Relaxe* » (affaire *Tati* versus *Kitetoa*). Et c'est ce qu'on voudrait nous faire croire sur l'affaire Bluetouff. Or, dans Bluetouff, il ne s'agit pas seulement de l'introduction dans un système informatique. Il y a eu relaxe sur l'introduction. *Open bar*. On rentre, mais on n'est pas poursuivi en raison de ce chef. En revanche, il y a eu maintien dans le système et vol. Donc il faut bien regarder la qualification. Les juristes savent que la qualification est essentielle.

Derrière cela, il y a peut-être la nécessité pour les services de police ou Europol de **renforcer la coopération internationale**, compte tenu de l'internationalisation.

Il faut sans doute aussi renforcer la protection des données à caractère personnel mais sans aller trop loin. **Le but n'est pas d'handicaper nos entreprises pour qu'elles ne soient plus compétitives.** Avec trois boulets, elles ne vendront plus les produits où l'on est *leader* mondial. En biométrie, les Français sont en tête dans le monde. Nous équipons la Maison Blanche, le Pentagone, l'aéroport de Tel Aviv, l'Afrique du Sud… On équipe toute la planète et en France, ses détracteurs assènent : « *la biométrie, quel crime attentatoire aux droits de l'homme !* » Les droits de l'homme ont bon dos. Et puis s'il y a des avancées, comme M. Philippe Wolf nous l'a dit, qui permettent de garantir des bases de données en empêchant l'extraction, alors peut-être que, grâce à la technologie, nous avancerons vers des points sur lesquels notre pays est fort.

Enfin, il faut veiller à la formation des magistrats, à leur sensibilisation, qu'ils aillent au fond des choses et qu'ils punissent à leur juste mesure les crimes, les délits et les actes qui sont répréhensibles. De fait, à côté des actes les plus répréhensibles, il faut aussi réprimer les atteintes aux biens, les atteintes aux personnes, qui peuvent résulter de la e-réputation, des données, des vols de numéros de cartes, ou autres, en tout cas qui causent de graves préjudices aux individus, aux entreprises et aux collectivités publiques.

M. Pierre Lasbordes. – Maître Pierre Desmarais, je crois que vous êtes acteur dans l'*open data* et vous allez nous parler de quelques vulnérabilités du numérique dans ce domaine.

Me Pierre Desmarais, avocat à la Cour d'appel de Paris, correspondant informatique et libertés, spécialisé dans les questions de sécurité numérique. – Je vais vous parler de la sécurité dans l'*open data*, principalement dans le

domaine de la santé. Mon confrère disait qu'il n'y a pas de sang dans le numérique, mais en santé, il peut y avoir du sang, un vrai risque vital. On l'a vu dans des hôpitaux publics pour des problématiques de dossier médical et d'aide à la prescription, où le mauvais interfaçage d'un logiciel a abouti au décès d'une patiente.

On pourrait le voir demain avec **l'absence totale de sécurité logique au niveau des dispositifs médicaux communicants qui peuvent être piratés à 90 mètres**. Avec de tels dispositifs, on peut envoyer une décharge électrique de 830 volts dans un *pacemaker*. Donc **le risque numérique peut sans difficulté se transposer dans la vie réelle, notamment dans le domaine de la santé**.

Particulièrement avec le *big data*, on va devoir veiller à la sécurité des données à caractère personnel en respectant la confidentialité des données et en s'assurant que tout ce qui va être dit dans le traitement d'*open data* ne va pas permettre de réidentifier une personne physique, nommément ou non. Et, derrière, il va falloir s'assurer qu'on ne va pas pouvoir discriminer cette personne physique pour accéder à l'assurance ou à un autre droit.

Il faut également s'assurer que l'ensemble des droits de la personne soit respecté. Depuis une semaine, la presse parle du moteur de recherche *shodanhq.com* qui a vocation à référencer tous les objets connectés à Internet et de permettre l'accès à ces dispositifs en utilisant les *logins* et mots de passe de la configuration. À l'issue, **vous accédez aux caméras qui sont installées dans le domicile de monsieur tout le monde ou éventuellement dans des entreprises ou des administrations publiques**.

Quelles sont les conséquences de ces failles ? La première est civile, à travers la responsabilité civile ou la responsabilité administrative si c'est une personne publique. Une personne qui subirait un préjudice, une atteinte à sa vie privée, pourrait ainsi déposer plainte au pénal mais aussi au civil où elle pourrait obtenir des dommages et intérêts, sur le fondement de l'article 9 du code civil – « *Chacun a droit au respect de sa vie privée.* » –, et ce serait relativement simple, étant donné qu'en la matière on n'a pas besoin de préjudice. Il suffit de prouver une faute et un lien de causalité. La faute serait facile à démontrer étant donné que l'opérateur, le responsable de traitement, a une obligation de sécurité et de moyens renforcés. C'est à lui de prouver qu'il a tout mis en œuvre pour qu'il n'y ait pas de divulgation des données.

Une autre hypothèse permettrait d'envisager une action en responsabilité civile délictuelle ou contractuelle. Le contractuel pourrait très bien être retenu dans le cadre du règlement *SEPA*. En effet, si une personne est victime d'une fraude, alors qu'elle n'a pas été mise à même de pouvoir s'opposer à des listes noires ou blanches de prélèvements, elle subit un préjudice et elle peut demander effectivement cette réparation.

Le premier problème avec l'*open data*, c'est qu'il touche les données personnelles mais également tout ce qui est information stratégique pour l'entreprise. Madame le bâtonnier, vous en parliez ce matin, notamment avec les appels d'offres qui constituent des mines d'or. **On y recueille un tas de données qui permettent ensuite d'attaquer une entreprise publique ou une administration. Si l'on ajoute le fait qu'à la fin de la procédure d'appel d'offres, on sait très précisément quel système a été acheté**, alors c'est la voie royale pour un attaquant qui sait, en plus, les mesures de sécurité qui ont été mises en œuvre. En effet, tout figure dans les avis de marché.

Le deuxième problème en matière d'*open data*, c'est la divulgation de données stratégiques. Actuellement, l'*open data* concerne exclusivement les entités du secteur public, État, collectivités, établissements publics et personnes privées qui assurent une mission de service public. Mais toutes ces personnes collectent également des données qui concernent des entreprises et qui ont une valeur stratégique. Comment les protéger ? Face à, éventuellement, une concurrence déloyale, du parasitisme à l'encontre de l'entreprise qui perd ses données stratégiques du fait d'un concurrent qui récupère les données et les réutilise, on peut envisager une action en responsabilité contre la personne qui a divulgué les données. Celle-ci va se retrouver dans une situation délicate parce qu'elle était obligée de les publier, et donc, en fin de compte, ce sera probablement l'État qui sera désigné comme le responsable au niveau civil.

Quelles sont les solutions ? Elles sont de deux ordres. Elles se situent au niveau des données à caractère personnel et du contrat.

Concernant les données à caractère personnel, le correspondant informatique et libertés (CIL), même si ce titre est un peu décrié, va s'assurer, en amont du traitement et de l'ouverture des données, qu'aucune atteinte ne sera faite à la confidentialité de la donnée. On ne pourra pas remonter à une personne physique à partir des données ouvertes.

La deuxième solution est le *privacy by design*. Quand on lance de l'*open data*, dès le début, il doit s'agir de systèmes producteurs de données respectueux des droits de chaque personne. De sorte, on sera sûr de ne pas trouver des données très sensibles sur la santé ou le numéro de sécurité sociale qui tout d'un coup se retrouveraient sur Internet par le biais de l'*open data*.

L'adoption d'une charte informatique et d'une politique de sécurité du système d'information sont un impératif.

Enfin, au niveau des données stratégiques, pour ce qui concerne les personnes publiques, notamment pour les opérateurs d'importance vitale, il existe **une solution : ce sont des marchés sans publicité et sans mise en concurrence préalable quand il s'agit d'acquérir le système d'information et les mesures de sécurité**. Le respect du droit de la commande publique est une

chose, mais si l'on respecte la publicité, c'est la sécurité du système d'information lui-même qui est remis en cause.

Dès lors que des données sensibles sont mises à disposition, l'*open data* doit être systématiquement encadré par un contrat. Ce contrat doit notamment écarter l'application du droit américain, déjà en déclarant que c'est une législation de l'Union européenne qui va s'appliquer, et, ensuite, en faisant **application de la Convention de La Haye, qui permet de rejeter tout le système probatoire américain**. Cela évite toutes les procédures de *Discovery* qui permettent aux Etats-Unis de rapatrier chez eux toutes les données françaises.

Enfin, **il faut changer de vision, en passant d'une vision de risque juridique à une vision de *compliance*, dans laquelle les opérateurs se chargent de respecter la législation**, de vérifier qu'ils y sont conformes, plutôt que d'apprécier un risque juridique et de se dire : « *Ici je suis dans une zone grise, je peux tenter d'y aller mais je n'irai pas dans la zone noire*. » Avec la *compliance*, on est censé rester dans la zone blanche et donc être respectueux des droits des personnes.

M. Pierre Lasbordes. – Madame Valérie Maldonado, vous êtes commissaire divisionnaire et vous êtes à la tête d'un service très important que les entreprises sont amenées à venir consulter lorsqu'elles ont connu un incident grave. Vous êtes donc sans doute l'organisme d'État qui est le plus à même de parler des risques rencontrés par les entreprises. Vous avez une quinzaine de minutes pour illustrer ces propos et nous donner quelques exemples concrets dus au risque numérique.

Mme Valérie Maldonado, chef de service, Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC). – Je vais d'abord vous brosser le contexte général dans lequel cet Office central, qui est rattaché à la direction centrale de la police judiciaire, a évolué très récemment. L'OCLCTIC est consacré à la problématique liée à la cybercriminalité avec un champ d'application d'infraction pris au sens large : les infractions purement cyber, principalement les atteintes au Système de traitement automatisé des données (STAD) et l'utilisation des nouvelles technologies qui vont faciliter la commission d'infractions plus larges qui existaient déjà, je pense en particulier aux escroqueries sur Internet, à la fraude aux cartes bancaires et autres.

En mai 2009, a été mise en place la plate-forme *PHAROS* de traitement des contenus illicites du *Net*. Ce site gouvernemental permet à l'internaute de signaler un contenu manifestement illicite (raciste, violent, homophobe, apologie du terrorisme, etc.).

Dernièrement, le 29 avril 2014, cet office central a été intégré au sein d'une sous-direction à part entière, la sous-direction de la lutte contre la cybercriminalité, ce qui donne une idée de l'importance donnée à

l'augmentation des moyens pour lutter contre ce phénomène extrêmement important.

En France, cette sous-direction doit être un acteur fort, à la fois en matière préventive et répressive, dans l'application de la loi pénale, puisque c'est notre métier. Nous devons pouvoir répondre de manière efficace aux commandes de deux structures : Europol, avec le Centre européen de lutte contre la cybercriminalité (*EC3*) qui est le complexe européen en matière de lutte contre la cybercriminalité, et Interpol qui va inaugurer, en septembre prochain, son complexe mondial en matière de lutte contre la cybercriminalité.

Les deux objectifs qui ont conduit à la création de cette sous-direction rejoignent le propos d'aujourd'hui. D'une part, il s'agit de prendre en compte l'importance de l'utilisation de l'Internet et des réseaux sociaux dans la commission d'un certain nombre d'infractions. D'autre part, au sein de la division d'anticipation et de l'analyse, nous prenons en compte la problématique des risques qui sont subis dans les atteintes des systèmes numériques liés aux PME. **Nous intervenons donc plutôt sur le spectre des PME, et de temps en temps, en fonction de la décision du magistrat et des cas de figure, sur certains opérateurs d'importance vitale.** Mais nous ne sommes pas compétents en matière de traitement judiciaire des attaques qui sont portées contre les opérateurs d'importance vitale. Celui-ci revient à l'ANSSI ainsi qu'à la DGSI à travers le traitement des dossiers au pénal.

Je vais faire un focus sur notre champ de compétences et ce que l'on fait précisément. Concernant les entreprises, les risques qu'elles encourent sont liés à la fois à des considérations internes liées à l'entreprise et à des attaques externes.

Schématiquement, en pratique, nous voyons des atteintes au STAD purement informatiques, liées à des exploitations de failles de sécurité, avec une pénétration dans les systèmes informatiques et des finalités qui peuvent être différentes et qui revêtent des qualifications pénales.

Cette finalité de l'attaque peut être : d'obtenir une défiguration du site, de pirater (par exemple, les fichiers clients d'une entreprise), d'opérer des chantages (ce qui se voit beaucoup en ce moment), des attaques *DDoS* en déni de service distribué (c'est-à-dire une saturation du serveur ciblé qui cesse de fonctionner sous un trop grand nombre de demandes et de requêtes). Plus récemment, on a vu l'utilisation de rançons logicielles. Ces attaques informatiques prennent en otage les données qui sont dans les ordinateurs, en particulier les documents.

On baptise souvent ces *malwares. CryptoLocker* par exemple, lorsqu'il s'est introduit dans le système visé, va crypter les données et dans un délai de 72 heures, il va exercer un chantage sur l'entreprise ou sur le particulier qui aurait été ciblé et infecté, ce qui l'obligera à payer une somme d'argent (en monnaie virtuelle la plupart du temps), en échange de quoi il va

récupérer une clé de décryptage qui devrait lui permettre de récupérer ses données. Pour les entreprises, ces données sont définitivement perdues parce que les puissances de calcul utilisées ne nous permettent pas, à nous, d'obtenir des solutions de décryptage en temps et en heure. Vous voyez que les menaces sont extrêmement importantes.

Il ne faut pas oublier les menaces qui viennent de l'intérieur même de l'entreprise. Nous voyons certains employés qui n'appliquent pas les chartes de sécurité informatique mais aussi des salariés ou des cadres malveillants, détenteurs d'un certain nombre d'informations, et qui vont pouvoir opérer des chantages de manière assez élaborée parce que la plupart du temps, ils maîtrisent l'élément informatique.

Pour le coup, particulièrement dans les affaires de chantage, **les enquêtes nécessitent une coopération de tous les instants avec la société, son dirigeant et son avocat**. Nous allons voir sur place comment nous allons construire ce lien avec le pirate, comment engager les négociations et faire en sorte d'acquérir assez rapidement tous les moyens d'acquisition de la preuve qui sont nos fondamentaux. Sans ces éléments probatoires-là, le travail sera complètement inefficace et sans résultat en termes d'identification ou de coopération internationale pour articuler les investigations qui peuvent être nécessaires. Parfois, on se rend compte que le pirate est à l'étranger ou qu'il opère avec des complices qui sont eux-mêmes basés à l'étranger.

En matière de cybercriminalité, les enquêtes pénales sont donc assez complexes, dans la mesure où l'on a une problématique technique pure mais aussi une problématique de **mise en œuvre de la coopération internationale** qui n'est pas évidente, d'autant que nos délais sont extrêmement contraints. Nous pouvons encore faire des progrès dans ce domaine.

Nous avons également affaire à des données liées au cryptage ou à toutes les techniques d'anonymisation. Ces outils de sécurisation de la sauvegarde peuvent présenter des difficultés supplémentaires pour les enquêteurs en charge d'aller rechercher les preuves qui vont permettre l'identification des auteurs.

Nous avons une problématique de lieu et de temps. Nous ne restons jamais en France puisque dès le début de l'enquête, nous nous dirigeons vers l'international et la coopération. Il faut aller vite. La conservation des données est pour nous, enquêteurs, un élément fondamental. À partir du moment où vous ne disposez pas des *logs* de connexions ou des données conservées, c'est autant de constatations qui deviennent à un moment donné impossibles à faire. C'est une difficulté à laquelle on peut être confronté dans le cas d'un pays à qui on demande la coopération mais qui ne pratique pas la conservation des données.

Pour arriver à des interpellations et à des résultats probants, il faut avant tout disposer de policiers. Ceux-ci doivent être formés aux techniques

informatiques mais ils restent des policiers rompus aux techniques de l'enquête judiciaire. C'est extrêmement important.

Il nous faut également des moyens spécifiques d'actions qui sont davantage liés, à mon sens, aux moyens de la procédure pénale qu'aux infractions pénales elles-mêmes qui existent déjà. On peut considérer que les infractions pénales cyber, telles qu'elles sont prévues, sont assez importantes. En revanche, au niveau des moyens procéduraux, nous serions très satisfaits d'obtenir deux éléments. Le premier, c'est l'élargissement des infractions nécessitant l'utilisation d'enquêtes sous pseudonyme. N'importe quelle personne peut ouvrir un compte *mail* sous un pseudo, ce qui est plutôt la règle et l'usage. Pour un service de police d'investigation, on peut imaginer l'importance qu'il y a à **pouvoir enquêter en ligne sous pseudonyme**. Cela doit se faire de manière encadrée, tel que c'est déjà prévu pour un certain nombre d'infractions. Mais **ce droit n'existe pas actuellement pour les atteintes au STAD et c'est dommageable** car ce sont les infractions les plus graves, et c'est le cœur de métier de la cybercriminalité. Les enquêtes sous pseudo nous permettent d'obtenir, la plupart du temps, à la fois des moyens probatoires par les échanges qu'on arrive à mettre en place et des identifications d'auteurs qui ne sont pas possibles par d'autres moyens.

Vous pouvez imaginer les précautions que prennent les pirates en matière d'anonymisation, d'utilisation des réseaux *Tor*. Il est beaucoup question du *darknet*. C'est là où les plus gros trafics se font. Pour discuter sur ces forums, il faut être coopté. Les services de police d'investigation ont besoin d'être outillés *a minima* pour pouvoir aller sur ces forums et discuter sans se faire identifier et être mis de côté.

Le deuxième moyen que nous souhaitons obtenir, c'est la captation des données à distance. Ce moyen est déjà prévu par la loi mais il doit être encore mis en application. C'est un sujet important puisque c'est **la capacité d'utiliser des logiciels espions** dans des conditions juridiques évidemment extrêmement encadrées mais qui restent des fondamentaux pour nous. En matière de lutte contre le terrorisme et autres, les services sont très attentifs aux progrès et à la mise en œuvre de ces processus déjà mis en place par de nombreux pays européens. La France devrait y arriver, c'est en bonne voie. **Souvent, c'est le seul moyen efficace pour contourner les moyens de cryptographie** utilisés dans le cadre d'échanges de données à travers des logiciels de communication parfaitement cryptés et anonymisés. Les enjeux se situent aussi à ce niveau-là.

M. Pierre Lasbordes. – Monsieur Benoît Virole, vous qui avez observé et analysé la psychologie des enfants et des jeunes face au numérique et au jeu vidéo, vous pouvez apprécier l'impact du numérique sur eux. Peut-être allez-vous nous apporter quelques remèdes et quelques solutions ?

M. Benoît Virole, docteur en psychopathologie, docteur en sciences du langage, membre de l'Observatoire des mondes numériques en sciences humaines (OMNSH). –Je vais prendre la parole en tant que psychologue d'enfants et d'adolescents, ayant une pratique et un lieu d'observation de l'impact du numérique sur le développement psychologique des enfants et des adolescents.

Oui, le numérique est un espace de risque important. Il y a une mise en insécurité chez nos jeunes quand ils sont confrontés aux espaces numériques. Cela ne veut pas dire que tout le monde numérique est négatif. Le numérique est une chance incroyable, il offre à la jeunesse des possibilités de connaissance, de prise d'action sur le monde et de développement de la créativité qui sont remarquables. Mais il est aussi associé à un risque majeur. Pour le comprendre, il faut avoir à l'idée un concept clé de la cyberpsychologie : le concept d'immersion.

Quand on s'immerge dans un monde virtuel, dans un monde numérique, se produisent dans l'esprit d'un sujet des mécanismes tout à fait orignaux et spécifiques, qui ne sont pas réductibles à ce qui se passe quand on joue à un jeu avec des petites figurines, quand on lit un livre ou quand on regarde un film. **Avec le numérique, on est acteur d'une action virtuelle.** Cela pose le sujet dans une position de responsabilité tout à fait particulière puisqu'il accomplit à la fois une action réelle et une action qui se situe dans un monde virtuel. Il y a donc **une sorte d'irresponsabilisation de l'acte** qui fait qu'il est dans un entre-deux, un espace transitionnel particulier.

Cet espace transitionnel peut avoir des effets intéressants. Les mondes virtuels sont, par exemple, utilisés pour soigner un certain nombre de jeunes qui ont des difficultés. Mais cet espace présente aussi des difficultés et des risques. J'ai identifié cinq risques.

Le premier risque est celui de la séduction traumatique. Aujourd'hui, **tout enfant ou tout jeune qui utilise une plate-forme numérique est à un ou deux clics d'une image pornographique ou d'une extrême violence**. Si on laisse un enfant utiliser librement des interfaces numériques, il y a un risque fort d'exposition à des scènes séductrices, des scènes sexuelles ou de violence qui vont générer un désir de voir, et ce désir est particulièrement pervers quand il y a une séduction traumatique, c'est la « compulsion de répétition », bien connu en psychologie de l'enfance, c'est-à-dire le désir d'aller rechercher à nouveau une image de ce type-là.

Je lance un appel à la régulation du marché. Il est assez anormal que lorsqu'un enfant utilise une tablette numérique du marché, *Android* ou *Apple*, et qu'il va chercher des applications de jeu, il se trouve immédiatement confronté à des applications de jeu à caractère sexuel ou de violence.

Une régulation a été mise en place, à travers une signalétique qui a d'ailleurs été discutée dernièrement au Parlement. Malheureusement, cette signalétique est le fruit d'une concertation entre les éditeurs du marché qui

se sont mis d'accord entre eux pour promouvoir une signalétique d'avertissement par classe d'âge. Elle est plus ou moins bien respectée. Les parents jettent un coup d'œil de temps en temps sans vraiment regarder. Les vendeurs de ces jeux vidéo ne prennent pas garde à qui les achète. Cette signalétique est donc purement symbolique, elle n'a pas vraiment d'efficacité. Son efficacité est d'ailleurs perverse, dans la mesure où les enfants ont envie de jouer à des jeux qui sont justement déconseillés pour leur classe d'âge. Je me demande s'il n'y a pas une mise en retrait de la part de la puissance publique par rapport à ces jeux.

Par exemple, le jeu *GTA* est remarquable sur les plans graphique et de sa construction mais il est parfaitement pervers sur le plan des valeurs. Le héros de ce jeu est un malfrat et son but est de tuer l'officier de police qui tente de l'arrêter. Ce jeu est intrinsèquement pervers. Certes, il est déconseillé aux moins de dix-huit ans mais beaucoup d'enfants y jouent.

Le deuxième risque est celui des conduites addictives. Il y a un grand débat entre les psychologues et les psychiatres sur le fait de savoir si c'est vraiment une addiction. Si c'est une addiction, il faut identifier un toxique. Or, c'est un produit du marché et l'on ne sait pas si on peut le classer sous le terme d'addiction. On utilise des mots plus faibles comme « pratiques intensives » : **5 % de la classe d'âge des quinze à dix-sept ans jouent de façon pathologique à des jeux vidéo** qui sont construits pour entraîner une forme de toxique, puisqu'ils fonctionnent dans des mondes persistants qui, par définition, ne s'arrêtent pas. Quand on se déconnecte, les autres joueurs continuent à jouer et donc on est poussé à continuer à jouer. Aujourd'hui, de jeunes adolescents, déscolarisés, plutôt des garçons, restent des nuits entières à jouer dans ces mondes persistants. Cela pose des **problèmes de santé publique** qui commencent à être vraiment émergents et qui inquiètent, à juste titre, les familles et les professionnels.

Le troisième risque est celui de la subversion des institutions cadres. La famille d'abord, dans la mesure où l'utilisation des jeux vidéo, des réseaux sociaux, des communications numériques, créent des néo-groupes entre jeunes, dans lesquels **la notion de régulation par la famille n'existe plus**. Il y a une forme de mise en retrait de l'institution familiale avec souvent la complicité implicite des familles qui confient à des systèmes automatiques la régulation de l'utilisation d'Internet. En confiant à des systèmes automatiques la régulation des affichages de contenu, il y aura un affaiblissement de la responsabilisation parentale. **Être parent ne s'arrête pas au seuil du numérique.** Un parent contemporain doit être parent y compris à l'intérieur des mondes numériques. Du fait des problèmes générationnels mais aussi des problèmes de société, beaucoup de parents n'exercent pas leur fonction parentale à l'intérieur du numérique.

La deuxième subversion est celle de l'école. C'est une subversion des institutions qui ont le monopole du savoir. Un jeune va penser que ce qu'il apprend à l'école ne pèse pas très lourd par rapport à ce qu'il peut

apprendre sur le *web*. Avec un moteur de recherche, il peut avoir accès à l'ensemble des connaissances, disponibles sur son s*martphone* à tout moment. « *À quoi ça sert d'apprendre les dates de l'histoire ou les contenus de connaissance qu'on m'apprend à l'école, au collège, au lycée, à l'université, en me forçant à rester assis alors que je les ai constamment présents sur mon* smartphone ? » Il y a une **sorte de délégitimisation des institutions qui ont le monopole de la délivrance du savoir**. Ces institutions sont remises en question par le développement du numérique. Une forme d'insécurité se crée. Beaucoup de jeunes sont déscolarisés aujourd'hui parce qu'ils n'accordent plus de crédit à l'école. Ils attribuent du crédit au *web* comme étant le vecteur premier de la connaissance.

Le quatrième risque est celui de la manipulation idéologique. Les jeunes qui regardent des vidéos sur *YouTube* sont confrontés en permanence à des discours qui peuvent être des discours de manipulation sur le plan politique et idéologique, ce qui amène à une mise en questionnement des savoirs institués. Un enseignant, ou un parent, peut dire que ceci est la vérité mais le jeune dira que c'est faux parce qu'il a vu le contraire dans une vidéo sur *YouTube*. Il y a un risque fort que le message républicain, par exemple, qui peut être délivré par l'école, le collège ou le lycée, se voit confronté à d'autres types de discours véhiculés par le *web*, *YouTube* ou les réseaux sociaux. Nos jeunes sont mis en danger parce qu'ils sont exposés à des discours clairement manipulateurs.

Le cinquième risque est celui de la confusion des valeurs. On peut se demander si les psychologues peuvent se mêler de ces valeurs. La réponse est oui. Les psychologues doivent se questionner sur les valeurs car c'est ce qui permet à un sujet de choisir une route lorsqu'il est à un carrefour de son existence. Dans nos vies, nous sommes constamment confrontés à des choix d'existence. À un moment donné, il faut choisir une route et ce choix est fait au nom de valeurs. C'est pourquoi **la transmission de valeurs est fondamentale. Des jeunes qui seraient exposés à une confusion ou à une dégradation permanente des valeurs seraient des jeunes mis en danger et en insécurité.**

Je prendrais l'exemple de **la dégradation de la valeur de l'amitié dans les réseaux sociaux. Non, les contacts ne sont pas des « amis ».** La comptabilisation du nombre d'amis sur *Facebook* ne donne pas une idée réelle d'une vie sociale réussie. Il y a dans l'utilisation des réseaux sociaux une dégradation complète des valeurs qui va jusqu'à la réification. Tout contact humain est ramené à une quantification mesurable et à un objet marchand. Selon la réification, au stade ultime du capitalisme, **la relation humaine va devenir un objet de marché**. D'une certaine façon, on y a est arrivé, avec le déploiement des réseaux sociaux.

Certes, c'est une vision apocalyptique qui ne circonscrit pas ma vision du numérique. Je pense aussi que c'est une grande chance. Et je partage l'opinion de M. Bernard Stiegler sur le fait que nous avons les

moyens d'accomplir de grandes choses grâce au numérique, y compris dans l'éducation de nos enfants.

En conclusion, je lancerais d'abord plutôt un appel à la présence de la République dans le numérique. En utilisant cette métaphore qui a fait un peu de bruit, on pourrait presque dire que **le numérique est un territoire perdu de la République française aujourd'hui**. Quand les jeunes passent du temps dans les jeux vidéo et dans les mondes virtuels, la République n'est pas présente. **Le marché américain et les éditeurs américains sont présents mais la République française ne l'est pas.**

Par ailleurs, se pose une question d'éducation. **L'éducation au numérique est une nécessité. Il faut éduquer à la critique du numérique.** Pour savoir utiliser les informations, il faut avoir une vision critique sur les informations qui sont données par le *web*.

Je pense aussi qu'il y aurait quelque chose à faire en direction des parents pour les **aider à être parents, y compris à l'intérieur de la culture numérique**.

Conclusion

Mme Anne-Yvonne Le Dain. – Depuis ce matin, j'ai mesuré pleinement l'ampleur des inquiétudes et des opportunités liées au numérique. Chacun, en vos grades et qualités, vous avez abordé des éléments très concrets qui pourraient être des facteurs d'évolution du droit ou des pratiques. Le sénateur Bruno Sido et moi-même avons bien entendu vos analyses et propositions. Nous en tiendrons compte.

Ce qui m'étonne, c'est ce mélange d'une sorte d'inquiétude qui est latente, face à notre monde compliqué et sur laquelle on a le sentiment qu'on pourrait tout de même agir. On ne sait pas très bien dans quel but ni vraiment comment et l'on n'est pas très sûr d'avoir quand même envie d'y aller.

Ce décalage me perturbe. Il n'est pas spécialement propre à la dernière intervention même si je vous remercie d'avoir également replacé les enfants dans ce système. En effet, les enfants sont une cible formidable que les grandes entreprises commerciales, américaines ou pas, ont visée très tôt et avec lesquels on est effectivement dans une réification du monde.

Mais au bout du compte, le monde numérique est là. On ne pourra pas l'empêcher d'être. Vouloir y agir d'une manière plus ferme, plus forte, uniquement sur le mode de la contre-attaque, avec des solutions juridiques, pour gérer les débordements, les difficultés, les attaques, les crimes, l'immoralité, le risque de recul de l'éducation, c'est une approche par le refus. Est-il envisageable de trouver une voie permettant une approche par l'action ?

Je manifeste un grand désarroi. Vous avez chacun votre angle de vue face aux risques et aux possibilités, sur ce qu'il faudrait faire pour un certain nombre de choses concrètes, la loi, la police, les autorisations, les interdictions. Mais là, on joue en défense. Ce qui serait déjà bien, si je vous entends. Mais on n'est pas dans un jeu offensif. Une société qui se borne à défendre peut-elle survivre ?

Quant au renvoi à l'Union européenne avec laquelle il faut toujours se caler… On est toujours en avance ou en retard par rapport à l'Europe. L'Europe est difficile à construire. Dix années compliquées viennent de s'écouler. On ne sait pas très bien où l'on en est mais il faut que l'Europe soit un avenir, on n'a pas d'autres solutions.

Quant à la logique de défense, elle doit laisser place plutôt à une logique d'attaque et de construction d'une économie autour du numérique. Or, on est dans le siècle du numérique, c'est un fait. J'ai appris à écrire avec un crayon en bois et au porte-plume *Sergent-Major*, en ce sens je suis déjà une antiquité. Je n'ai eu une boîte de feutres qu'à mon entrée en seconde.

Je n'avais pas de calculette, mais j'avais une table de logarithme jaune, magnifique, quand je suis entrée en classe préparatoire. Et une table de nombres au hasard aussi. Ça, c'est magique. Où peut-on en acheter une aujourd'hui ? Ce sont des objets tangibles, aux noms poétiques, et qui vous construisent. Aujourd'hui, tout est immatériel, tout est dématérialisé, tout est accessible, tout est possible. Les jeunes d'aujourd'hui sont loin d'être tous désespérés ou suicidaires. Où les jeunes construisent-ils leur avenir mental ? Et que leur donne-t-on à lire et à voir pour qu'ils cessent d'être utilisés par des gens sans état d'âme qui sont des marchands, qui le disent et l'assument pour construire une économie nord-américaine de puissance. Ont-ils tort ? Ou est-ce nous qui avons tort de ne pas être en capacité de construire quelque chose en regard ?

M. Bruno Sido. – Je voudrais maintenant remercier particulièrement M. Pierre Lasbordes de sa venue cet après-midi. Bien entendu, les conclusions de ces auditions ne vous seront pas proposées ce soir puisqu'elles constitueront une partie de notre rapport. Avec Mme Anne-Yvonne Le Dain, nous allons retravailler tout ce que vous avez dit.

Cette journée a été particulièrement riche. Au fond, nous avons fait du numérique pratique et concret. Nous avons parlé du droit, de la difficulté d'appliquer le droit national alors même que tout se passe à la vitesse de la lumière à travers le monde. Un professeur du Collège de France est venu nous l'expliquer.

Nous avons discuté du positionnement des données ou *data*, qu'elles soient *open* ou *big*.

De même, nous avons bien vu les origines du *web*. Créé pour les chercheurs, et pour le Pentagone, effectivement, aux États-Unis d'Amérique. Et l'on sait ce que c'est devenu. L'utilisation que l'on en fait et les risques constatés sont peut-être dus à cette origine. Le *web* n'était pas fait pour cela. Peut-être qu'il sera bon de revenir, dans une troisième phase, à ce à quoi il était destiné.

Nous avons vu également, et c'est une grande leçon à retenir, que les États-Unis nous ont complètement débordés en application d'une véritable volonté politique. Après l'échec, ou la fin de l'industrie américaine, les Américains ont trouvé une autre stratégie de développement. Ils ont réussi, peut-être au-delà de ce qu'ils avaient imaginé à l'époque. Aujourd'hui, ce sont les seuls à produire des puces dont on ignore les capacités exactes et à développer des nouveautés, avec les *Google* et autres, qui sont chez eux et chez personne d'autre.

Nous avons entendu des usagers et je remercie l'*UFC-Que Choisir*. Les usagers sont un peu perdus. Évidemment, ils ne ressentent pas la nécessité de se protéger et veulent souvent aller plus vite que ceux qui cherchent à leur prendre leurs données. Nous devrons y revenir.

Je vous remercie, monsieur Benoît Virole, d'avoir parlé des enfants. Tous ceux qui ont des enfants en âge d'utiliser Internet ne peuvent qu'être totalement d'accord avec ce que vous avez dit. Il y a des réalités que je ne savais pas formuler et que, désormais, je formulerai mieux. D'ailleurs, j'ai pris un tas de notes pour les partager avec mon épouse.

Au fond, nous avons parlé des risques d'Internet, en particulier pour les entreprises, ils sont multiples, avec, bien entendu, les avantages, l'intérêt qu'on peut aussi y trouver.

Nous avons également abordé un sujet passionnant qui est celui de l'utilisation anonyme, un sujet qui conduit à évoquer celui de la liberté d'anonymat, que la police n'approuve pas forcément. À cet égard, je voudrais rappeler que la plus grande conquête de l'humanité, c'est probablement la liberté, en tout cas dans nos sociétés occidentales. Il importe d'être très sourcilleux sur la protection de la liberté des uns et des autres, même si, comme chacun le sait, la liberté a des limites.

Je remercie tous les intervenants d'avoir participé à cette journée passionnante. Merci également à son instigatrice, Mme Anne-Yvonne Le Dain. C'était une journée très riche dont nous nous efforcerons de tirer le plus grand profit pour notre rapport.

COMPTE RENDU DE L'AUDITION PUBLIQUE DU 26 JUIN 2014 : SÉCURITÉ NUMÉRIQUE DES OPÉRATEURS D'IMPORTANCE VITALE (OIV)

SOMMAIRE

INTRODUCTION

M. Bruno Sido, sénateur, président de l'OPECST
Mme Anne-Yvonne Le Dain, députée, vice-présidente de l'OPECST

Table ronde de la matinée

M. Ahmed Bennour, directeur des systèmes d'information, *Areva*

M. Lionel Darasse, chef du service de protection des activités classées et des informations (SPACI), direction centrale de la sécurité, Commissariat à l'énergie atomique et aux énergies alternatives (CEA)

M. Jean-Jacques Tourre, responsable sécurité des systèmes d'information, *Total*

Mme Pascale Bernal, directeur du système d'information, *Gaz réseau distribution France (GrDF)*

M. Alexandre Archambault, responsable des affaires réglementaires, en charge des obligations légales, *Free*

M. Christian Daviot, chargé de la stratégie auprès du directeur général, Agence nationale de la sécurité des systèmes d'information (ANSSI)

Table ronde de l'après-midi

M. Stanislas de Maupeou, directeur du secteur conseil en sécurité et évaluation, *Thales*
M. Lionel Gervais, directeur de la stratégie, *Airbus Defence & Space - CyberSecurity*

M. Thierry Floriani, responsable de la sécurité des systèmes d'information, *Numergy*

M. Cédric Prévost, directeur sécurité, qualité et programmes, *Cloudwatt*

M. Laurent Heslault, directeur des stratégies de sécurité, *Symantec en France*

M. Jean-Luc Beylat, président du Pôle Systematic Paris-Région

Mme Agnieszka Bruyère, directrice de services de sécurité, *IBM France*

M. Luc Renouil, directeur du développement et de la communication, *Bertin Technologies*, vice-président de l'association *Hexatrust* d'éditeurs français de la confiance numérique

M. Bernard Ourghanlian, directeur technique et sécurité, *Microsoft France*

Table ronde de l'après-midi (suite)

M. Badi Ibrahim, directeur des opérations, *P1 Security*

M. Stéphane Lenco, membre du bureau, Groupement interprofessionnel pour les techniques de sécurité des informations sensibles (GITSIS)

M. Jean-Marc Grémy, vice-président du Club de la sécurité de l'information français (CLUSIF)

M. Christian Daviot, chargé de la stratégie auprès du directeur général, l'Agence nationale de la sécurité des systèmes d'information (ANSSI)

AUDITION SOUS FORME DE TABLE RONDE SUR LE RISQUE NUMÉRIQUE (SÉCURITÉ DES RÉSEAUX INFORMATIQUES, STOCKAGE DES DONNÉES PERSONNELLES OU INDUSTRIELLES ET LEUR EXPLOITATION)

Mme Anne-Yvonne Le Dain, députée, vice-présidente de l'OPECST. – M. Bruno Sido, sénateur et président de l'Office parlementaire d'évaluation des choix scientifiques et technologiques (OPECST) et moi-même, députée et vice-présidente de ce même office, vous remercions de votre présence.

Le rapport relatif au risque numérique, dont nous sommes rapporteurs, est issu d'une saisine de la Commission des affaires économiques du Sénat. Nous vous recevons dans le cadre d'une table ronde, dont le compte rendu ne sera rendu public qu'avec votre accord. En effet, nous souhaitons aborder les enjeux de la sécurité des réseaux informatiques, du stockage et de l'exploitation des données, et des risques et des opportunités du numérique. Notre attention se tourne prioritairement, à titre d'illustration, vers les opérateurs d'importance vitale (OIV) et vers les entreprises des secteurs des télécommunications et de l'énergie.

Avant l'affaire Snowden, il était rare de parler publiquement de la sécurité numérique qui demeurait l'apanage de la presse spécialisée et de cercles restreints. Depuis cet événement, une inquiétude a émergé, à laquelle le Parlement doit répondre tout en notant que, au-delà des risques sécuritaires et économiques, le numérique est également porteur d'opportunités qui doivent être saisies.

Dans une économie immatérielle et concurrentielle, le numérique, qu'il soit perçu comme un atout ou une contrainte, est devenu une réalité incontournable. Contrairement à ce que l'on pouvait croire dans les années 1990, le XXIe siècle ne sera pas le siècle des sciences du vivant mais celui des sciences de la matière. Le numérique a donné naissance à une économie caractérisée par l'interconnexion, l'instantanéité et l'incertitude. Plus globalement, il a conduit à une reconfiguration de toutes les catégories : l'individu, les corps intermédiaires et la nation. Rien n'est stable, hormis notre personne physique. Les opérateurs d'importance vitale (OIV) sont essentiels à notre pays sur un plan économique, diplomatique et militaire. Ils fabriquent de la valeur ajoutée à partir du virtuel qui vient améliorer l'économie et le monde réel.

La sécurité numérique nécessite du temps ainsi que du personnel formé, du matériel fiable et une architecture adaptée. Elle concerne non seulement les OIV, mais aussi leurs sous-traitants et leurs clients. Ainsi

intéresse-t-elle également les petites et les moyennes entreprises (PME), les très petites entreprises (TPE), les réseaux et les individus.

Nous avons réalisé à ce jour près de quatre-vingts auditions, ainsi que des visites de terrain à Paris et en région. La présente table ronde marque le terme de cette phase de travail préliminaire. Nous procédons ce matin à l'audition d'OIV des secteurs des télécommunications et de l'énergie, et, cet après-midi, à celle d'entreprises proposant des solutions de sécurité numérique.

Je vous remercie une nouvelle fois de votre participation et donne la parole à M. Ahmed Bennour, directeur des systèmes d'information d'*Areva*.

M. Ahmed Bennour, directeur des systèmes d'information, *Areva*. – Je vous remercie, madame la vice-présidente.

Je souhaiterais tout d'abord vous présenter les moyens dont nous disposons afin d'assurer notre sécurité numérique. Le premier d'entre eux est la prévention qui s'exerce lors de la formation de notre personnel, de l'élaboration de nos processus et du choix de nos technologies. Nous devons toutefois garder à l'esprit que, compte tenu de l'essor et de l'évolution des risques, **nul moyen de prévention n'est infaillible et nul système d'information n'est inattaquable**. Afin de pallier ces difficultés, il existe des outils de lutte défensive qui consistent en un système de détection, d'analyse et de réaction face aux agressions.

Comme toute entreprise sensible, ***Areva*** **fait face à des tentatives d'attaque permanentes**. Il existera toujours une dissymétrie de moyens entre la cible et l'auteur de l'attaque, notamment en cas d'agression par une officine paraétatique. Sur ce point, je vous rappelle que la presse indique que les cyberattaquants chinois disposent de moyens dignes de ceux d'une armée. Même lorsque l'intrusion est le fait d'organisations moins sophistiquées, ces dernières peuvent mobiliser des réseaux et des techniques de cyberguérilla. Dans ce contexte, nous avons besoin de moyens étatiques, comme ceux de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Je témoigne du fait qu'**il nous serait difficile d'assurer la sécurité de notre système d'information sans le soutien de l'ANSSI**.

Je voudrais souligner que le secteur du numérique est en évolution permanente, ce qui nous oblige à constamment nous adapter. À titre d'illustration, les envois de *spams* ont augmenté et se sont perfectionnés, rendant leur détection d'autant plus difficile. Il nous faut trouver un équilibre entre les risques que nous pouvons accepter et les moyens que nous souhaitons mobiliser. **Il n'est pas possible de protéger de manière identique tout le système d'information d'une entreprise.** Il faut donc être capable d'**identifier ce qui est vital pour l'entreprise**, son fonctionnement, son patrimoine immatériel, sa compétitivité. Par exemple, les moyens techniques du système d'information doivent être impérativement protégés.

En somme, il s'agit d'abandonner l'illusion d'une sécurité absolue, de s'adapter face à des menaces évolutives et d'identifier un « coffre-fort », c'est-à-dire les données, les techniques et les activités les plus importantes, afin de leur allouer l'essentiel des moyens de protection.

L'origine des technologies pose des questions de souveraineté et de confiance. L'écosystème numérique français n'a actuellement pas la taille critique pour développer certaines technologies. Des entreprises étrangères, comme *Microsoft*, *Oracle* ou *SAP*, ont acquis une place prépondérante sur le marché. Il convient d'identifier les technologies importantes pour la sécurité numérique des entreprises et de la nation, telles que les *Public Key Infrastructures* (*PKI*) – qui sont des systèmes d'authentification ou de chiffrement –, afin d'investir dans les offres les plus fiables et d'encourager leur production en France.

Ce travail de hiérarchisation des systèmes et des technologies d'information en fonction des risques est également valable s'agissant des données.

En ce qui concerne le *cloud computing*, nous lui accordons une confiance limitée dans la mesure où la géolocalisation des données et le degré d'application des mesures d'hygiène informatique ne sont pas garantis. Il est difficile de s'assurer que le prestataire, soumis à des objectifs de rentabilité financière, soit en capacité d'appliquer les mesures de sécurité requises. En outre, il existe un problème de réversibilité : une fois les données mises dans le nuage, existe-il des moyens suffisamment robustes pour les récupérer ?

J'insiste sur le fait que l'accompagnement de l'ANSSI est capital, étant donné la dissymétrie des moyens et la complexité des enjeux. La Commission nationale de l'informatique et des libertés (CNIL) joue également un rôle, davantage axé sur la protection des données personnelles.

S'agissant de la sous-traitance, **les contrats peuvent prévoir des engagements, un accompagnement et un contrôle en matière de sécurité**. La composante humaine demeurant fondamentale, nos collaborateurs doivent être formés à ces problématiques afin d'utiliser le système d'information de manière sécurisée. Sur ce point, je constate que l'affaire Snowden, dont on parle tant, est révélatrice d'un problème, non technologique mais humain.

Mme Anne-Yvonne Le Dain. – Utilisez-vous un téléphone portable sécurisé ?

M. Ahmed Bennour. – Encore un fois, il s'agit de mettre en balance les données devant être protégées avec les moyens pouvant être utilisés. Mon téléphone portable comprend un dispositif de sécurité permettant l'**isolement des messages professionnels** dans un *container*. Les messages électroniques chiffrés ne sont lisibles que sur mon *PC* à l'aide d'une carte à puce.

M. Alexandre Archambault, responsable des affaires réglementaires, en charge des obligations légales, *Free*. – Un exemple de téléphone sécurisé est *Teorem* de *Thales*. **Il faut promouvoir la défense en profondeur et l'hygiène informatique auprès des utilisateurs de téléphones standards** pour qu'ils les utilisent à bon escient. Les informations sensibles doivent, quant à elles, transiter par des canaux particuliers.

M. Christian Daviot, chargé de la stratégie auprès du directeur général, Agence nationale de la sécurité des systèmes d'information (ANSSI). – Le président de la République et le ministre en charge de la défense utilisent un téléphone sécurisé pour leurs conversations relevant du secret de la défense nationale. Ce terminal n'est pas ergonomique. Il ne disposait initialement pas d'une fonction *Short Message Service* (*SMS*). Il ne fonctionne toujours pas dans les pays où les communications sont chiffrées. Le pouvoir exécutif dispose donc de téléphones, certes sécurisés, mais peu ergonomiques.

L'ANSSI a développé le téléphone sécurisé *Secdroid.*

Nous avons eu recours à des solutions commerciales, dans un souci d'ergonomie. Ces solutions n'ont pas un niveau de fiabilité suffisant car elles offrent peu de résistance aux attaques testées par nos ingénieurs.

M. Ahmed Bennour. – Comme je le dis souvent à notre direction générale et à nos collaborateurs, la sécurité représente des coûts et des contraintes qui doivent être mis en regard des risques en présence.

Des interrogations subsistent quant aux logiciels antivirus. Je les considère comme un moyen, non de protection mais de prévention. **Ils ne sont pas totalement fiables** car ils reposent sur une identification des failles qui varie dans le temps et selon les fabricants. Il est donc nécessaire d'**utiliser plusieurs antivirus**, aux différents niveaux du système d'information.

Pour en revenir aux tentatives d'attaque, celles-ci sont quotidiennes pour une entreprise comme *Areva*. Nous avons adapté notre organisation en conséquence : à travers **un centre opérationnel de sécurité** et un système de collecte, d'analyse, d'identification, d'alerte et de réaction.

Nous avons également défini une politique de sécurité moderne. Émanant du président du groupe et impliquant toutes les directions, elle accorde une **place centrale à la cybersécurité**. Chaque direction a un rôle à jouer : la direction des ressources humaines s'assure de la restitution du matériel et des accès informatiques par le personnel sortant tandis que la direction juridique élabore les clauses contractuelles relatives à la sécurité numérique et que la direction des achats veille au respect des règles de sécurité auprès des fournisseurs. L'implication de toutes les parties prenantes permet une meilleure acceptation des coûts et des contraintes liés à la sécurité numérique.

Mme Anne-Yvonne Le Dain. – À partir de quand avez-vous mis en place la politique de sécurité dont vous parlez ?

M. Ahmed Bennour. – Nous avons actualisé notre politique de sécurité il y a deux ans.

Je souhaiterais vous faire part d'interrogations d'ordre juridique sur la sécurité numérique. **La protection des systèmes d'information ne doit pas se muer en une surveillance du personnel.** Nous nous gardons bien de prendre connaissance d'informations personnelles auxquelles nous pourrions pourtant avoir accès, tels que les courriers électroniques. Il faut être très rigoureux sur ce point : un cadre légal et des considérations éthiques s'imposent. Cela est d'autant plus important que la sécurité du système d'information repose sur la confiance des utilisateurs. Si le personnel n'a plus confiance dans la messagerie professionnelle, alors il utilisera une messagerie personnelle, ce qui nuira *in fine* à la sécurité du système d'information.

Les produits que nous achetons posent également question dans la mesure où ils peuvent contenir des portes dérobées ou *backdoors*. Aussi est-il préférable de **recourir à des entreprises françaises pour la fourniture des éléments les plus importants du système d'information.**

S'agissant de l'attribution des noms de domaine, qui est réalisée par une société américaine, elle me semble avoir le mérite de la transparence et ne pose **pas de difficulté en termes de sécurité**.

Je voudrais enfin évoquer un axe d'amélioration de la sécurité numérique. Selon moi, il est essentiel d'inclure la gouvernance et l'organisation de l'entreprise dans le champ de la politique de sécurité numérique. L'approche a changé : il ne s'agit plus de se conformer à des normes mais d'évaluer les risques acceptables et les moyens mobilisables.

Mme Anne-Yvonne Le Dain. – Je vous remercie de votre intervention. Je passe la parole à M. Lionel Darasse, du Commissariat à l'énergie atomique et aux énergies alternatives (CEA).

M. Lionel Darasse, chef du service de protection des activités classées et des informations (SPACI), direction centrale de la sécurité, Commissariat à l'énergie atomique et aux énergies alternatives (CEA). – Je vous remercie, madame la vice-présidente.

Je souhaiterais présenter successivement les activités, le système d'information et la politique de sécurité numérique du CEA.

Le CEA est un établissement public à caractère industriel et commercial, qui regroupe dix établissements et 16 000 salariés. La diversité de nos activités a une incidence sur notre système d'information et nous soumet à des obligations réglementaires particulièrement denses. Aussi doit-on répondre aux besoins exprimés par nos unités de recherche fondamentale, de recherche appliquée, d'exploitation d'instruments de

recherche et d'installations nucléaires, et de fourniture d'éléments de la dissuasion nucléaire.

Le CEA est un opérateur d'importance vitale (OIV) à plusieurs titres. Il participe à la protection du potentiel scientifique et technique de la nation ainsi qu'à la protection du secret de la défense nationale. Il respecte des règles d'exploitation qui visent à garantir l'intégrité des données, telles que celles afférentes à la protection et au contrôle des matières et des sites nucléaires et la disponibilité des outils de suivi. Cette situation nous astreint à maintenir un système d'information fiable, disponible et intègre.

Le CEA est également un déposant important de brevets, ce qui nous oblige à accorder une attention particulière à la propriété intellectuelle. Nous protégeons les résultats des recherches et développons une stratégie partenariale d'industrialisation.

Des notes d'instructions générales, validées par l'administrateur général du CEA, donnent des instructions dans un certain nombre de domaines, comme par exemple, la publication et la gestion des communications externes.

Le contexte précisé, je voudrais maintenant présenter le système d'information du CEA, principalement pour sa partie « civile », la direction des applications militaires (DAM) doit être traitée à part car elle fait l'objet de mesures de sécurité renforcées.

Concernant le *BYOD* et le recours à des solutions externalisées, puisque ce sujet vient d'être abordé dans l'intervention précédente, rappelons que, si les outils informatiques d'entreprise fournis au personnel sont moins performants que ceux proposés au grand public, ils auront tendance à ne pas être utilisés et nous verrons apparaître des pratiques de contournement, non maîtrisées et potentiellement dangereuses pour la sécurité. Il faut donc veiller à **offrir des services informatiques sécurisés, de confiance et de qualité de service équivalent à ceux accessibles à l'extérieur de l'entreprise**.

Mme Anne-Yvonne Le Dain. – MM. Ahmed Bennour et Lionel Darasse, vous venez tous deux d'indiquer qu'il vous faut proposer au personnel une offre équivalente à celle du marché afin qu'il n'ait pas recours à des outils extérieurs, et donc non sécurisés. Ne devriez-vous pas, à votre tour, déposer des brevets et proposer des formations en la matière ?

M. Lionel Darasse. – Je crois que l'offre externe disponible sur le marché sera toujours légèrement supérieure à celle développée en interne car nos solutions, sécurisées, sont issues d'un compromis entre l'efficacité technique et l'acceptabilité sociale. Les règles de sécurité numérique doivent donc être raisonnablement adaptées et suffisamment ergonomiques pour qu'elles n'excèdent pas le niveau qui est toléré par le personnel et qui est observé dans des organismes comparables.

Ces considérations ne s'appliquent pas à nos activités relevant du secret de la défense nationale pour lesquelles le compromis n'existe pas, seul le résultat compte.

M. Ahmed Bennour. – Nous assistons à un phénomène de « consumérisation » de l'informatique. Autrefois, la technologie allait de l'entreprise au domicile privé. Les ordinateurs ont été conçus pour un usage professionnel, avant d'être affectés à un usage personnel. Aujourd'hui, la technologie va du domicile privé à l'entreprise. Les *smartphones* et les tablettes ont été créés pour la sphère privée avant d'être introduits dans le milieu professionnel.

Les entreprises ne peuvent pas, pour des raisons de sécurité et de coût, introduire en leur sein toutes les technologies disponibles. Les nouvelles technologies doivent avoir un degré de maturité suffisant. La flotte de terminaux mobiles d'une entreprise ne saurait être remplacée au rythme de la commercialisation d'un nouvel *iPhone* tous les six mois. En outre, les nouvelles technologies ne doivent pas avoir un coût excessif. Une tablette étant aussi chère qu'un ordinateur, est-il possible et souhaitable de doubler le coût du parc informatique d'une entreprise ? Une contrainte de sécurité nécessite enfin d'observer un temps d'analyse et d'information avant d'intégrer les technologies à l'organisation et au fonctionnement de l'entreprise.

M. Lionel Darasse. – Pour en revenir au système d'information du CEA, celui-ci englobe des composantes scientifique, bureautique et industrielle.

Le CEA utilise Internet depuis 1993. Notre dotation informatique et notre degré d'exposition aux risques sont importants.

Le système d'information du CEA comprend : 20 000 postes, 30 000 comptes, deux artères Internet avec un débit de 10 Gigabits, 5 000 utilisateurs d'outils informatiques dits nomades et 300 serveurs affectés aux collaborations scientifiques en ligne. Notre principal système d'exploitation est *Windows*, devant *Linux* et *Macintosh*.

Notre activité est localisée exclusivement en France. Autrefois organisé autour de dix établissements seulement, le CEA a également développé des antennes de recherche mixte ou de représentation régionale. Il nous a donc fallu développer notre réseau et notre offre numériques.

Outre la sécurité numérique, nous sommes également attentifs à la sécurité physique. **Nos locaux reçoivent une habilitation avant d'accueillir des installations numériques**, ce qui apporte davantage de fiabilité et de traçabilité face aux effractions et aux vols.

Le CEA a une position claire sur le *cloud computing* et l'infogérance. **Nous n'utilisons pas le *cloud computing* car nous souhaitons conserver la**

maîtrise de notre système d'information. Nous recourons à l'infogérance mais nous hébergeons les sous-traitants dans nos locaux.

Mme Anne-Yvonne Le Dain. – Est-ce à dire que vos sous-traitants utilisent votre réseau de fibre optique ?

M. Lionel Darasse. – Tout à fait. Nos sous-traitants sont hébergés sur notre réseau ; ils y disposent de profils gérés par nous et d'outils importés par eux mais supervisé par le CEA.

Quant à **notre utilisation d'Internet**, je constate que celle-ci **est peu liberticide**. Sans doute faut-il y voir une explication historique et intrinsèque aux activités de recherche qui nécessitent un usage large d'Internet. Aussi notre politique de sécurité est-elle plutôt orientée vers des mesures relatives à l'organisation du travail, à l'utilisation des équipements, à la sécurité des produits, à la formation des utilisateurs et à une importante activité de supervision des réseaux.

Dans les années 2000, le CEA a créé un laboratoire de sécurité des systèmes d'information, placé **auprès de la direction centrale de la sécurité**. Il s'agit là d'une organisation singulière car la plupart des entreprises disposent d'un service de sécurité rattaché à une direction en charge de l'informatique. L'organisation retenue par le CEA offre à mes équipes une grande liberté d'action. Au sein de commissions de gouvernance, généralement présidées par l'administrateur général adjoint, la direction centrale de la sécurité et le laboratoire de sécurité des systèmes d'information évaluent, sur le plan de la sécurité, l'ensemble des besoins en informatique exprimés par le personnel. Ce système, dont le fonctionnement est satisfaisant, permet de garantir notre indépendance de jugement et d'appréhender le sujet au plus haut niveau hiérarchique de l'organisme. On assiste ainsi à une appropriation du sujet et de ces enjeux à tous les niveaux de l'entreprise, dès le début des projets. L'équipe que j'anime a d'autres missions : l'analyse des risques numériques, la formation et l'animation du réseau fonctionnel, l'évaluation de produits de sécurité et la supervision des réseaux et parfois la réalisation de **tests de contrôle**. Nous conduisons en effet des **tests d'intrusion du réseau** afin de s'assurer du maintien dans le temps des règles de sécurité.

Le CEA a mis en place une charte d'utilisation des moyens informatiques et des services Internet, signée par son administrateur général. L'usage personnel des moyens informatiques est toléré dans la limite d'un usage raisonnable et dans la mesure où l'activité professionnelle ne s'en trouve aucunement affectée et où celui-ci n'est pas susceptible de porter atteinte à la sécurité des systèmes d'information, aux intérêts ou à l'image du CEA Cependant, **est présumée avoir un caractère professionnel toute information traitée par les moyens informatiques du CEA**. Cela signifie que nous avons toute latitude pour intervenir sur une machine, un serveur ou un compte d'utilisateur pour un motif de sécurité. Les données que nous collectons visent seulement à vérifier l'existence ou non d'un détriment,

d'une attaque caractérisée, d'une intrusion volontaire ou d'une utilisation détournée du système. En matière de téléphonie, **le CEA fournit des téléphones et des abonnements professionnels qui peuvent donc être désactivés en cas de difficulté**.

Parmi les politiques de sécurité que nous avons mises en place, la plus importante est celle relative aux réseaux. Elle permet aux exploitants des systèmes d'information d'apprécier, au moyen d'un questionnaire pédagogique, le degré de sensibilité de leurs données pour que celles-ci soient stockées de manière appropriée sur notre réseau.

En ce qui concerne les technologies dites nomades, nous disposons de plusieurs outils de sécurité : **les ordinateurs portables sont sécurisés au moyen de deux systèmes de chiffrement** – antivol et *data* ; **les** *smartphones* **portables disposent d'un code d'accès et ne permettent pas d'afficher les contenus chiffrés de la messagerie CEA**. Quelques hautes personnalités du CEA ont exprimé le souhait de disposer de **téléphones sécurisés** (étude en cours).

Mme Anne-Yvonne Le Dain. – Je vous remercie de votre exposé. Je passe la parole à M. Jean-Jacques Tourre.

M. Jean-Jacques Tourre, responsable de la sécurité des systèmes d'information, *Total*. – Je vous remercie, madame la vice-présidente.

Présent dans cent trente pays, le groupe *Total* emploie 100 000 personnes, ayant, par ailleurs, une forte mobilité. Si notre groupe est un opérateur d'importance vitale, il n'est pas soumis pour autant aux obligations « secret défense » ou « confidentiel défense ». La sécurité numérique est un enjeu important pour le groupe *Total* et sa direction générale.

Nous avons assisté à une évolution notable des menaces ces dix dernières années. Au début des années 2000, nous étions vulnérables aux infections virales généralisées, comme *I love you* ou *Nimda*. Au milieu des années 2000, la situation s'est stabilisée. Depuis lors, nous constatons un net avantage aux attaquants, notamment en termes de moyens.

Depuis 2012, soit bien avant l'affaire Snowden, plusieurs éléments ont contribué à une prise de conscience au sein du groupe *Total*. Nous avons tout d'abord élaboré une **cartographie des risques numériques**, qui a clarifié lesdits risques liées à la sécurité, aux projets ou à la sous-traitance. Nous avons également participé à un ***benchmark* sur la sécurité des systèmes d'information des compagnies pétrolières** qui a mis en lumière une situation plus contrastée que nous le pensions. Enfin, en 2012, les attaques dont ont été victimes les compagnies *Saudi Aramco* et *Rasgas* (association de *Qatar Petroleum* et *ExxonMobil*), dans le golfe Arabo-Persique, ont été déterminantes. *Saudi Aramco*, avec qui nous entretenons des relations de haut niveau, a perdu les deux tiers de ses postes informatiques. *Rasgas*,

qui, comme nous, exploite une usine de gaz naturel liquéfié au Qatar, a fait l'objet d'une agression concomitante.

Dans ce contexte, nous avons élaboré et présenté au comité exécutif du groupe un plan pour améliorer la sécurité de notre système d'information. Il a donné à la sécurité une visibilité ainsi que des moyens, sur la période 2013-2016.

Les affaires Snowden et *Target* sont venues, par la suite, confirmer la nécessité de notre démarche.

Mme Anne-Yvonne Le Dain. – La multiplication des incidents informatiques et leur divulgation au grand public représentent-elles une opportunité de prise de conscience ou un risque de banalisation ?

M. Jean-Jacques Tourre. – Je pense que les incidents informatiques seront de plus en plus connus du grand public ; et, ce, d'autant plus que certaines dispositions juridiques, y compris européennes, obligent à rendre compte de la perte de données personnelles.

J'observe une prise de conscience des entreprises et des particuliers. Il y a encore cinq ans, la cybersécurité n'était pas à l'ordre du jour politique et parlementaire. Les cas de fraude aux moyens de paiement en ligne ont joué un rôle de révélateur auprès du grand public.

M. Ahmed Bennour. – Les médias, qui sensibilisaient hier les individus aux risques, participent aujourd'hui à une banalisation des enjeux.

La communication est un outil important pour l'entreprise confrontée à une attaque. Celle-ci doit se garder de signifier à l'agresseur qu'elle l'a détecté. L'agresseur ayant tiré profit d'un effet de surprise lors de l'attaque, l'entreprise a le droit d'en faire usage à son avantage au cours de la riposte.

La réputation des entreprises présentes sur les marchés internationaux peut également être mise à mal par la survenue d'incidents à répétition.

Il conviendrait davantage d'aborder l'enjeu de la communication sous l'angle du « besoin d'en connaître » plutôt que de la transparence. Si je trouve justifié de notifier les attaques à l'ANSSI, je ne saisis pas l'intérêt de leur divulgation au grand public.

M. Lionel Darasse. – Je souhaiterais ajouter une remarque sur la banalisation des incidents. Je crois que ce phénomène est dû au fait que **chacun diffuse des informations personnelles sans nécessairement s'en rendre compte**. S'agissant des données ne pouvant faire l'objet d'aucune attaque, nous élaborons des partenariats avec l'ANSSI et des filières industrielles françaises pour maintenir le plus haut degré de sécurité.

Le partage des indices d'intrusion, même s'il est éminemment difficile, permettrait à chacun de s'assurer de l'efficacité de sa politique de

sécurité. Il importe de trouver un équilibre entre la confidentialité et l'échange des informations afin de nous permettre de répondre rapidement aux alertes. Sur ce point, dont nous discutons avec l'ANSSI, une marge de progression existe.

M. Christian Daviot. – Il existe deux filières complémentaires : celle de la CNIL, qui prévoit une obligation de divulgation en cas de contrefaçon de données personnelles, et celle de l'ANSSI, qui privilégie la confidentialité des informations.

Sur la centaine d'attaques de grande ampleur ayant visé des entreprises ou des administrations françaises en trois ans, seules deux ou trois ont été rendues publiques.

L'article 22 de la loi de programmation militaire confirme le principe de confidentialité des informations privilégiant ainsi l'approche de l'ANSSI sur celle de la CNIL.

M. Jean-Jacques Tourre. – S'agissant du plan de sécurité des systèmes d'information du groupe *Total*, sa première partie concerne les infrastructures. Nous avons considéré qu'il était essentiel de définir une feuille de route afin de fixer des priorités et de sélectionner les offres. Compte tenu de l'évolution rapide des menaces et des technologies, ce plan pourra être actualisé annuellement.

Je voudrais insister sur un point. Nous avons évoqué les outils de prévention tels que les logiciels antivirus. Je constate que l'on assiste au **passage d'une logique de prévention à une logique de détection et de réaction**. Ce qui importe est de détecter et de répondre rapidement aux intrusions.

Je souhaiterais revenir sur la cyberintelligence, c'est-à-dire le partage d'informations dans le domaine de la sécurité informatique. Il est important de **mettre en place des systèmes d'échange**. Le centre opérationnel de sécurité que nous avons instauré au sein du groupe *Total*, a révélé l'importance du partage des données. Une information, transmise par l'ANSSI ou par une autre société, peut nous permettre de détecter plus efficacement les attaques.

Mme Anne-Yvonne Le Dain. – Diriez-vous ainsi que davantage de solidarité est nécessaire entre les entreprises ?

M. Jean-Jacques Tourre. – J'ignore si le terme de solidarité est le plus approprié mais je crois à l'utilité d'une structure telle que l'ANSSI, assurant la collecte et le partage des informations, dans le respect du principe de confidentialité. La loi de programmation militaire va en ce sens. L'existence d'un tiers facilite grandement les échanges et n'empêche pas les relations bilatérales entre sociétés.

Je voudrais évoquer l'enjeu crucial de la souveraineté numérique. S'il est illusoire de penser qu'un système informatique puisse être

entièrement souverain, il demeure pertinent de **disposer d'entreprises françaises assez importantes pour assurer la conception de certains équipements stratégiques, comme les systèmes de gestion des clés publiques ou *Public Key Infrastructures (PKI)***.

Notre plan de sécurité comprend un deuxième volet spécifique au système d'information industriel. Nous avons participé à l'élaboration d'un guide édité par l'ANSSI à ce sujet. Cet enjeu est primordial puisque les systèmes d'information industriels sont plus ouverts qu'auparavant. En outre, il est plus difficile d'assurer la sécurité du système d'information industriel, éclaté sur plusieurs sites industriels, que celle des infrastructures, centralisées. Le groupe *Total* dénombre plus d'un millier de sites industriels, dont 300 de type SEVESO.

Le troisième volet concerne la sécurité des applications, en particulier la gestion des identités et des accès.

Le quatrième volet a trait à la sensibilisation du personnel. L'objectif n'est pas d'informer le personnel, déjà bien au fait des risques numériques, mais de **conduire à un changement de comportements**. Nous avons mis en place des actions de sensibilisation et allons développer un programme transversal au sein du groupe.

Il existe enfin deux autres volets complémentaires. Le premier concerne les processus de gestion et de sécurité des systèmes d'information, comme la gestion de crise. L'enjeu est d'instaurer une approche commune aux directions des systèmes d'information des différentes entités du groupe. Le second porte sur le *management* des risques. En abordant la politique de sécurité par le prisme des risques, nous pouvons communiquer plus facilement sur la sécurité numérique, notamment auprès de la direction générale. Nous travaillons à la mise en place d'un système de *management* des risques qui nous permettra d'actualiser notre cartographie des risques et de disposer d'une aide à la décision lors du lancement des programmes.

Mme Anne-Yvonne Le Dain. – Quelle est la réaction du personnel face à ces évolutions ?

M. Jean-Jacques Tourre. – La réaction du personnel est plutôt bonne. La direction en charge de la sécurité au sein du groupe *Total* organise des sessions de sensibilisation et de formation. L'explication des risques est généralement bien comprise par le personnel même si la sécurité est souvent perçue comme une contrainte.

Nous avons souhaité, dans notre programme relatif aux infrastructures, accompagner l'innovation et les nouvelles technologies. À titre d'exemple, l'information dans le nuage ou *cloud computing* est une réalité qui ne doit pas être niée mais qui doit être davantage sécurisée, par un **système d'authentification** et des **outils de chiffrement**.

L'innovation et la sécurité sont les deux facettes d'une même pièce. Il y a quelques années, la sécurité était moins valorisée que l'innovation. La protection des informations est aujourd'hui considérée comme un enjeu important et il est davantage admis de se préoccuper à la fois d'innovation et de sécurité. Le vol de dizaines de millions de cartes bancaires (affaire *Target*) conforte cette prise de conscience. Notre plan allie résolument innovation et sécurité.

Mme Anne-Yvonne Le Dain. – Je souhaiterais vous poser la même question que celle que j'ai posée à MM. Ahmed Bennour et Lionel Darasse : pensez-vous que ce que le couple sécurité-innovation, que vous vous évertuez à mettre en place, puisse donner lieu à des solutions commercialisables ?

M. Jean-Jacques Tourre. – Notre rôle est d'intégrer à notre organisation des solutions disponibles sur le marché afin de faire bénéficier le personnel de nouvelles fonctionnalités. Les innovations que vous évoquez sont peut-être commercialisables mais pas par nous, qui en sommes seulement utilisateurs.

Mme Anne-Yvonne Le Dain. – Je vous remercie de cet élément de réponse.

Je donne maintenant la parole à Mme Pascale Bernal.

Mme Pascale Bernal, directeur du système d'information, *Gaz réseau distribution France (GrDF)*. – Je partage une grande partie de ce qui a été dit précédemment : nous faisons face aux mêmes enjeux et aux mêmes préoccupations.

Je souhaiterais tout d'abord présenter l'entreprise *GrDF*. Notre activité de distribution de gaz s'adresse à onze millions de clients et se limite à la France métropolitaine. Nous partageons un service commun, composé de 46 000 personnes, avec *Électricité réseau distribution France* (*ErDF*). Une partie de nos applications est gérée par les *data centers* du groupe *GDF Suez* et l'autre par ceux du groupe *Électricité de France* (*EDF*). Nous devons nous assurer que nous respectons les règles de sécurité de ces deux groupes. Cette particularité nous oblige à accorder une attention particulière à la sécurité. Nous n'avons pas d'obligations « secret défense » et nous ne possédons pas aujourd'hui des systèmes d'information industriels.

Je voudrais évoquer le projet de compteur communiquant *Gazpar*, sur lequel nous collaborons actuellement avec l'ANSSI. Ce programme permettra de relever automatiquement les compteurs de l'ensemble des clients de notre activité de distribution de gaz. L'objectif n'est pas d'agir à distance sur les compteurs mais de disposer d'**une chaîne d'information, cryptée et authentifiée, allant des compteurs à notre système d'information**. Aussi partagerons-nous un système de *PKI* avec les fabricants de compteurs. Les données transiteront également par des concentrateurs, soumis aux mêmes règles de confidentialité. **Nous nous**

préoccupons de la sécurité numérique dès la conception de nos applications et travaillons tant avec l'ANSSI qu'avec la CNIL.

Avec onze millions de clients et trente fournisseurs, le groupe *GrDF* dispose de données personnelles ou de données commercialement sensibles. Nous sommes assujettis à une stricte obligation de neutralité, qui nous interdit de communiquer à un fournisseur des informations susceptibles de l'avantager. Nous veillons à ce que cette obligation soit également respectée par le fournisseur historique de gaz qui appartient au même groupe que le nôtre.

Nos données sont, à 90 %, stockées dans des centres privés *(data centers)* mais celles qui ne présentent pas de caractéristique particulière sont conservées dans un nuage (*cloud)* public. Comme déjà souligné, la sécurité de nos applications est évaluée dès leur conception. Le degré de confidentialité de nos données fait également l'objet d'un examen. Sur la base de ces analyses, **plusieurs niveaux de sécurité** déterminent les conditions de fonctionnement de nos applications et de mise à disposition de nos données.

Les systèmes d'information sont de plus en plus ouverts alors qu'ils étaient auparavant internes à l'entreprise. Le système d'information de *GrDF* a davantage d'utilisateurs externes qu'internes. On dénombre des dizaines de milliers d'utilisateurs auprès de nos fournisseurs et des clients en contrat de livraison directe. Les utilisateurs d'objets connectés viendront s'ajouter à ces utilisateurs externes dans un avenir proche. L'ouverture des systèmes d'information pose un problème de sécurité et nécessite des mesures destinées à protéger le « coffre-fort ».

L'autre point important est l'essor de la mobilité. La plupart de nos collaborateurs, y compris le personnel en charge des interventions techniques, disposent d'outils de mobilité. Ces applications, qui sont reliées à notre système d'information, doivent faire l'objet d'une **protection particulière**. Il nous faut constamment nous adapter afin d'éviter une séparation trop stricte entre les systèmes d'information, contraignants, et le numérique, attractif. C'est à cette condition que les usagers acceptent de ne pas utiliser d'applications externes et de se conformer aux règles de sécurité. Il importe également de **promouvoir une organisation souple et innovante**. Les systèmes d'information sont le moteur de la performance de l'entreprise d'aujourd'hui et de l'innovation de l'entreprise de demain. Le travail des directions des systèmes d'information s'est donc diversifié et complexifié.

Comme je l'ai déjà évoqué, nous collaborons avec l'ANSSI au sujet du projet de compteur communiquant *Gazpar*. Une attention particulière est portée à la protection des données personnelles et commercialement sensibles. Nous avons fait l'objet d'une visite inopinée de la CNIL, il y a deux ans. Cette dernière a contrôlé la manière dont nous traitons les données personnelles. Nous travaillons également avec un certain nombre de collectivités territoriales, au titre d'opérateur de réseau. S'il est justifié de

leur transmettre des informations, il faut veiller à ce que ces données ne révèlent pas, après un recoupement, la situation spécifique d'entreprises ou de particuliers. Nous agissons dans la **double préoccupation de mettre à la disposition des parties prenantes des informations utiles et d'assurer la sécurité des données personnelles et commercialement sensibles**. À nouveau, l'enjeu est de maintenir un équilibre entre la sécurité et l'innovation dont notre entreprise et nos clients puissent tirer profit.

Mme Anne-Yvonne Le Dain. – Les fichiers de données personnelles dont vous disposez ne sont donc pas susceptibles d'être commercialisés ?

Mme Pascale Bernal. – Non, en aucun cas. Cela n'est pas possible d'un point de vue juridique et n'est pas envisagé sur un plan commercial. **Les données personnelles sont les informations que nous protégeons le plus** au sein de notre système d'information.

Mme Anne-Yvonne Le Dain. – En est-il de même pour vous ?

M. Lionel Darasse. – Oui.

M. Jean-Jacques Tourre. – Oui.

Mme Pascale Bernal. – Nous achetons des informations pour qualifier nos fichiers mais nous n'en vendons pas nous-mêmes.

Mme Anne-Yvonne Le Dain. – Ce sujet est à l'heure actuelle très sensible mais pourrait l'être moins à l'avenir. Serait-il alors possible de faire de l'exploitation des données une activité profitable à la nation ?

Pour en revenir au compteur communiquant *Gazpar*, je constate que beaucoup de personnes, y compris des responsables publics, expriment une angoisse quant à la protection de leur vie privée. Pour parler trivialement, ils craignent que l'on sache ce qu'ils font à deux heures du matin. Comment répondez-vous à cette appréhension ?

Mme Pascale Bernal. – Nous entendons ces interrogations. Cependant, les compteurs de gaz ne sont pas, ni ne seront jamais, en capacité de savoir ce que les utilisateurs font à deux heures du matin. Le compteur communiquant *Gazpar* nous transmettra quotidiennement des informations relatives à la consommation de gaz. En conséquence, **les données transférées ne seront ni personnelles ni instantanées. Les informations recueillies concerneront seulement le chauffage, l'eau chaude ou la cuisson**. Si nous entendons les interrogations exprimées, elles ne concernent pas directement l'activité gazière.

Mme Anne-Yvonne Le Dain. – Mais vous partagez cependant des fichiers avec *ErDF*. L'angoisse dont je parle est également répandue parmi les couches aisées de la société. Il demeure des inquiétudes, notamment quant à l'utilisation des données à des fins publicitaires.

Mme Pascale Bernal. – La protection des données fait partie des discussions que nous avons engagées au sujet du compteur communiquant

Gazpar, avec les collectivités territoriales et les associations de consommateurs. Au sein d'instances de concertation, dont la Commission de régulation de l'énergie (CRE), nous conduisons un dialogue destiné à répondre aux interrogations sur la collecte et l'exploitation des données.

Mme Anne-Yvonne Le Dain. – Je vous remercie de votre présentation. Je passe la parole à M. Alexandre Archambault.

M. Bruno Sido, sénateur, président de l'OPECST. – Monsieur Alexandre Archambault, vous avez la parole.

M. Alexandre Archambault, responsable des affaires réglementaires, en charge des obligations légales, *Free*. – Monsieur le président, madame la vice-présidente, je vous remercie de votre invitation. Je m'associe pleinement à ce qui a été exprimé précédemment. Mon intervention est structurée autour de deux questions : quelle conception avons-nous du risque numérique ? Quelles propositions souhaitons-nous soumettre au décideur public ?

Je souhaiterais présenter succinctement notre activité. Avec plus de quatorze millions d'abonnés, le groupe *Free* est le troisième opérateur français. Notre offre est majoritairement destinée au marché grand public. Cependant, nous sommes également un opérateur d'infrastructures et de services Internet. Nous disposons à ce titre de 15 000 m² de *data centers*. Ces centres permettent aux OIV d'externaliser l'hébergement de leurs données. Par le passé, nous avons constaté que la localisation des données constituait une question centrale. Au sein de notre secteur d'activité, nous devons y apporter une réponse collective.

Le fondateur de *Free* en est l'actionnaire majoritaire et les collaborateurs sont intéressés aux résultats du groupe, ce qui nous distingue d'autres sociétés davantage internationalisées. Nous veillons à partager de manière équitable les gains de productivité entre les collaborateurs, les abonnés et les actionnaires, qui constituent trois groupes d'acteurs clés pour tout opérateur.

Le numérique est un domaine où il faut faire preuve d'agilité, ce qui nous est d'une grande utilité en matière de cybersécurité. Il ne se passe pas un jour sans que nous soyons, individuellement ou collectivement, la cible d'une tentative d'intrusion. Pour autant, **nous n'avons jamais eu à déplorer de perte de maîtrise du système, d'intégrité du réseau ou de confidentialité des données**. Il faut néanmoins garder à l'esprit que le risque zéro n'existe pas. Un réseau est fréquemment confronté à des difficultés qui lui permettent toutefois de gagner en compétences et en efficacité. Sur un marché grand public, il faut vivre avec l'idée que le pire peut toujours arriver. Nous devons nous protéger mais également réagir rapidement afin de détecter, d'analyser et de corriger les problèmes. **La capacité de réaction importe plus que tout.** C'est une chance que la France ait été précurseur en matière de sécurité numérique.

Quelle conception avons-nous du risque numérique ?

Nous considérons qu'il faut, pour être réactif, **disposer d'une organisation agile**, calquée sur les entreprises de l'économique numérique, où les cycles de décision sont courts et où les dirigeants et les collaborateurs sont impliqués et pragmatiques. Il importe également de **tenir compte des risques avec réalisme**. Les jeunes générations, qui sont nées à l'ère du numérique, constituent un talent dont les entreprises françaises ne sauraient se priver. Il convient enfin d'**opter pour « *une protection dans la profondeur* », soit un système de défense organisé autour de cercles concentriques de plus en plus sécurisés**. Au niveau de chaque cercle, les problèmes doivent être détectés, analysés et corrigés. Nous devons **être dans un état de « *paranoïa raisonnable* »**, c'est-à-dire qu'il nous faut nous astreindre à une vigilance permanente, où tout risque de relâchement – dû notamment à la croyance en une technologie miracle –, est prohibé.

Le second élément majeur est l'internationalisation des compétences stratégiques. La cybersécurité, préventive ou défensive, doit faire partie de la vie de l'entreprise ; et, ce, de la conception à la commercialisation de l'offre de biens ou de services. **Cette attention accordée aux compétences est le seul moyen pour les entreprises de demeurer souveraines dans la mesure où les technologies sources ne sont plus fabriquées en France.**

Mme Anne-Yvonne Le Dain. – Comment procédez-vous juridiquement en cas de problème ? Auprès de qui et selon quelles modalités, vos contrats sont-ils passés ?

M. Alexandre Archambault. – Pour le système *Freebox*, nous tâchons de réaliser en interne tout ce qui peut l'être : nous concevons le *hard*, nous sélectionnons le système d'approvisionnement et nous maîtrisons le *soft*. Les infrastructures de réseaux, tels que les routeurs ou les solutions mobiles, posent davantage de difficultés. Un dialogue exigeant avec les équipementiers nous permet d'accéder au *soft* et d'exclure toute infogérance. En d'autres termes, **nous achetons les équipements mais maîtrisons les réseaux** après une formation éventuelle du personnel. Ces éléments ont présidé au choix de notre équipementier mobile. **L'affaire Snowden a conduit à une prise de conscience sur la nécessité de limiter le recours à l'infogérance et de stocker les données sensibles en interne.**

Mme Anne-Yvonne Le Dain. – Quant au CEA, monsieur Lionel Darasse, le groupe gère-t-il tout lui-même en interne ?

M. Lionel Darasse. – Je souscris à ce qui vient d'être dit sur la nécessité de se doter de capacités de gestion en interne afin de conserver le contrôle du système d'information. La maîtrise du matériel étant généralement faible, notamment en cas d'externalisation, l'entreprise doit utiliser son organisation, sa structure et son administration comme des leviers d'action. Le CEA a fait le choix de s'approprier son système d'information de cette manière.

M. Alexandre Archambault. – Cela n'empêche pas de recourir à des prestations externes comme le conseil. La prise de décision doit cependant demeurer en interne. Pour gérer une entreprise de manière éclairée, il convient d'avoir une connaissance approfondie des produits commercialisés et des difficultés rencontrées.

Afin de renforcer la motivation des collaborateurs, le plus efficace est de les sensibiliser au risque numérique et de les intéresser à la bonne marche de l'entreprise. La résistance au changement est humaine. Cependant, lorsqu'un collaborateur se rend compte que son relâchement peut avoir des conséquences, y compris financières, il tend à respecter les règles de bonne hygiène informatique.

Le système *Freebox* a été développé en interne car les solutions présentes sur le marché ne répondaient pas à nos attentes. Cela nous a permis de devenir, en quelque sorte, notre propre équipementier. Notre maîtrise du *soft* comme du *hard* nous permet de réagir rapidement lorsqu'une difficulté est rapportée.

En ce qui concerne les routeurs et les solutions mobiles, notre marge d'action est contrainte par les équipementiers. Le cadre juridique existant nous permet de **soumettre les équipementiers à des obligations de sécurité spécifiques**. Les équipementiers européens ont compris qu'il leur fallait faire preuve de davantage de compétence, d'indépendance et de coopération, afin de conserver leurs parts de marché. Depuis la création de la CNIL en 1978, la France est devenue une référence européenne en matière de protection des données personnelles. Elle est également précurseur pour la sécurité des systèmes d'information, le rôle de l'ANSSI devant être souligné. En tant qu'opérateur, il ne nous faut pas introduire de la rigidité, et donc de la vulnérabilité, dans notre réseau. Un point mérite d'être signalé : grâce à un dialogue fructueux entre l'ANSSI et les professionnels du secteur, **les réseaux français de troisième génération (3G) et de quatrième génération (4G) ont un degré de sécurité supérieur aux normes définies par le *Third Generation Partnership Project* (3GPP)**.

Sur un plan prospectif, il importe de passer d'un objectif de sensibilisation du personnel à un objectif de conduite du changement, en association avec les organisations professionnelles concernées. Les PME et les collectivités locales sont les parents pauvres de la sécurité numérique.

Quelles propositions souhaitons-nous soumettre au décideur public ?

En premier lieu, il est important de **ne pas multiplier les lois**, dont les décrets d'application sont parfois pris de manière tardive. **Le cadre juridique actuel est suffisamment outillé pour nous permettre de faire face risque numérique. Les acteurs privés et les autorités régaliennes devraient coopérer davantage, au moyen de plates-formes d'échange.** À titre d'illustration, dans notre secteur d'activité, une entreprise a été confrontée il

y a peu à une tentative de chantage. Le vendredi soir, l'entreprise a alerté l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC). Dans la nuit de vendredi à samedi, l'OCLCTIC a saisi le procureur qui a formulé une demande de coopération internationale. Dès le lundi, le maître chanteur a été interpellé. Les outils juridiques sont d'ores et déjà disponibles. L'action de l'État est efficace dès lors qu'il existe une bonne connaissance du risque numérique, une relation de confiance avec les acteurs privés et une coopération interministérielle et internationale. À nouveau, la réactivité est un élément central en matière de cybersécurité.

En second lieu, il est nécessaire de **développer une culture du numérique au sein de la sphère politique et administrative**. Des initiatives, telle que la table ronde qui nous réunit aujourd'hui, peuvent permettre une diffusion de l'information et une montée en compétences. La proposition de M. Tariq Krim de **doter l'État d'un « *CTO* numérique » *(CTO : Chief Technology Officer)*, c'est-à-dire d'une direction technique consacrée aux enjeux numériques et ayant autorité sur les différentes administrations**, mérite d'être étudiée.

L'on ne saurait que trop insister sur la nécessité d'**inclure une sensibilisation au risque numérique dans la formation initiale et continue des avocats et des magistrats.** Mme Myriam Quemener, magistrat spécialisé en cybercriminalité, porte une proposition en ce sens. Il reste à évaluer l'opportunité de créer un pôle consacré à la cybercriminalité au sein ministère de la justice comme cela est déjà le cas pour la délinquance financière ou le terrorisme. Sur ce point, la mise en place d'une division consacrée à la cybercriminalité auprès de la Police judiciaire ne peut qu'être saluée.

En troisième lieu, il est souhaitable de **disposer, au sein de l'appareil d'État, d'une organisation permettant un traitement fluide des cas de cybercriminalité. Il est choquant que certains décrets d'application de la loi de confiance dans l'économie numérique, dont on va célébrer les dix ans, n'aient toujours pas été pris**, par exemple en ce qui concerne le périmètre des données de connexion devant être conservées par les fournisseurs de services. Si ces acteurs ne savent pas quelles données doivent être conservées, alors toute la chaîne de traitement est viciée en cas d'enquête.

En dernier lieu, il convient de **pérenniser la Plate-forme nationale d'interceptions judiciaires (PNIJ)**. Cette structure du ministère de la Justice permettra la dématérialisation des réquisitions relatives à la sécurité numérique. La dématérialisation permet à l'État de renforcer sa sécurité, son efficacité et sa célérité. En outre, elle lui offre un moyen de mieux maîtriser ses coûts de fonctionnement.

Pour élargir notre propos, sans doute nous faut-il **apprendre à vivre avec le risque**. D'autres pays, comme l'Allemagne et les États-Unis

d'Amérique, ont cessé de diaboliser la figure du *hacker*. Il ne doit pas être assimilé à un pirate mais plutôt à un lanceur d'alerte qui permet de révéler à l'entreprise les défaillances de son système d'information. La plupart des grands succès du numérique sont le fait d'anciens *hackers*. **Le *hacking* peut constituer un outil de formation complémentaire**, utile pour faire face aux attaques, de plus en plus sophistiquées, des officines paraétatiques.

M. Bruno Sido. – Dans la mesure où *Free* est tributaire d'*Orange* en matière d'itinérance, la sécurité de votre système d'information ne dépend-elle pas de cette société ?

M. Alexandre Archambault. – L'itinérance concerne la couverture de bas niveau comme la radio. Dès que la couverture est plus sophistiquée, elle est assurée par *Free*. Cette situation nous oblige à rendre compatibles deux systèmes d'information et deux solutions d'équipementiers différents. Le développement d'une passerelle d'intermédiation y contribue.

Il existe une forte interdépendance entre les entreprises de télécommunication. Les responsables des systèmes d'information sont pragmatiques et partagent rapidement toute information en cas de risque avéré, en veillant toutefois à maintenir une muraille de Chine avec les services commerciaux.

M. Bruno Sido. – Quels sont les textes législatifs dont nous attendons encore les décrets d'application ?

M. Alexandre Archambault. – Je citerai tout d'abord le texte relatif aux **données devant être conservées par les opérateurs de services**. Dans l'ignorance de ce qui doit être gardé, certains se fondent sur des usages, comme les *Requests for Comments* (*RFC*), tandis que d'autres choisissent de ne rien faire.

Je mentionnerais également le texte afférent au blocage. Selon nous, le blocage ne doit être envisagé qu'en dernier recours, c'est-à-dire si l'éditeur, l'hébergeur et l'opérateur ne répondent plus. Le législateur a limité le recours au blocage aux comportements manifestement illicites. Cependant, **en matière de pédopornographie ou de terrorisme, le texte d'application est toujours en attente**. Si *Free* se conforme dès à présent à ses obligations légales, il demeure difficile de mobiliser certains acteurs en l'absence des décrets d'application. Dans certains cas, le blocage peut créer plus de problèmes que de solutions : au mieux, il participe à la dissémination des contenus ; au pire, il complique les tâches des enquêteurs. En effet, **le blocage ne pouvant pas être modulé, il entraîne la coupure des réseaux de filature des enquêteurs**.

M. Bruno Sido. – Je vous remercie de votre intervention. Je passe la parole à M. Christian Daviot.

M. Christian Daviot, chargé de la stratégie auprès du directeur général, Agence nationale de la sécurité des systèmes d'information (ANSSI). – Je vous remercie, monsieur le président.

Je souhaiterais apporter des éléments de nature différente de ceux développés précédemment. L'ANSSI s'intéresse, non seulement à l'économie du numérique, mais également à la place du numérique dans l'économie : il s'agit, d'une part, de promouvoir notre tissu industriel et, d'autre part, de sécuriser les objets connectés. Cinquante milliards d'objets connectés pourraient être mis en circulation avant 2050. Cet enjeu, jusqu'à présent peu évoqué, constitue une préoccupation majeure pour l'ANSSI.

L'affaire Snowden a révélé un problème de communication en notre sein : **les ingénieurs, les hommes politiques et le personnel administratif se parlent trop peu**. Ces difficultés d'échange et de compréhension me semblent depuis lors avoir été dépassées. Cette affaire a également participé à la prolifération des capacités techniques américaines. Aussi le risque numérique devrait-il augmenter à l'avenir.

Le coût de la sécurité est moindre que celui de l'insécurité. Chaque année en France, l'insécurité informatique est à l'origine de la perte de centaines voire de dizaines de milliers d'emplois. Il est nécessaire que cette problématique fasse l'objet d'une étude plus précise. Si les attaques des administrations nuisent à notre souveraineté, celles des entreprises pénalisent notre compétitivité. À mon sens, les conséquences de l'insécurité informatique sur l'emploi ne sont pas suffisamment mises en avant. La cybersécurité est une composante de la compétitivité de notre économie et la condition du maintien de l'emploi en France.

L'ANSSI ne peut pas rendre publics les exemples d'attaque informatique. En 2010, le ministère des finances avait reconnu avoir fait l'objet d'une intrusion. Beaucoup de cas mériteraient d'être communiqués, non au grand public mais aux professionnels. À titre d'illustration, au Royaume-Uni, le Premier ministre, David Cameron, a réuni les principaux acteurs économiques britanniques au sujet des attaques informatiques. Cela a permis de mobiliser les dirigeants d'entreprises, de renforcer la cybersécurité et de développer le tissu industriel. Les entreprises britanniques ont une compétence supérieure aux nôtres pour certaines prestations de service développées plus précocement, comme la détection des attaques informatiques.

La communication peut également être renforcée en matière de sécurité numérique. La première intervention à ce sujet a été réalisée, le 20 février 2014, par le Premier ministre, Jean-Marc Ayrault. Si tous les gouvernements ont veillé à ce que l'ANSSI dispose des moyens financiers et humains pour exercer ses compétences, la parole publique pourrait être davantage utilisée. À cet égard, il faut saluer les rapports parlementaires rédigés respectivement par M. Jean-Marie Bockel, sénateur, et, plus récemment, par Mmes Corinne Ehrel et Axelle Lemaire, députées.

M. Bruno Sido. – Toute entreprise est susceptible d'être attaquée. Des systèmes de détection automatiques sont-ils à l'étude ? La sécurité progresse-t-elle plus vite que la menace ou assiste-on à une course sans fin entre ces dernières ?

M. Alexandre Archambault. – Il existera toujours une course sans fin. Cependant, on observe une **réduction de l'écart entre la menace et la sécurité**. Dans certains cas, l'agression peut même être anticipée, grâce à des *scenarii* et à des exercices.

La technique évolue en permanence. **Il existe des règles de bonne hygiène, qui permettent de répondre de manière quasi automatisée aux attaques les plus simples.** Toutefois, l'automatisation ne doit pas conduire à un relâchement des comportements. Les machines détectant bien les anomalies mais analysant mal les situations, les moyens humains demeurent indispensables.

M. Bruno Sido. – Il arrive que des entreprises détectent l'attaque des années après sa survenue. Une marge de progression existe-elle ? Comment réagissez-vous face à ces enjeux ? Si l'hygiène numérique est une bonne chose, est-elle suffisante ? Un système de détection automatique est-il envisageable ou utopique ?

M. Christian Daviot. – Nous pouvons penser qu'il s'agit là d'une utopie et que **l'agresseur aura toujours une longueur d'avance**.

Nous sommes actuellement confrontés à des problèmes simples : *primo*, on ne trouve que ce que l'on cherche ; *secundo*, lorsque l'on détecte une attaque, c'est que cette dernière a déjà réussi ; *tertio*, **les équipements de détection d'attaque informatique ne sont pas souverains**.

Il existe un État dominant en matière d'équipements de détection. Il est donc nécessaire de **développer à notre tour des outils de détection** afin de faire face à d'éventuelles attaques venues de ce pays. **Le Programme d'investissements d'avenir a mis à la disposition des équipementiers français les fonds nécessaires.**

M. Bruno Sido. – Nous n'avons pas employé, au cours de notre table ronde, l'expression de « guerre » informatique. La législation permet-elle une action offensive contre un agresseur ?

M. Christian Daviot. – L'article 21 de la loi de programmation militaire permet, en cas d'attaque d'un système d'information critique, de pénétrer le système d'information adverse pour caractériser l'attaque et en neutraliser les effets. **N'est légale que l'action défensive.**

Comme l'a rappelé le Livre blanc sur la défense et la sécurité nationale de 2013, **la France a annoncé se doter de capacité offensive en 2008**.

M. Jean-Jacques Tourre. – Je souhaiterais souligner que ces enjeux régaliens ne concernent en rien les entreprises privées, comme le groupe *Total*.

M. Bruno Sido. – Il s'agit en effet de sujets régaliens. Il me semble que les moyens de détection et de réaction sont, à eux seuls, insuffisants.

M. Christian Daviot. – L'ANSSI n'a qu'une action de défense.

M. Lionel Darasse. – En cas d'attaque, le fait d'intervenir sur un canal de contrôle commande, qui aurait été établi par les agresseurs pour prendre la main sur un poste, est une manière de se signaler. Avant de procéder à toute riposte, il convient d'en évaluer les conséquences. L'exploitation ou la coupure du réseau demeurent justifiées dans certaines circonstances.

Quant à votre question sur les progrès technologiques réalisés, je crois qu'il existera toujours une course sans fin en matière de sécurité numérique. **Cependant, il n'est pas possible de s'affranchir d'un niveau de sécurité minimal, qui correspond aux critères d'hygiène informatique définis par l'ANSSI.** Le CEA s'intéresse actuellement à la problématique de la supervision et à la technique de la métrologie.

Enfin, **le système d'information doit disposer d'une structure d'administration à même de le préserver de toute réaction en chaîne en cas d'agression**. Il faut en effet circonscrire l'attaque et limiter la propagation latérale et les éléments de privilège. Cette réflexion constitue une modeste réponse à la course sans fin observée.

M. Jean-Jacques Tourre. – Nous avons assisté ces dernières années au **passage d'une logique de protection à une logique de détection et de réaction**. Beaucoup de travail et de progrès ont été réalisés à ce sujet.

Pour en revenir à la question de l'automatisation, je souhaiterais y répondre en prenant le cas du service de supervision et de sécurité du groupe *Total*. Si nous nous appuyons sur des algorithmes, compte tenu du volume très important de données à traiter, **la dimension humaine reste primordiale pour détecter et analyser les problèmes**. La gestion des compétences est de ce fait un maillon important de notre système de sécurité.

M. Christian Daviot. – L'article 22 de la loi de programmation militaire dispose que le Premier ministre peut imposer des règles techniques aux opérateurs d'importance vitale (OIV). Le décret d'application sera pris cet automne et les arrêtés à partir de la fin de l'année. Un travail collaboratif a été engagé avec les OIV, qui permettra d'améliorer la sécurité de leurs systèmes d'information. Au-delà de l'enjeu de la détection, le renforcement de la prévention et de la résilience est en cours.

M. Bruno Sido. – Observez-vous des anomalies dans notre législation, qui pourraient être corrigées ?

M. Alexandre Archambault. – De manière générale, **le cadre législatif me semble suffisamment outillé, cependant, il demeure trop focalisé sur les OIV, les grands comptes et les grandes administrations. La sécurité des systèmes d'information concerne toutes les couches de la société, notamment les sous-traitants, les PME et les collectivités territoriales.**

M. Christian Daviot. – La loi de programmation militaire cible les OIV car **il n'existe pas de liste d'entreprises à protéger clairement définie en droit français**. L'idée est bien d'étendre ces dispositions aux entreprises relevant du potentiel scientifique et technique, dont les entreprises innovantes. Sur ce point, nous pensons que **les assureurs auront un rôle à jouer**.

Bien que cette mesure soit d'ordre réglementaire, **l'impossibilité pour les salariés d'un OIV de savoir que son entreprise est classée comme telle est problématique**. Je pense que **l'on pourrait rendre publique la liste des OIV ou, à tout le moins, informer les seuls salariés des OIV**. Ils sauraient ainsi que les mesures de sécurité qui leur sont imposées ont un sens et une justification : la protection des intérêts de la nation.

M. Bruno Sido. – Il s'agit d'une question de citoyenneté. Ne craigniez-vous pas cependant que la publication de la liste des OIV ne donne aux attaquants des cibles nommément désignées ?

M. Christian Daviot. – Il faut peut-être sortir de la logique, issue de la Guerre froide et aujourd'hui périmée, qui consistait à cacher les objectifs. Il n'est peut-être pas bon de publier la liste des OIV dans son intégralité. Cependant, **l'opportunité de lever l'interdiction sanctionnée pénalement, pour un chef d'entreprise, de révéler la qualité d'OIV de son établissement, reste à évaluer**. Un tel assouplissement faciliterait les choses, y compris la mise en place des objectifs de la loi de programmation militaire.

M. Bruno Sido. – Je remercie chacun d'entre vous pour sa contribution et vous propose de poursuivre les dialogues entamés ce matin au cours de la table ronde de cet après-midi.

Introduction

M. Bruno Sido, sénateur, président de l'OPECST. – Dans le cadre du rapport sur le risque numérique et la sécurité des réseaux utilisés par les entreprises, lancé à la suite d'une saisine de la commission des affaires économiques du Sénat, il est apparu essentiel aux rapporteurs désignés par l'Office – Mme Anne-Yvonne Le Dain et moi-même – de focaliser l'étude sur les opérateurs d'importance vitale (OIV) et, parmi ceux-ci, sur deux catégories d'entre eux, ceux du secteur des télécoms et ceux du secteur de l'énergie.

Il ne nous a pas échappé que, au-delà des opérateurs d'importance vitale eux-mêmes, la sécurité des réseaux numériques qu'ils utilisent devait s'étendre à ceux utilisés par leurs sous-traitants, voire leurs clients.

Cette sécurité de haut niveau ne se met pas en place du jour au lendemain. Elle suppose des personnels dotés d'une culture de sécurité et des matériels fiables, incluant des dispositifs au sein d'une architecture de systèmes dont les failles éventuelles doivent être très rapidement repérées et réparées au fur et à mesure de leur découverte.

À ce jour, les rapporteurs que nous sommes ont effectué environ quatre-vingts auditions comprenant des visites de sites. Ce matin, une audition en forme de table ronde a déjà été tenue pour entendre des opérateurs d'importance vitale des secteurs des télécommunications et de l'énergie tandis que la table ronde de cet après-midi sera tournée vers l'écoute des solutions de sécurité qui peuvent être proposés par chacun d'entre vous. Ces deux tables rondes marqueront quasiment le terme de cette phase de nos travaux. Lors du déjeuner, nous avons déjà eu l'occasion d'échanger avec les participants des deux tables rondes sur nombre d'aspects de la sécurité numérique.

Au cours de cet après-midi, chacun d'entre vous disposera d'une dizaine de minutes pour une intervention sur le cœur de la problématique à laquelle se trouvent confrontés les fournisseurs de solutions de sécurité des réseaux numériques lorsqu'il s'agit d'assurer, en toute circonstance, la sécurité numérique des opérateurs d'importance vitale. Les situations de crise seront bien évidemment évoquées.

Il est possible que, au fur et à mesure de l'après-midi, vos interventions soient interrompues par les questions des rapporteurs ou pour demander à un autre intervenant de réagir à chaud à un propos tenu.

Jusqu'à présent, les auditions collectives que nous avons organisées se tenaient sous forme d'auditions publiques ouvertes à la presse et à tous les membres de l'Office parlementaire. Cet après-midi, comme ce matin, compte tenu du caractère sensible des questions évoquées et pour permettre un dialogue aussi ouvert que possible entre nous, nous avons retenu le principe d'une audition collective limitée aux rapporteurs.

Nous n'y avons convié ni le public ni la presse. Un compte rendu sera simplement établi et vous sera soumis. Nous verrons ensemble par la suite s'il doit donner lieu, ou non, à une publication. Je précise cela afin de vous encourager à vous exprimer de la manière la plus directe possible, avec une grande liberté de ton.

Je vous remercie vivement d'avoir bien voulu aider les rapporteurs dans leurs travaux et d'avoir accepté de participer à tout ou partie de cette journée. À l'intention de ceux qui n'ont pu se libérer assez tôt pour participer au déjeuner, je précise qu'il sera encore possible d'échanger au cours des trois prochains mois et de nous adresser tous les documents que vous jugerez utiles pour nos travaux, puisque nous comptons terminer notre rapport à l'automne.

Mme Anne-Yvonne Le Dain, députée, vice-présidente de l'OPECST. – Nous sommes ici, le sénateur Bruno Sido et moi-même, pour vous écouter et éventuellement interagir, c'est-à-dire pour vous faire part d'opinions, d'ambitions mais aussi parfois d'échos qu'il nous arrive de recevoir dans l'univers qui est le nôtre – qui n'est pas seulement de politique nationale car nous sommes tous élus sur des territoires où nous rencontrons de nombreuses personnes.

Le monde du numérique évolue très vite, techniquement mais aussi en termes de positionnement européen, international, en fonction de la stratégie, de l'évolution des matériels et de la perception qu'ont les uns et les autres des possibilités qu'offre cette technique. En outre, nous devons prendre en considération ces évolutions sur l'ensemble du territoire national dans les mondes métropolitains, villageois, ruraux, banlieusards – j'emploie à dessein le terme quotidien de « banlieusards » car la banlieue existe et ne revêt pas forcément une apparence dramatique.

Nous sommes dans l'économie du XXIe siècle et partons du principe selon lequel nous ne devons pas envisager seulement la question sous l'angle du risque et de l'incertitude : il faut aussi l'envisager dans une logique de projet et d'avenir. Sommes-nous dans une impasse subie ou sur une autoroute qui peut nous emmener vers un futur qui n'est pas nécessairement compliqué ?

Table ronde

M. Stanislas de Maupeou, directeur du secteur conseil en sécurité et évaluation, *Thales*. – Je tiens à vous remercier de me donner l'occasion de m'exprimer devant l'Office parlementaire sur un sujet qui nous anime tous autour de la table. Je n'avais pas prévu de débuter ainsi mais je serais tenté de dire, en écho à vos mots introductifs, que nous n'avons pas le choix. Nous sommes dans la société de l'information et il ne faut pas attendre la crise majeure qui risque de survenir. Nous devons prendre le sujet à bras-le-corps.

Les deux dernières éditions du Livre blanc ont mis en exergue le sujet qui nous réunit mais nous semblons avoir du mal, collectivement, à passer à l'acte. Nous sommes encore dans le besoin de pédagogie. Beaucoup de choses ont été dites et de nombreuses auditions ont eu lieu. Il faut maintenant franchir le pas pour aborder une nouvelle étape, marquée par une vision industrielle.

Je voudrais m'attacher, au cours de ces dix minutes, à souligner que le cyberespace est aujourd'hui une réalité de la société de l'information. Le rapport de MM. Collin et Colin, produit pour le ministère des finances, montre l'impact de la société de l'information dans l'économie. C'est à cette aune que doit être apprécié l'impact d'une cyberattaque éventuelle, en tenant compte de la dépendance de notre société, d'une façon générale, aux outils numériques. Il s'agit d'un espace risqué, contesté et proliférant. Je reviendrai brièvement sur ces trois notions dans mon propos.

Nous savons tous que diverses menaces nous environnent (espionnage, déstabilisation, voire la destruction, dans le cas d'opérations de sabotages). Nous n'en sommes plus, comme il y a quelques années, à expliquer que cela pourrait se passer. **Du seul fait que l'on travaille avec l'informatique, aucune entreprise du CAC 40 ni aucun espace gouvernemental n'échappe aujourd'hui à ces attaques.** Cette dépendance de nos organisations industrielles et étatiques vis-à-vis des systèmes informatiques, plus largement la dépendance de l'économie vis-à-vis de la société de l'information, me semble encore un sujet sous-estimé. Ce type d'initiative montre bien **la dépendance de nos sociétés aux outils numériques et informatique**s, avec une dimension générationnelle intéressante dans le phénomène car, si ces outils sont utilitaires pour ma génération, ils sont identitaires pour ceux qui ont aujourd'hui moins de vingt-cinq ans. Je crois que cette dépendance est sous-estimée. J'ai eu l'occasion d'aider des grands comptes dans la résolution d'attaques informatiques. Très vite, cela devient le sujet de la société et non celui d'un expert technique. Nous pourrions aisément transposer ce constat au plan sociétal.

Un deuxième sujet me semble extrêmement important. Nous le vivons en tant qu'industriels puisque nous opérons la supervision de sécurité de grands comptes dans l'espace privé et dans l'espace public.

Globalement, les technologies et les architectures sont assez communes, ne serait-ce que la formation des ingénieurs.

Je ne vois **pas de grande différence entre le réseau informatique d'une entreprise et celui d'un ministère. Nous ne sommes pas là dans l'apanage du monde de la défense.**

Ce *continuum* doit aussi être envisagé dans un monde globalisé. **Une attaque de nature terroriste ou venant d'un État pourrait passer par des biais qui ne sont pas militaires** au sens traditionnel du terme. À l'inverse, les systèmes militaires dépendent aussi de plus en plus des systèmes informatiques. Il existe donc un *continuum* extrêmement fort qui est la conséquence directe de l'interconnexion des réseaux. On sous-estime les effets de ces interconnexions nécessaires mais qui constituent autant de chemins d'attaque potentiels.

Depuis les deux dernières éditions du Livre blanc et, de façon plus ouverte encore, nous ne sommes plus, du côté des entreprises, dans un scénario de crise potentielle : il s'agit d'une réalité opérationnelle qu'il faut désormais prendre en compte. Cette problématique n'est pas suffisamment bien comprise. La population des responsables de la sécurité des systèmes informatiques (RSSI) n'est peut-être pas inscrite de façon suffisamment identifiée dans les parcours professionnels. On peut le comprendre au regard de la « jeunesse » du sujet mais il est difficile de le comprendre lorsqu'on mesure l'impact d'une attaque sur une entreprise.

Dans le champ économique, on observe depuis quelques semaines en France une structuration du marché, à la faveur de différentes acquisitions dont la presse s'est faite l'écho. Je voudrais qu'on réalise que ces événements sont microscopiques au regard des restructurations qu'on observe dans le monde anglo-saxon, où toutes les restructurations les plus significatives du marché dépassent le milliard de dollars, ce qui traduit une échelle différente de ce qu'on observe en France et plus largement en Europe. L'hyperpuissance s'applique de façon très significative à ce monde de la sécurité. J'y vois un risque au regard de l'ambition de l'ANSSI dans la stratégie nationale de cyberdéfense définie en février 2011, annonçant la volonté de faire de la France une puissance mondiale de cyberdéfense. C'est un véritable défi pour notre pays.

Je pense que **nous sommes là au cœur de l'autonomie stratégique de la France et même de l'Europe en termes de capacité à développer une capacité de renseignement et à conserver une maîtrise académique et technologique**. Quelle est notre réelle maîtrise académique et industrielle d'une chaîne de production informatique ? Je pense qu'il s'agit d'un des grands sujets aujourd'hui. Il doit être examiné à l'aune de la souveraineté dans un contexte économique extrêmement contraint. La cybersécurité n'est pas seulement un sujet technique. On ne pourra inspirer confiance dans les systèmes d'information sans une connaissance des métiers et de leur environnement. Nous voyons d'ailleurs, au travers de nos contacts avec les

entreprises, que les choses bougent de ce point de vue. Les métiers commencent à comprendre l'impact que pourrait avoir sur eux une attaque informatique.

Enfin, nous n'avons pas le choix : **pour faire face aux attaques informatiques, l'État doit coopérer avec les industriels et ceux-ci doivent coopérer avec l'État et entre eux**. Une attaque ne pourra se résoudre seule. Nous avons besoin de coopération. Nous avons aussi besoin, en tant qu'industriels, d'une direction. Il me semble fondamental, pour orienter nos investissements, d'**avoir une visibilité sur la stratégie nationale de cybersécurité à plus long terme pour pouvoir mettre en œuvre une politique d'investissement qui corresponde à des enjeux de sécurité**. Le marché est en train de se structurer et le passage à l'acte doit advenir pour aboutir à une feuille de route technique et stratégique.

Mme Anne-Yvonne Le Dain. – Qu'entendez-vous par le terme de feuille de route technique et stratégique ? Faut-il qu'on oblige toutes les entreprises à se doter d'un système de sécurité ?

M. Stanislas de Maupeou. – À titre d'exemple, dans le cadre du Programme d'investissements d'avenir, l'État définit des objectifs et veut par exemple se doter, dans un horizon de trois à cinq ans, d'une **sonde de détection d'intrusion** qui soit maîtrisée. Il s'agit d'une sonde souveraine. L'État impulse ainsi une orientation vis-à-vis des industriels en affirmant un objectif clair. Aujourd'hui, en réalité, la quasi-totalité des outils de détection d'attaques informatiques ne sont pas maîtrisés, sur le plan technologique, par la France. Cet objectif constitue un élément de cette feuille route. Nous devons étendre ce travail de prospective pour pouvoir orienter les investissements des entreprises. Le plan des investissements d'avenir va dans le bon sens de ce point de vue. Il faut multiplier les initiatives de ce type dans la durée.

Je ne sais pas si vous percevez le retard qu'a la France dans ce domaine. **Le domaine de la cryptographie est parfaitement maitrisé académiquement et techniquement. Pour le reste, toute la chaîne (*hardware* et *software*) n'est pas suffisamment maîtrisée par la Nation.** Nous avons besoin de sentir que ce problème est bien compris et que l'État impulse une direction pour l'avenir et pour l'ensemble des acteurs privés.

M. Bruno Sido. – Nous allons maintenant entendre M. Lionel Gervais, directeur de la stratégie, chez *Airbus*.

Lionel Gervais, directeur de la stratégie, *Airbus Defence & Space - CyberSecurity*. – L'entité *Cyber Security* d'*Airbus Defense and Space* est européenne, même si elle a des racines françaises. Ce n'est pas anodin, après les propos de M. Stanislas de Maupeou qui ont bien exprimé le besoin de notre industrie de s'asseoir sur un marché important. Nous sommes confrontés à une compétition américaine, en particulier, et monter en puissance dans cet écosystème impose que notre marché ait une taille

critique minimale. L'entité d'*Airbus Defense and Space* réunit environ **six cents experts en cybersécurité** dans trois pays principaux, la France, l'Allemagne et le Royaume-Uni. L'entreprise s'adresse en particulier au secteur public (gouvernement et défense) mais aussi aux grandes entreprises nationales et européennes.

Nous couvrons toutes les dimensions nécessaires pour répondre aux besoins clés des clients en matière de cybersécurité, de l'anticipation à l'information de nos clients sur l'actualité de la menace : nous récupérons des informations par le biais de nos propres outils ou auprès de nos partenaires et, en nous appuyant sur notre expérience, cela nous permet d'informer nos clients suffisamment tôt. Il s'agit d'un aspect important car, jusqu'à présent, notre devoir de fourniture d'informations aux autorités nationales pour informer les acteurs nationaux a été rempli.

Nous couvrons aussi la protection dynamique et la supervision, vingt-quatre heures sur vingt-quatre et sept jours sur sept, depuis les trois pays concernés. Nous utilisons une base de données très importante afin de pouvoir **identifier, de façon quasiment instantanée, les attaques et réagir à des situations d'urgence**.

Dans des situations de ce type, nous envoyons des équipes d'experts pour travailler main dans la main avec les clients et corriger d'éventuels problèmes.

Au titre des principaux enjeux du risque numérique, je mentionnerai deux points qui me semblent essentiels, le besoin d'innovation et la sensibilisation des acteurs.

Le besoin d'innovation est critique pour faire évoluer les outils de défense que nous utilisons pour protéger nos clients, ce qui est notre mission principale. **La menace évolue extrêmement rapidement** et nous sommes confrontés quasiment toutes les semaines ou tous les mois à de nouveaux types d'attaques. Pour faire face à ce type de situation, il faut investir constamment et continuer de faire évoluer notre offre. Il nous est arrivé plusieurs fois par le passé, en travaillant avec des partenaires capables de fournir des solutions complémentaires de bon niveau, de se rendre compte que certains ratent un tournant technologique. Nous avons donc besoin d'une flexibilité particulière pour pouvoir contrer les problèmes éventuels. Cela nous oblige à tester de manière continue des solutions et des partenaires et à investir fortement en recherche et développement.

Nous investissons 20 % de notre chiffre d'affaires dans le développement de solutions pour protéger les clients en cybersécurité. Nous devons aussi attirer de nouveaux experts, ce qui est un problème français et européen. Les experts, sur ce marché, sont rares et de plus en plus chers.

Le besoin d'innovation est également important pour **construire une offre française et européenne, souveraine** sur certains points tout en se

démarquant, sur d'autres aspects, de la compétition internationale. Nous rencontrons des problèmes, comme ailleurs en Europe, du fait de la fragmentation de l'offre nationale, de la rareté des expertises et d'une capacité d'investissement limitée. Ce n'est pas seulement une question de rapport culturel au risque même si d'autres nations ont peut-être une moindre aversion au risque que la nôtre. C'est aussi parce que la période actuelle en Europe est un peu plus difficile. L'innovation est souvent présente, dans les entreprises que nous rencontrons mais la taille critique est rarement atteinte, ne leur permettant pas d'entrer dans la compétition internationale. C'est pour toutes ces raisons, que je pense qu'il faut constituer une filière française et européenne forte pour être présent sur ce marché.

La sensibilisation des acteurs, en particulier des dirigeants des entreprises, employés et comités exécutifs, constitue un autre axe de travail essentiel. L'ANSSI a œuvré en ce sens par le passé (et continuera certainement à le faire), en publiant notamment de nombreuses études pratiques et des recommandations (quarante règles d'hygiène, passeport du voyageur, etc.), qui offrent au moins un premier niveau de protection et de sensibilisation.

D'une manière générale, en France, la prise de conscience est croissante sur le sujet. Demeurent, toutefois, des **problèmes basiques, par exemple des personnes qui utilisent des clés *USB* ou qui installent des logiciels personnels sur leur poste de travail**. On est parfois surpris de devoir récupérer une situation délicate à cause de la négligence personnelle d'un employé. Il existe aussi des tendances nouvelles de l'*IT* comme le *cloud* ou l'utilisation du portable personnel à des fins professionnelles, qui interfèrent et rendent la tâche un peu plus compliquée. Cela demande des investissements supplémentaires. Il s'agit d'éléments spécifiques de la complexité du travail sur la cybersécurité. **Il n'est pas question de fermer un réseau ni de restreindre l'utilisation des solutions. Il faut anticiper les comportements à risque et fournir des solutions adaptées.**

Les efforts entrepris jusqu'à maintenant sont très positifs. Je pense notamment au plan de la Nouvelle France industrielle. Il reste cependant un écart entre la préconisation et la mise en œuvre.

La loi de programmation militaire (LPM) (notamment dans son article 22) sera certainement un élément très positif pour faire évoluer les choses. Les OIV auront à réfléchir aux implications de cette loi, qui devrait tout de même permettre de hausser sensiblement le niveau de protection de ces opérateurs avec probablement un impact positif sur la sécurité des partenaires et sous-traitants. Plus généralement, les recommandations à formuler pour les entreprises françaises sont assez évidentes à nos yeux.

Il s'agit d'abord de l'application des recommandations de l'ANSSI, de la sensibilisation des employés et des dirigeants, qui est cruciale. Il faut aussi **établir un état des lieux pour comprendre au moins l'exposition au**

risque. Après une mise à niveau de la protection périmétrique, il faut qu'il existe une **supervision permanente**, par exemple par un *SOC*. En cas d'attaque, il faut disposer d'un **contrat permettant d'intervenir sur place.** La question d'**une assurance « cyber »** se pose même à mes yeux car l'exposition au risque de sécurité informatique a des implications économiques qui peuvent être dramatiques pour toute entreprise. Tous les acteurs économiques sont protégés contre l'incendie mais ils ne le sont pas forcément contre une attaque informatique.

En résumé, s'agissant du travail en commun réalisé jusqu'à présent par les acteurs publics et privés, du moins en France et en Europe, la situation progresse. Il faudra continuer pour assurer une protection suffisante des entreprises et **créer une filière suffisamment forte en France** pour répondre à ces besoins.

Mme Anne-Yvonne Le Dain. – La question des assurances ouvre des perspectives considérables car un assureur assure plus volontiers par principe un risque moindre, ce qui permet de couvrir les drames. Comment aborderiez-vous cette question ?

M. Lionel Gervais. – L'assureur seul ne pourra, à l'évidence, estimer l'exposition au risque. Il a besoin de travailler avec un spécialiste pour comprendre la situation. On peut envisager de rechercher un minimum d'hygiène informatique en mettant en place une proposition permettant de confirmer que le client a réalisé un audit et dispose du niveau de protection suffisant pour son installation. Les assureurs ne disposent pas des statistiques permettant de comprendre tout à fait l'exposition au risque. En commençant par une coopération avec les spécialistes en cybersécurité pour bénéficier de leur expertise, une compagnie d'assurance devrait être capable d'estimer grossièrement une exposition et des impacts éventuels ainsi que la capacité de réaction d'un client. Des cas particuliers peuvent être extrêmes. Nous avons tous entendu parler de *Target*, avec des millions de clients impactés, la chute du cours de bourse et une perte de chiffre d'affaires importante. Pour un premier niveau d'hygiène, il est sans doute possible de trouver des solutions.

M. Bruno Sido. – Je donne maintenant la parole à M. Thierry Floriani.

M. Thierry Floriani, responsable de la sécurité des systèmes d'information, *Numergy*. – *Numergy* est une société qui fournit de l'informatique en nuage souveraine. La Caisse des dépôts et consignations est présente dans notre capital. Nous venons d'être agréés pour l'hébergement de données de santé. Si nos centres de données *(data centers)* sont remplis de données de santé et que notre société est rachetée par une société étrangère, on voit bien l'usage que celle-ci pourrait faire de ces données qui concernent des patients français. L'existence d'un contrôle et même d'une minorité de blocage, dans la constitution du capital de l'entreprise, l'État ayant voix au chapitre sur le sujet, paraît donc légitime.

Cela signifie aussi que **nos activités et les données elles-mêmes sont localisées sur le territoire français, sous le contrôle de la loi française**. Notre monde n'est pas si virtuel qu'on le dit parfois lorsqu'on traite de ces sujets. Il s'agit de lignes de machines, de centres de données et de consommation électrique. La France est plutôt bien positionnée de ce point de vue compte tenu du coût de l'énergie et de la disponibilité de locaux industriels ayant de fortes capacités et un prééquipement industriel. Nous récupérons ce type de locaux et nous les réhabilitons pour en faire des centres de données.

La souveraineté s'exprime aussi dans la maîtrise des outils logiciels nécessaires à la virtualisation des données. Le choix qui a été fait par notre entreprise vise à internaliser les ressources en constituant des équipes de développement assez importantes au regard de notre chiffre d'affaires et de notre taille (puisqu'elles représentent 60 % du personnel). Nous travaillons à partir de **logiciels libres** et contribuons au développement et à la maîtrise de ces outils par la participation à des instances de pilotage de ces logiciels libres. En effet, **il est important, dans la cyberdéfense, de pouvoir modifier l'outil de production pour réagir à des évolutions de la menace**. Nous ne sommes plus dans un contexte où des produits de confiance et une architecture robuste correctement administrée suffisaient à apporter un niveau minimum de sécurité. La menace évolue si vite que ce paradigme est rapidement mis en défaut. Il faut analyser la menace et réadapter l'outil au regard de cette menace. Sur les points sensibles, il faut donc maîtriser ces éléments. On pourra parler **de virtualisation, des pare-feu, des sondes de détection d'intrusion**.

Ce sont des éléments qu'il faut être capable de maîtriser en interne ou avec des partenaires de confiance, français dans la mesure du possible.

À l'évidence, **une partie des moyens que nous utilisons ne sont pas sous maîtrise française**. Je parle notamment des matériels informatiques qui sont extrêmement importants. Même si ces machines ne sont pas forcément piégées, il n'est pas sûr que les conditions commerciales qui nous sont faites soient les mêmes que celles faites à de grands concurrents américains (surtout si le fabricant est américain) et cela représente un coût non négligeable de la prestation.

En ce qui concerne le logiciel, **on a su y répondre en interne. Mais tout cela requiert l'atteinte d'un volume critique.** Nous investissons beaucoup en proportion du chiffre d'affaires que nous réalisons, ce qui est normal. Nos grands compétiteurs ont de l'avance et bénéficient d'un effet de masse qui joue en leur faveur. Or, en l'état, il faut aller vite. Nous avons rattrapé le retard technique et je n'ai pas d'état d'âme à ce sujet. La moyenne d'âge de nos collaborateurs est de trente-et-un ans et nos équipes sont performantes. Il faut cependant atteindre un effet de masse, en termes de volume, pour financer la recherche et prendre de l'avance. À titre d'exemple, il existe une association entre *Oracle* et *Microsoft* qui a investi trente-

six milliards de dollars pour faire du nuage numérique *(cloud)*. Cela ne veut pas dire que cet argent sera forcément bien utilisé. Mais il serait illusoire de croire qu'ils ne sauront pas en faire quelque chose.

Par ailleurs, les données ont une valeur que de nombreuses entreprises ne mesurent pas comme il se doit. Une entreprise comme *Facebook* investit 1,2 milliard de dollars dans un *data center* sans faire payer le client ; les ressources proviennent donc de l'exploitation des données des clients et de la publicité. Rien n'est gratuit sur Internet. Nous ne nous inscrivons pas dans cette logique et nous n'avons pas ce volet d'optimisation financière : les clients qui viennent chez nous paient le service que nous proposons. Cela dit, **nous respectons la loi française et n'exploitons pas les données de nos clients**.

Nous sommes « nuage souverain ». Des collègues étrangers, des groupes mafieux ont essayé de récupérer des données sensibles chez nous. Nous avons eu la chance d'avoir cette contrainte dès le démarrage de la société. Nous avons donc conçu la plate-forme pour résister et **nous sommes dotés d'un centre de supervision de la sécurité dont une partie des équipements sont américains** car il s'agissait des seules solutions disponibles. D'autres équipements sont fournis par des sociétés innovantes. Nous avons pris le risque de ces sociétés innovantes car c'était dans notre ADN de favoriser l'écosystème français. Néanmoins, certaines sociétés qui comptent vingt ou trente personnes et qui obtiennent de meilleurs résultats qu'un certain nombre de produits américains n'ont pas atteint le volume critique pour assurer leur survie.

Mme Anne-Yvonne Le Dain. – Le terme d'innovation est dans le vocabulaire politique depuis plus de vingt ans, avec la stratégie de Lisbonne puis le Traité de Lisbonne, à dix ans d'écart. L'innovation est le cœur du système mais j'ai l'impression qu'il s'agit là d'une « tarte à la crème » depuis vingt ans.

M. Thierry Floriani. – Je suis assez à l'aise pour répondre à votre question car je reviens de l'étranger, où j'ai passé cinq ans. J'étais parti avec une image de la France un peu pessimiste, « plan-plan ». Je suis revenu car mon contrat s'arrêtait et non parce que je l'avais décidé.

Lorsque j'ai relevé le défi d'assurer la sécurité des clients de *Numergy*, dans un nuage public, j'ai été amené à entrer en contact avec de nombreuses petites sociétés innovantes françaises que je trouve remarquables mais qui n'ont pas l'ingénierie financière dont peuvent jouir des sociétés américaines pour amener leurs produits au niveau de développement optimal, avec un volume d'activité permettant d'entretenir ce niveau de performance. Nous avons un programme de *start-up* et nous voyons de nombreuses sociétés innovantes, parfois avec trois ou quatre personnes bien qu'elles proposent un produit extrêmement intéressant. Pour un éditeur de logiciel, il faut compter six commerciaux pour un ingénieur qui produit le logiciel. Une société innovante qui a dix

développeurs ne peut se payer soixante commerciaux pour vendre son produit. Un fonctionnement en nuage avec des services associés peut constituer un levier intéressant car cela leur permet de toucher un plus grand nombre de clients plus rapidement. C'est d'ailleurs la raison pour laquelle ces sociétés viennent nous voir.

Nous avons en partie été financés par l'État pour démarrer et je ne compte pas « cracher dans la soupe ». Cela nous a permis de développer **une plate-forme technique qui est à la hauteur des grands du marché**. Il nous manque encore un peu de « customisation » mais nous sommes au niveau. L'enjeu consiste aujourd'hui à atteindre la masse critique pour s'auto-alimenter et parvenir à exister afin de se battre avec les plus grands. Je suis assez confiant. **Nous venons d'être agréés hébergeur de données de santé.** Cela représente un dossier de 1 310 pages et neuf mois d'attente. Nous travaillons avec l'ANSSI en vue d'obtenir une certification. Le temps a de l'importance car les mois qui s'écoulent représentent du chiffre d'affaires que nous ne réalisons pas. Dans le même temps, il faut payer nos ingénieurs et leur donner de quoi monter en puissance rapidement. Or le temps ne joue pas en notre faveur. Nous allons vite mais nous avons conscience qu'il faudrait aller encore plus vite.

Mme Anne-Yvonne Le Dain. – L'idée selon laquelle « le temps, c'est de l'argent » est vieille comme le monde. Pourquoi cela va-t-il moins vite ici ? Y a-t-il vraiment beaucoup plus d'argent aux États-Unis ? En France et en Europe, on a l'impression que le système financier nous dit « ce n'est pas notre affaire » et ne veut pas prendre de risque.

M. Thierry Floriani. – L'État a accompli sa part en investissant dans le démarrage de sociétés comme la nôtre pour leur permettre d'exister. Pour le reste, je vais prendre l'exemple d'*Amazon*. **Le gouvernement américain a acheté, au bénéfice d'*Amazon* un *data center* complet avec les données du gouvernement américain à l'intérieur, ce qui représente un avantage compétitif considérable.** Il est difficile d'imaginer ce type d'opération en France. Il existe aussi des différences culturelles. Une offre de *cloud* impacte le fonctionnement des DSI dans les grands groupes et il existe des freins au changement. Il faut « évangéliser » les entreprises.

En France, on parle toujours de la sécurité du nuage qui est un vrai problème. On y a à peu près répondu et on est à peu près certain d'y avoir bien répondu. Aux États-Unis, le débat en est à la phase suivante : la question est celle de la diminution des coûts des systèmes d'information des entreprises pour utiliser l'argent ailleurs. Un autre débat a trait, avec l'informatique en nuage, à la rentabilisation de l'informatique, c'est-à-dire de la consommation électrique en minimisant la pollution et la consommation énergétique. Le modèle n'est viable, à mes yeux, qu'à partir du moment où l'on atteint une masse importante. Il faut mutualiser et industrialiser. Plus vous mutualisez, plus vous baissez le coût et reportez ces baisses de coût vers les partenaires et utilisateurs finaux.

M. Bruno Sido. – Nous donnons à la parole à M. Cédric Prévost.

M. Cédric Prévost, directeur de la sécurité et de la qualité des programmes, *Cloudwatt*. –Je vous remercie de nous recevoir pour cette audition. Mon propos se veut un peu plus « terre-à-terre » que ce que j'aurais pu envisager initialement. **Le numérique est actuellement un des principaux moteurs de la croissance en France et en Europe. Le nuage ou *cloud* public est le moteur des systèmes d'information de demain.** L'ensemble des systèmes d'information va basculer, d'ici trois, cinq, dix ou quinze ans dans le nuage public car c'est aujourd'hui la voie privilégiée. C'est la manière d'exploiter le numérique. Nous sommes aujourd'hui très loin de mesurer l'ensemble des bouleversements qui vont être induits par cette migration des systèmes des entreprises et de l'État vers le numérique. Lorsque l'on est passé de la bougie à l'électricité, on ne s'est pas rendu compte immédiatement de l'ampleur des changements dans l'industrie. Nous pensons que nous sommes à la veille de ce type de bouleversement pour l'écosystème industriel de l'*IT* et pour l'industrie dans son ensemble.

Il existe un enjeu important pour la France à faire bouger les choses. J'identifie **trois enjeux en particulier pour la France**. Le premier vise à **développer des acteurs industriels qui comptent à l'échelle européenne et mondiale dans ce monde du numérique**. Les acteurs européens ne sont pas si nombreux puisqu'il n'existe que *SAP* et *Dassault Systèmes*. Nous avons une problématique de crédibilité de ce point de vue.

Le deuxième enjeu réside dans la nécessité de **faire bouger les lignes de ce qu'on appelle la sécurité numérique. Le développement d'un écosystème numérique viendra avec la confiance dans ces nouveaux systèmes**. Or ceux-ci sont poussés, dans l'immédiat, par les nouveaux usages numériques, plutôt « grand public », avec un focus « sécurité » qui n'est orienté que vers certaines parties. Pour développer les échanges numériques entre les entreprises et leurs fournisseurs, il faut une confiance de fond dans le système numérique. Cette confiance n'est pas établie aujourd'hui et **les mécanismes de sécurité mis en œuvre en Europe et singulièrement en France sont dépassés**.

Le troisième enjeu est celui du développement territorial car **derrière le numérique se dessine la possibilité pour les territoires de tirer un bénéfice économique direct**, avec par exemple l'implantation de *data centers* et surtout la création d'écosystèmes de *start-up* et d'entreprises innovantes qui évoluent dans l'informatique ou qui vont bénéficier des avantages de ce secteur.

Cloudwatt fait partie des acteurs industriels capables de répondre à ces défis numériques. Nous nous attachons à accompagner l'évolution du paradigme dominant en termes de sécurité. Nous avons aussi vocation à utiliser de multiples centres de données, ce qui doit se traduire par une diversité d'implantations régionales et européennes.

Mme Anne-Yvonne Le Dain. – Nous voyons des *data centers* portés par des entreprises américaines qui fonctionnent très bien. Le *cloud* est par définition quelque chose d'improbable même s'il est tout à fait concret et réel. Comment situez-vous l'enjeu du nuage numérique pour l'économie française et la société française, dans une société mondialisée ?

M. Cédric Prévost. – Nous n'affirmons pas que ce nuage numérique doive être seulement porté, en France, par des entreprises franco-françaises, par exemple les deux *cloud* souverains qui ont été constitués. Ce serait une vision parfaitement archaïque. Il existe de nombreux besoins de développement du numérique qui ne requièrent pas d'être portés par un nuage régi seulement par les lois françaises ou européennes.

En revanche, **les données d'une entreprise sensible comme *Airbus*, de même que pour *Valeo* ou de nombreuses autres entreprises industrielles françaises ou européennes, peuvent être exposées à des risques si elles sont stockées dans des *clouds* de filiales de groupes mondiaux, sachant que les principaux acteurs du secteur sont aujourd'hui américains**. Cet hébergement voudrait dire que vous êtes soumis aux règles qui s'appliquent à ces entreprises telles que le *Patriot Act*, en conséquence de quoi ces données peuvent « fuiter » à votre insu quelles que soient les bonnes paroles et les promesses qu'on vous fait. Il y a un enjeu important autour de ces données sensibles qui représentent peut-être 30 % à 40 % des données et traitements réalisés en France et en Europe. Cette part des données traitées est cependant porteuse d'une grande part de la croissance pour l'économie française.

Cloudwatt est l'un des deux *cloud* souverains que je mentionnais. **L'un des enjeux de cette souveraineté est la localisation des données et des traitements qui ne sont soumis qu'à la législation française et européenne.** Cela peut être vérifié par les autorités compétentes et **le travail réalisé par l'ANSSI autour du référentiel du *cloud* auquel nous avons contribué est extrêmement important car il permet qu'un tiers de confiance parfaitement reconnu garantisse que ce que nous faisons est assorti du bon niveau de sécurité** pour assurer l'étanchéité et le cloisonnement de ces données qui ne doivent pas quitter le giron de l'entreprise. Cette maîtrise s'étend à la localisation et aux technologies mises en œuvre. Nous ne sommes pas en mesure de construire en France un *cloud* avec des technologies 100 % françaises mais l'enjeu n'est pas là. Nous utilisons un maximum d'*open source* avec des ingénieurs formés en interne ou dans le cadre de la politique de développement de l'entreprise. Certes, **les composants tels que les processeurs sont fabriqués à Taiwan ou au Japon et il n'existe quasiment plus de routeur européen**. Nous nous attachons à construire une infrastructure de *cloud* qui a pris en compte ces risques.

J'évoquerais enfin le besoin de changer le paradigme de sécurité. La construction d'une offre de *cloud* française qui se veut souveraine, à des prix fixés par le marché, représente un défi. Le prix de la souveraineté est

aujourd'hui difficile à monnayer. **Les prix du marché, dans le *cloud*, sont fixés essentiellement par *Amazon*, dans une moindre mesure par *Google* et *Microsoft*. Si vous ne vous alignez pas sur ces prix, vous ne survivrez pas.** L'enjeu consiste à construire des éléments souverains qui répondent à ces contraintes externes. Cela suppose notamment de faire évoluer la perception de la sécurité, qui a surtout été envisagée, depuis quinze ans, comme une sécurité périmétrique, de façon statique. On mettait en place les bons équipements, de façon bien pensée, avec les bonnes règles. Dans la vraie vie, cela ne se passe évidemment pas de cette façon. **La sécurité d'un système ne s'apprécie pas uniquement lors de sa construction mais tout au long de sa vie.** Même si vous construisez un système sain, sa sécurité se dégrade naturellement dans le temps. **L'enjeu consiste, avec des dizaines de millions de connexions et d'utilisateurs, à maintenir ce niveau de sécurité en sachant que le système subira des attaques « classiques » (qui représentent 98 % des attaques constatées, répertoriées et aisément identifiables) et des attaques atypiques. Il faut donc être en mesure d'identifier les 1 % ou 2 % d'attaques qui sortent de ce schéma avec des technologies aujourd'hui maîtrisées par un faible nombre d'acteurs.** L'un des atouts de *Cloudwatt* réside dans la présence, au sein de son actionnariat, de *Thales*, qui est un des experts mondiaux pour ce type de sécurité. Cela permet aussi de bénéficier de ce type d'innovation en termes de recherche de solutions de sécurité adaptées aux nouveaux schémas avec une volumétrie importante.

M. Bruno Sido. – La parole est à M. Laurent Heslault, de *Symantec en France*.

M. Laurent Heslault, directeur des stratégies de sécurité, *Symantec en France*. – Je vous remercie de nous donner la parole et de nous donner l'occasion de nous exprimer. Notre mission est de développer des outils pour protéger des infrastructures informatiques et industrielles mais aussi les informations et les identités.

Pour ce faire, nous avons construit en un peu plus de vingt ans un grand système d'observation et de l'évolution des menaces qui nous permet de développer des outils qui seront ensuite utilisés par les différents clients ou fournisseurs de services, entreprises, Gouvernement et particuliers, pour mettre en place ces solutions de sécurité. Je suis en phase avec ce qu'indiquait M. Stanislas de Maupeou sur la cyberdépendance, voire la « cyberinterdépendance », car il sera difficile de revenir en arrière. Nous sommes hyperconnectés, partout et tout le temps. Nous sommes dans un environnement qui s'est fortement complexifié.

Il y a vingt ans, on pouvait dessiner à main levée, sur un tableau, le schéma du système d'information d'une entreprise. Avec le *cloud*, les réseaux sociaux, la mobilité, c'est fini. **Nous sommes dans une société d'hyperconnectivité et d'hypercomplexité.** S'y ajoute un État hypercompétitif. **Nous sommes dans l'hypercompétitivité au niveau des**

entreprises et des États, ce qui relève fortement le niveau d'attaques au regard de ce qu'on a pu connaître ces dernières années.

Il y a quelques mois, un de nos patrons affirmait que les antivirus étaient morts. Cela a surpris tout le monde mais ce n'est pas faux car les menaces auxquelles nous avons affaire aujourd'hui sont très différentes de ce qu'on voyait il y a trente ans lorsque nous commencions à protéger les ordinateurs. Ce territoire d'évolution a été marqué par la progression, en maturité, des attaquants et par la diversification de leurs motivations (*hackers*, cybercriminels, cyberterroristes, cybermercenaires, etc.). La modélisation de ces attaques est faite et nous disposons de modèles précis de ces attaques. La question porte sur la façon dont on y répond.

Au niveau macroscopique, il nous semble que **c'est la cyberrésilience qu'il faut rechercher**. Dans quelle mesure le système d'information est-il résilient ? Qu'ai-je fait pour me protéger de la prochaine attaque voire de l'attaque en cours ? Que vais-je faire pour y répondre et redémarrer le plus rapidement possible, avec des moyens dégradés voire avec du papier ? On va traiter la question en réfléchissant à la notion de risque. À quel niveau la gestion des risques informatiques est-elle positionnée dans le traitement des risques qui entourent l'entreprise ? Le *World Economic Forum*, qui se tient à Davos chaque année, a classé les **cyberattaques** au **quatrième rang mondial des risques concernant notre société** et considère que ce sujet devrait occuper la de**uxième place d'ici douze à dix-huit mois**. La *Lloyd's* place les cyberrisques au troisième rang des risques qui menacent les entreprises. **La *Lloyd's* propose d'ailleurs des systèmes de cyberassurance, sauf pour l'énergie, domaine jugé trop risqué.**

Il faut envisager la gestion des risques en traitant les vulnérabilités, qui sont de trois ordres : les hommes, les processus et la technologie. S'agissant des êtres humains, on peut agir par la formation et l'information en vue de parvenir à une prise de conscience correspondant à un véritable état de vigilance. Tous les tests de pénétration parviennent encore à leur but, c'est-à-dire mettre en évidence une faille dans le système de sécurité d'une entreprise, parce qu'on laisse une clé *USB* dans un parking. Il y a toujours beaucoup de travail à faire de ce côté-là. Il y a aussi beaucoup à faire du côté procédural. Toutes les études réalisées à ce sujet montrent que des employés qui quittent une entreprise emportent toujours avec eux des données appartenant à l'entreprise. En France, 61 % des personnes interrogées quittent l'entreprise avec des données appartenant à cette dernière. Nous avons aussi conduit une étude demandant aux entreprises françaises à quel niveau elles valorisaient le capital informationnel. Le chiffre moyen obtenu en France est 30 %, alors qu'il est de 50 % dans le monde. Nous sous-valorisons ce capital.

D'ailleurs, lorsqu'on demande à nos interlocuteurs où se trouvent leurs informations sensibles et s'ils savent qui y a accès, la réponse est « non ». Il existe des technologies qui sont là pour mettre en œuvre ce niveau

de sécurité. Elles nécessitent des ressources humaines. Nous proposons des produits qui seront mis en œuvre dans les entreprises dont c'est le métier. Là aussi, il existe un vrai manque et **nous pourrions avoir beaucoup plus d'entreprises françaises en mesure de traiter la protection des infrastructures et des identités**. Il faudra d'abord mettre en place le niveau de communication et de coordination pour les internautes mais aussi pour les professionnels, les entreprises et, évidemment, pour le secteur public, car il y a aujourd'hui un vrai manque de communication et de collaboration.

Il y aurait grand intérêt pour la collectivité à **renforcer ces liens de coopération avec des spécialistes**, pourvu que les pouvoirs publics nous montrent la voie. M. Bruce Schneier, qui est reconnu sur les sujets dont nous parlons, et à qui il peut arriver de dire des choses intelligentes, a dit : « *la sécurité, c'est un état d'esprit* », ce qui est tout à fait vrai. Ce ne sont pas seulement des outils, des lois et des personnes compétentes.

Mme Anne-Yvonne Le Dain. – Vous avez insisté sur le terme d'identité. Pourriez-vous préciser votre pensée ?

M. Laurent Heslault. – Il s'agit des éléments permettant d'identifier de manière certaine un individu, un fichier ou un objet connecté. Cela fait partie des vulnérabilités que l'on observe. Le vol d'identité, au sens des individus mais aussi pour l'objet informatique au sens large, nous préoccupe au plus haut point. **En ce qui concerne l'Internet des objets, nous avons devant nous des milliards d'objets qui sont censés nous représenter.** C'est un des principaux enjeux pour demain. Nous avons commencé, historiquement, à protéger les infrastructures. Avec l'Internet des objets, l'identité de toute chose sera fondamentale, ne serait-ce que **les adresses *IP*, qui deviennent un véritable sujet de préoccupation**.

Mme Anne-Yvonne Le Dain. – L'adresse *IP* n'est pas un élément que l'on peut changer très facilement.

M. Laurent Heslault. – Cela va évoluer avec les nouvelles versions de l'*Internet Protocol*. Sa version 6 va répondre à un certain nombre de questions devenues courantes du fait du nombre limité fourni par l'*IPV 4*. On voit souvent l'*IPV 6* comme une réponse à ces limites. Mais le protocole a aussi été pensé de façon un peu plus sécurisée.

Par ailleurs, **un grand nombre de systèmes connectés arrivent sur le marché sans que la sécurité n'ait été spécifiquement pensée dans leur processus de fabrication**. Lorsqu'on choisit un véhicule, la sécurité est un élément très important. Pour à peu près n'importe quel objet connecté, la sécurité apparaît comme un élément négatif, ce qui est finalement assez paradoxal. Certaines technologies permettent d'identifier de façon plus précise « qui fait quoi » et comment.

Mme Anne-Yvonne Le Dain. – Il y a une espèce de grand « on » qui crée des choses, des mots, un vocabulaire que nous nous approprions tous mais avec deux ou trois ans de retard. Le *cloud*, le nuage, est dans le paysage

public depuis quatre ou cinq ans à peine. On a l'impression que le vocabulaire arrive puis s'impose à tous. Or il naît avant de se diffuser. Comment se fait-il que nous ne participions pas, en France et en Europe, à la création de ce vocabulaire ? Nous savons tous que le vocabulaire fait sens. Comment crée-t-on les mots pour désigner tous ces champs et ces objets nouveaux ?

M. Thierry Floriani. – Nous étions présents lors de la première révolution de l'informatique, avec l'ordinateur – qui est un mot français. **Nous avons raté la révolution Internet.** Ce sont des mots anglo-saxons. Ce sont eux qui ont imposé la technologie et le savoir tout en maîtrisant l'influence qui accompagne ces sujets. Par exemple, **les adresses *IP* sont définies par des organismes extra-européens**. L'objectif est de **ne pas rater la troisième révolution qui est celle des objets communicants et du citoyen numérique**, de l'avatar numérique de chacun d'entre nous pour faire en sorte qu'il existe et soit protégé.

Mme Anne-Yvonne Le Dain. – J'ai un peu l'impression que les Américains imposent la norme, comme si le marché créait la norme et non l'inverse. Comment se fait-il qu'en Europe, nous n'y parvenions pas ? Prenons l'exemple des noms de domaine. Je trouve magique ce qu'il se passe en ce moment avec les noms de domaine. Les Américains, très brillants, décident d'un seul coup d'externaliser le système et nous trouvons tous cela formidable. Pourquoi ne sommes-nous pas aussi malins ? Je pense d'abord, à travers ce « nous », à la France et, en second lieu à l'Europe.

M. Stanislas de Maupeou. – Il me semble que ce n'est pas tant un sujet de sécurité qu'un sujet de gouvernance de l'Internet. Il y a deux ou trois ans, **la ville de Paris a dû payer 180 000 dollars aux États-Unis pour pouvoir enregistrer le nom de domaine « .paris »**. De ce point de vue, **nous sommes quasiment dans un état de « colonie numérique » et la reconquête est à organiser**, ce qui me semble être le sens de la création d'entreprises comme *Cloudwatt*. Mais la sécurité n'est que le révélateur d'une perte de maîtrise plus large qui ne se réduit pas à cet aspect.

M. Luc Renouil, directeur du développement et de la communication, *Bertin Technologies*, vice-président de l'association *Hexatrust* d'éditeurs français de la confiance numérique. – Il faut être lucide. Les Américains se sont développés parce qu'ils ont été intelligents et manœuvriers. Leurs sociétés se sont développées à partir de zéro. Ce qu'on constate dans le numérique, c'est l'héritage d'une vision industrielle limitée à quelques champions en déconsidérant la filière et tous les outils de construction de solutions industrielles dans la durée. L'intelligence des Américains est d'avoir été manœuvriers. Nous ne le sommes pas et nous ne sommes pas près de l'être. Nous avons deux sociétés européennes parmi les cinquante premiers éditeurs mondiaux, *SAP* et *Dassault Systèmes*. Je me suis permis de prendre la parole en tant que représentant d'une PME soucieuse de faire bouger cet état de fait.

M. Badi Ibrahim, directeur des opérations, *P1 Security*. – Le monde des télécoms est un des rares exemples où l'Europe a imposé ses normes. Avec l'avènement de la 4G, les Américains et Asiatiques nous rejoignent après que ce fut le cas pour le GSM, pour lequel nous étions en avance. Nous sommes donc capables d'être leaders et ce n'est pas une fatalité d'être à la traîne partout.

M. Bruno Sido. – La parole à M. Beylat, président du Pôle Systematic.

M. Jean-Luc Beylat, président du Pôle Systematic Paris-Région. – Je vous remercie de votre invitation. Je m'exprimerai ici au nom du Pôle de compétitivité Systematic, centré sur les problèmes dont nous discutons. L'intitulé de la présente audition me fait réagir d'emblée car **le numérique n'est pas un risque mais une opportunité. Il faut parler de confiance numérique.** Dans le numérique se trouvent des risques mais manger est également risqué comme tous les actes de la vie. Globalement, le numérique constitue une opportunité.

Dans le groupe thématique « confiance numérique » du Pôle Systematic sont réunis trente-six grands groupes et soixante-dix PME (dont celle dirigée par M. Luc Renouil), huit entreprises de taille intermédiaire (ETI) et vingt-six laboratoires de recherche publique. Depuis la naissance du pôle, cet environnement sur la confiance numérique a engagé et labellisé un peu plus de quatre-vingts projets, pour un investissement global de 400 millions d'euros en R&D – montant financé majoritairement par le secteur privé.

Les acteurs de ce segment envisagent la question comme un espace d'innovation. Je signale d'ailleurs que les objectifs de Barcelone n'avaient rien à voir avec l'innovation puisqu'ils portaient sur des dépenses de R&D.

Ce n'est pas parce qu'on dépense qu'on est efficace. Le focus n'a pas réellement été mis sur l'innovation dans la stratégie de Barcelone puisqu'il s'agissait d'injonctions de dépenses. Comme cela a été souligné, tout passe par les outils numériques. La confiance ou la sécurité numérique constitue un terrain de bataille économique dans lequel l'innovation fait la différence. Plusieurs acteurs en France peuvent prétendre jouer un rôle dans ce domaine. Globalement, la filière du numérique génère **un chiffre d'affaires de 13 milliards d'euros pour les acteurs français, dont 65 % sont réalisés à l'exportation**. C'est donc un espace de croissance pour les acteurs français, avec une **croissance moyenne de 7 % par an** selon les données de l'Alliance pour la confiance numérique.

La cybersécurité doit s'adapter aux mutations du comportement des entreprises. Il faut d'abord souligner la rapidité de l'évolution des technologies. Avec la « cloudification » des services, il devient essentiel de suivre la dynamique des innovations. Il faut innover autour de la mobilité-sécurité. **Il ne faut pas arriver avec des solutions plaçant l'employé dans un**

environnement sécurisé mais impraticable car il emprunterait alors les portes latérales et les risques seraient amplifiés.

Il en est de même pour le nuage, vers lequel il faut pousser les entreprises car celles-ci vont y trouver une dynamique, en termes de service et de coûts de fonctionnement, dont elles ne bénéficieront pas si elles conservent leurs anciennes solutions. Mais il faut les accompagner dans la sécurisation de ces développements. Il faut projeter les acteurs français vers ces objectifs en termes d'innovation.

La plupart du temps, on se rend compte que la conception des systèmes est suffisante en termes de sécurité car **de nombreuses attaques ne sont pas très « fortes »**. Elles deviennent performantes dès lors que l'architecture d'ensemble n'a pas été bien pensée. Il faut **diffuser la culture de sécurité parmi les entreprises** et particulièrement les PME qui présentent une vulnérabilité particulière. Travaillant chez *Alcatel-Lucent*, qui est une entreprise franco-américaine, j'ai pu constater qu'**il existait une culture de sécurité plus aisément enseignée dans les entreprises américaines que dans les entreprises européennes**. Il y a pourtant là des choses assez simples à mettre en place.

Le groupe thématique « confiance numérique » du Pôle Systematic a avancé quelques propositions qui méritent d'être débattues. La première consisterait à **réformer la législation française et européenne en visant un niveau de protection obligatoire pour les opérateurs d'importance vitale (OIV), en aidant les PME à se protéger**. On peut en effet être un opérateur d'importance vitale sans que le cadre législatif associé n'ait été défini en matière de sécurité. Cela paraît l'élément le plus important, plutôt que de placer des éléments dans telle structure au motif qu'elle est financée par la Caisse des dépôts et consignations – sans vouloir être désobligeant. **Ce n'est pas le financement qui crée la souveraineté.**

Mme Anne-Yvonne Le Dain. – Je rebondis sur vos propos pour évoquer ce qui se produit actuellement entre *BNP Paribas* et les États-Unis. On peut se demander d'emblée pourquoi les Américains mettent à l'amende une banque française et ce n'est pas très lisible même si on se penche sur la question. On découvre que la menace de sanction est brandie parce que la *BNP Paribas* a encaissé des transactions réglées en dollars.

Mme Agnieszka Bruyère, directrice de services de sécurité, *IBM France*. – Les fonds ont transité par *BancWest*, une filiale de *BNP Paribas*.

Mme Anne-Yvonne Le Dain. – Il est impensable pour une PME de raisonner de la sorte. Les entreprises n'ont-elles pas intérêt à tout facturer en euros ?

M. Stanislas de Maupeou. – C'est le client qui impose de traiter dans telle ou telle devise. L'euro est une monnaie européenne. Il est très rare de rencontrer, hors d'Europe, des clients acceptant de régler en euro.

Mme Agnieszka Bruyère. – Si les clients se trouvent dans des pays étrangers, on s'aligne sur la monnaie qui y est couramment utilisée.

M. Stéphane Lenco, membre du bureau, Groupement interprofessionnel pour les techniques de sécurité des informations sensibles (GITSIS). – Pour le groupe *Airbus*, le marché a été structuré par les Américains et la monnaie attendue par les clients, où qu'ils se trouvent dans le monde, est le dollar. À quelques exceptions près, nous négocions d'emblée en dollars.

Mme Anne-Yvonne Le Dain. – Nous sommes donc pilotés par le *Patriot Act*.

M. Stéphane Lenco. – C'est quelque peu le cas, en effet.

M. Jean-Luc Beylat. – Je souhaitais formuler une deuxième proposition. **La taille des grands acteurs est liée à la dépendance européenne. Or on peut réduire cette dépendance grâce à des outils français ou européens en s'appuyant sur la dynamique de l'*open source*.** C'est ce que nous avons vu dans le *cloud.* Lorsqu'on sort des modèles propriétaires, on quitte d'abord une dépendance. Les logiciels de l'*open source* bénéficient d'un cerveau collectif archi-connecté et avancent beaucoup plus vite. Ce sont pratiquement les éléments structurants du *cloud* aujourd'hui et ne sont dépendants de personne. Nous le voyons bien dans la communauté du Pôle Systematic.

La troisième proposition vise à **mettre en place des solutions de souveraineté européennes lorsqu'elles sont pertinentes**. Il faut différencier ce qui est pertinent et ce qui ne l'est pas. À titre d'analogie, dans une salle blanche, on va s'attacher à avoir un niveau de propreté très important à l'entrée de la pièce. Dans les zones où la propreté est moins critique, la vigilance sera moindre. Il en est de même en matière de sécurité. Il faut focaliser les efforts là où ils sont pertinents d'autant plus que la situation évolue aussi du point de vue de la valeur des données et de leur criticité. Il y a aujourd'hui de nombreuses informations qui ne valent plus rien.

M. Bruno Sido. – La parole est à Mme Agnieszka Bruyère.

Mme Agnieszka Bruyère, directrice de services de sécurité, *IBM France*. – Je vous remercie pour votre invitation. Je représente *IBM*, l'entreprise qui propose à la fois les solutions de sécurité, une très large gamme ayant pour ambition de traiter les questions de bout en bout, les services de sécurité et les services du *cloud.* Nous avons commencé cette aventure avec notre *data center* basé à Montpellier, transformé ensuite en une plate-forme de fourniture de service de type *cloud.*

L'information est numérisée partout et des systèmes tels que le *cloud* s'ouvrent de plus en plus aux consommateurs de même qu'aux partenaires et clients des entreprises, dans tous les pays. Même les consommateurs français peuvent acheter des services et des biens hors de France.

Il faut prendre garde à la réflexion menée sur la cybersécurité en France pour ne pas amputer les entreprises françaises de gains potentiels de compétitivité sur un marché global qui permet à certains pays de progresser.

Il existe aussi des enjeux de sécurité et *IBM* reconnaît la nécessité de protéger de façon particulière le champ relevant de la souveraineté de la France avec des moyens précisément identifiés. Il peut s'agir de solutions françaises si on ne peut pas certifier une solution étrangère. On peut également s'appuyer sur des services de confiance et des dispositifs tels que des solutions de chiffrement ou encore des systèmes de détection des anomalies. Nous comprenons parfaitement cette nécessité. Nous essayons de nous y inscrire et espérons obtenir la certification de certains de nos produits car nous pensons que ce sont de bons produits. **Il ne faut pas que la France soit amputée des capacités de défense contre les cyberattaques au motif d'une politique industrielle qui ne tienne pas compte de certains impératifs de sécurité.**

En ce qui concerne les sociétés de télécommunications ou du secteur de l'énergie, il existe des domaines critiques qui nécessitent une vigilance absolue car ces domaines sont vitaux pour la nation. De nombreux systèmes d'information de ces entreprises relèvent simultanément néanmoins d'une informatique classique. Il faut adapter ses moyens au regard de la typologie des données et des systèmes considérés.

Dans l'industrie, l'énergie et les télécoms, il faut **tenir compte de la résilience des infrastructures**. Il ne faut pas pousser à réaliser des investissements colossaux mais plutôt rechercher un équilibre entre les investissements relevant des domaines d'importance vitale et ceux nécessaires pour le fonctionnement des entreprises et des organisations au quotidien.

Un autre sujet important a trait à la nature des attaques. **Statistiquement, les attaques proviennent majoritairement des États-Unis, du Japon et de la Chine** et nous avons besoin de connaître les modes opératoires des attaques ainsi que les techniques utilisés pour être performant dans la façon de se protéger. Cette collaboration doit être établie. J'espère qu'elle le sera enfin entre les États. Mes collègues ont évoqué des groupes d'attaques sponsorisées par des gouvernements en visant la propriété intellectuelle d'un État ou de ses entreprises clés. Au titre des services de surveillance que nous proposons aux entreprises, nous nous rendons compte aussi que des groupes vont attaquer de grandes entreprises car ils estiment que leur comportement sociétal n'est pas approprié. Il faut chercher à comprendre qui sont ces acteurs et comprendre comment ils opèrent sur le plan technologique pour mettre en place des défenses appropriées. Nous jouons un rôle important vis-à-vis des opérateurs d'importance vitale pour proposer ces services qui ne nécessitent pas d'entrer dans leur système d'information, ce qui est un point important.

Il faut des solutions souveraines dans certains domaines mais l'État et la France, d'une façon générale, ne vont pas assez vite dans la transformation des systèmes d'information vers des dispositifs de type *cloud*. Effectivement, l'État américain a décidé d'acheter une solution de *cloud* à *Amazon* ; ce serait formidable s'il pouvait en être de même en France. On ne va pas assez vite, ce qui est dommageable pour les solutions françaises destinées à servir les intérêts souverains. Ce rythme d'évolution se répercute sur les petites entreprises dans l'adaptation de leurs solutions de sécurité.

Enfin, vous avez mentionné le *Patriot Act* et la question de la sécurité du *cloud*. Je voudrais juste apporter une réflexion à ce sujet car nous échangeons beaucoup avec nos clients qui sont des opérateurs d'importance vitale ou non. Le *cloud* n'est qu'une capacité de calcul et de stockage. **Il existe des technologies ouvertes ou propriétaires.** On y place ensuite des données mais on a les capacités technologiques de protéger ces données même si elles se trouvent dans le *data center* d'un tiers et si l'exploitation des couches techniques incombe à un tiers. Il faut avoir cela en tête. **Le *cloud* peut être tout à fait sûr et cette sûreté peut être apportée par une politique de souveraineté mais aussi par les choix de technologie en conséquence desquels même l'hébergeur ou l'exploitant ne pourra avoir accès aux données.**

IBM a fêté sa présence en France depuis cent ans et nous souhaitons continuer d'accompagner les entreprises françaises. C'est la raison pour laquelle nous souhaitons obtenir la certification de nos services. Nous comprenons les besoins de sécurité qui existent et nous souhaitons pouvoir apporter notre expertise, à travers un service qui ne touchera pas le système d'information de nos clients. Nous plaidons aussi pour une harmonisation des textes réglementaires en France et en Europe. Je crois que c'est de visibilité et de la cohérence de l'ensemble que nous avons le plus besoin.

M. Bruno Sido. – Vous dites qu'on cherche à savoir qui sont les attaquants. Sont-ils toujours les mêmes ou se renouvellent-ils ? Par ailleurs, comment gagnent-ils leur argent et quelles sont leurs motivations ? L'objectif est-il ensuite de vendre des systèmes de sécurité informatique ?

Mme Agnieszka Bruyère. – **Les groupes d'attaquants organisés existent et sont assez facilement identifiables.** Ils opèrent en utilisant différentes techniques de plus en plus sophistiquées. Je ne livrerai pas nos secrets sur la façon de suivre ces groupes. Il faut *a minima* suivre les groupes existants.

Certains groupes sont financés par les États, pour l'espionnage et parfois pour introduire l'instabilité dans un État. Il existe aussi des liens financiers. Dans l'affaire *Target*, qui a déjà été mentionnée, une entreprise de distribution s'est fait voler, après l'introduction dans son système d'un programme pirate, les données de caisse et les informations contenues sur les cartes bancaires de ses clients, ce qui a donné lieu à des préjudices qui se

comptaient en centaines de milliards de dollars, au point de faire couler l'entreprise. Des gains peuvent venir d'usurpations d'identités voire de la vente de cartes bancaires volées. Ces opportunités de gains sont nombreuses, d'où l'intensification des attaques.

M. Laurent Heslault. – Les sources de financement dépendent beaucoup de la motivation des groupes concernés. Pour les attaquants qui suivent une motivation politique ou idéologique, le financement ne pose pas trop de problème. La connexion avec les réseaux de cybercriminalité est assez ténue. Ce sont des groupes qui pratiquent ainsi depuis des années. Ils sont organisés comme des entreprises avec des services R&D, *marketing*, etc. Vous pouvez acheter ce type de service. Il existe du « *crimware as a service* ». Ceci existe depuis des années. Il s'agit parfois de groupes très identifiés. Dans certains cas, on est confronté à des groupes qui se forment en fonction des besoins et de leurs projets. Ils se reconnaissent sans se connaître. On trouve ces acteurs dans ce qu'on appelle le « *dark web* » ou le « *deep web* ». Il y a beaucoup d'argent qui y circule, avec sans doute **un chiffre d'affaires de quelques dizaines de milliards de dollars**.

Je voudrais ajouter un dernier point sur le *cloud.* Nous avions demandé aux entreprises françaises de taille petite et moyenne si elles étaient présentes dans le *cloud*. Elles répondaient majoritairement « non », au motif de la sécurité des données. Dans le même temps, 90 % d'entre elles nous disaient qu'elles seraient plus sécurisées qu'aujourd'hui si elles devaient être présentes un jour dans le *cloud*. Il y a là un vrai paradoxe.

M. Bruno Sido. – Nous poursuivons avec M. Luc Renouil.

M. Luc Renouil, directeur du développement et de la communication, *Bertin Technologies*, vice-président de l'association *Hexatrust* d'éditeurs français de la confiance numérique. – Je suis un dirigeant de *Bertin Technologies*, PME française ayant une activité d'éditeur de logiciels. Je suis aussi un des fondateurs d'*Hexatrust*, une alliance d'éditeurs de logiciels de sécurité français qui cherchent à se développer sur le marché français et à l'exportation. Nous avons créé cette alliance il y a un peu plus de six mois.

Récemment, les notaires français ont choisi une solution de deux de nos adhérents – de préférence à une solution étrangère – pour la sécurisation de certaines de leurs données. Nous, nous disons que nos idées peuvent, petit à petit, faire leur chemin.

S'agissant de *Bertin*, nous avons une offre assez simple qui repose sur deux produits, l'un de vigilance et *d'early warning*, *MediaCentric*, et l'autre une solution souveraine de cloisonnement logiciel sur le poste de travail, *Polyxène*. Je me sens à l'aise dans la discussion qui a lieu cet après-midi.

Je suis frappé par la **convergence des questions qui se font jour aujourd'hui entre le monde des entreprises et du marché, d'une part, et celui de la défense, d'autre part**. On a construit des systèmes de sécurité sur

le principe de la ligne Maginot, en oubliant le mode de défense en profondeur. En développant un *OS* souverain pour le gouvernement français, on a fait le choix de la défense en profondeur. Je pense que ce choix sera payant dans la durée. Parallèlement, **on est impacté aujourd'hui par une lubie selon laquelle nos employés pourraient apporter leur propre matériel informatique sur leur lieu de travail**.

Le patron de la sécurité de *Hewlett-Packard* (*HP)* explique sans ambages que, sur un ordinateur *HP*, il n'y a que des données de *HP* et qu'il est interdit de l'utiliser à titre personnel. Encore faut-il avoir le courage d'affirmer les choses de cette manière.

Je crois qu'il faut réconcilier les usages, la sécurité et les environnements de travail. C'est notre travail au quotidien que d'essayer d'apporter des réponses pour favoriser cette convergence. De leur côté, les entreprises américaines sont extrêmement efficaces pour proposer des solutions qui conviennent à la plupart des clients français et européens.

Je suis frappé par la nécessaire notion de souveraineté numérique. Il ne faut pas être naïf. **Nous sommes dans une guerre économique et nous avons négligé la réflexion sur la notion de souveraineté qui est rarement évoquée hors du domaine de la défense.** Elle émerge de nouveau et je raisonnerais en termes de **cercles de confiance** plutôt que de façon dichotomique : que devons-nous absolument faire avec des solutions intégralement françaises ? Que pouvons-nous faire avec des partenaires européens ? Que devons-nous faire, y compris vis-à-vis d'alliés comme les Américains, qui pourraient le comprendre ? Pour le reste, qu'est-ce qui relève d'une coopération fondée sur les mécanismes de marché en souhaitant que le meilleur gagne ? Je pense qu'il faut creuser cette problématique de souveraineté.

Le point suivant que je souhaitais aborder n'a été qu'effleuré : il s'agit de l'exposition du tissu des PME et des entreprises de taille intermédiaire. Ce tissu peut être très exposé aux menaces et au risque numérique. De nombreuses entreprises du secteur de l'énergie (en particulier dans le domaine nucléaire) ont été victimes d'attaques répétitives il y a deux ou trois ans, parmi lesquelles des entreprises relativement grandes, d'autres beaucoup plus petites. **On peut envisager des applications « tout en un » destinées aux PME pour mettre à leur portée des services de sécurité relativement simples mais nécessaires.** Il faut y réfléchir en ayant conscience du fait que la culture et les moyens mis en œuvre aujourd'hui ne sont pas toujours à la hauteur des enjeux.

Enfin, je voudrais rappeler que si la sécurité n'a pas de prix, elle a un coût. Chacun doit l'intégrer, au niveau de l'État comme dans les grands groupes. Dans chacune de nos entreprises, cela coûte de l'argent. Il s'agit aussi d'un champ de compétences et de services que nous rendons à nos clients. La question rejoint celle des modèles économiques. **On parle du *cloud* comme s'il s'agissait d'un fait acquis. L'Europe découvre les modes**

de délivrance des solutions informatiques et il y a là une ingénierie extrêmement efficace de nos meilleurs amis américains. Nous devons nous montrer tout aussi vigilants. On parle par exemple aujourd'hui d'antivirus français. Mon collègue de *Symantec* vous confirmera sans doute qu'un antivirus ne paie pas : on le met à la disposition des utilisateurs pour pouvoir leur vendre d'autres services associés. Le développement d'un antivirus coûte très cher et on recherche nécessairement la vente de services plus globaux.

M. Laurent Heslault. – La réalité est plus compliquée que cela. C'est une logique industrielle. Même avec le meilleur outil du monde, on ne pourra le maintenir durant trente années, vingt-quatre heures sur vingt-quatre et sept jours sur sept. En outre, les virus représentent moins de 2 % de toutes les menaces et « saletés » qui circulent aujourd'hui.

M. Luc Renouil. – J'en viens aux deux ou trois propositions que je souhaiterais formuler, dont certaines ont déjà été mentionnées, notamment par le représentant de *Numergy*.

Je crois que les grands acteurs français, éventuellement avec leurs alliés (comme *Microsoft* pour *Bertin Technologies*) doivent **rechercher des partenariats en vue de la mise au point de solutions de souveraineté entre des éditeurs et offreurs de solutions** tels que des PME et de plus grands donneurs d'ordres. Les pouvoirs publics, à commencer par l'ANSSI, doivent faire preuve de volontarisme de ce point de vue. Ne nous leurrons pas : les qualifications de sécurité présentent un coût. Il faut pouvoir l'assumer car elles permettent de se différencier de la concurrence.

Ma deuxième préconisation vise à **discerner les thématiques et les axes de coopération européenne qui permettent de couvrir des besoins liés aux opérateurs** d'importance vitale quel que soit leur domaine d'activité (énergie, télécoms). C'est en effet à ce niveau que l'on peut rendre viables des modèles économiques distincts. De la sorte, on parviendra à construire les différents cercles de confiance avec des moyens *ad hoc*.

M. Cédric Prévost. – Un point important vient d'être soulevé à propos du coût de la sécurité. Les prix du marché ne sont fixés ni par les acteurs français ni par les acteurs européens. On ne peut ajouter des couches de prix dans les offres industrielles et **l'enjeu de la sécurité numérique ne réside pas dans « plus » de sécurité mais dans la recherche d'un « mieux » en termes de sécurité**. Depuis quinze ans, on a ajouté des couches de sécurité. Il faut à mon avis en enlever pour créer une sécurité plus simple, plus lisible et qui coûte moins cher.

M. Bruno Sido. – La parole est à M. Bernard Ourghanlian.

M. Bernard Ourghanlian, directeur technique et sécurité, *Microsoft France*. – Le panorama de la sécurité numérique, au sens large, met en évidence trois évolutions récentes importantes. La première est hélas l'irruption, dans de nombreux systèmes d'information de très grandes

entreprises françaises ou étrangères et de grands organismes étatiques, des *Advanced Persistent Threats (APT)*, c'est-à-dire des adversaires déterminés à attaquer des systèmes d'information dans l'objectif d'en prendre le contrôle.

Il faut admettre que **ces tentatives sont souvent couronnées de succès, y compris dans des entreprises très honorablement connues ou dans de grands ministères**. Je pense en particulier au ministère des finances, victime d'une attaque dont la presse s'est faite l'écho. Ce phénomène tend à s'installer. Nos équipes travaillent notamment en collaboration étroite avec l'ANSSI pour tenter d'éradiquer ces phénomènes une fois qu'ils sont intervenus. Depuis cinq ans, je crois qu'il n'y a pas une seule journée où nos équipes n'ont pas été impliquées par au moins une crise de sécurité majeure chez de grands acteurs. Le phénomène est donc préoccupant car il aboutit à l'exfiltration de centaines de giga octets de données qui sortent des systèmes d'information des entreprises et organismes publics en direction d'endroits difficiles à identifier mais situés souvent dans le sud-est asiatique. Force est de constater que ces tentatives sont malheureusement très efficaces puisque **l'installation dure pendant des mois, parfois des années**, conduisant souvent à l'évaporation d'un certain nombre de secrets industriels ou de propriété intellectuelle, de façon très préjudiciable.

Le deuxième phénomène est potentiellement prometteur mais inquiétant si on ne l'utilise pas de la bonne façon : il s'agit du *big data*, c'est-à-dire la capacité à collecter des données en provenance des individus et, d'une façon générale, toutes les traces numériques que nous laissons derrière nous. Cette possibilité peut avoir des impacts tout à fait positifs (par exemple s'il est envisagé d'utiliser ces données pour développer un vaccin contre le sida) ou au contraire très négatifs (par exemple s'il s'agit de transformer un État ou une entreprise en une sorte de « *big brother* » extrêmement dangereux).

Le troisième phénomène est sans doute le plus médiatisé depuis l'affaire Snowden et les démêlés divers et variés liés à la *NSA*. Je veux parler du rôle des États. Ceux-ci ont eu un rôle significatif dans le cyberespace ces dernières années mais leur rôle n'a jamais été autant mis en évidence qu'à travers cette affaire. Ce rôle est extrêmement subtil, allant de celui de simple **utilisateur** (pour conduire les opérations de l'État et servir les citoyens) à celui d'**exploitant du cyberespace** (pour assurer l'ordre public, effectuer des tâches d'espionnage voire conduire la guerre par d'autres moyens) en passant par le rôle de **protecteur du cyberespace** (faire en sorte que des crimes commis par l'utilisation de technologies numériques puissent être punis comme le prévoit la loi).

Dans ce contexte, l'État joue un rôle subtil de protection des citoyens, de leur liberté et de protection de la sécurité et de l'ordre public. L'affaire Snowden met en lumière la complexité de ce rôle et la difficulté à trouver un juste équilibre entre la sécurité et le respect de la vie privée. Pour

prendre le *big data* comme une illustration de cette subtilité, on peut aujourd'hui imaginer de collecter des données sans savoir à l'avance de quelle façon on pourra en tirer parti (positivement ou négativement pour l'utilisateur). La réglementation en vigueur en matière de respect de la vie privée prévoit **le recueil du consentement explicite de l'utilisateur mais ces dispositions ne sont pas appliquées de façon à permettre à l'utilisateur d'être pleinement conscient de ce qu'il accepte en permettant la collecte de ses données**. Il semble difficile d'imaginer qu'on pourra l'informer de manière suffisante sans pour autant décrire toutes les utilisations qui seront faites de ses données, pourvu qu'on sache que ces données pourront être utilisées dans deux, trois ou quatre ans pour son bien (par exemple pour une étude épidémiologique). Il en résulte des interrogations sur l'adéquation du régime actuel de protection de la vie privée. L'internaute moyen n'a pas les moyens de lire les dix pages de contrats relatives à l'utilisation qui pourrait être faite de ses données. Il est aussi très difficile de prévoir l'usage que l'on pourrait faire de ces données.

Bien que la France et l'Europe soient assez en avance dans la prise en compte des sujets liés au respect de la vie privée, l'irruption du *big data* suscite des interrogations et appelle une réflexion plus approfondie que ce qui a été conduit jusqu'alors. On pourrait imaginer de reporter sur l'utilisateur des données la responsabilité de cette utilisation, avec par exemple une charte éthique ou une loi décrivant ce qu'il est autorisé de faire et jusqu'où il est possible d'aller. Ce cadre n'est pas défini aujourd'hui. Les nouveaux usages du numérique mettent ainsi en évidence **l'insuffisante prise en compte de nombreuses dimensions liées aux enjeux du respect de la vie privée**.

Il est nécessaire de prendre en compte la nécessaire amélioration de la sécurité qui ne procède pas toujours de dépenses substantielles. Il y a deux ans et demi, M. Patrick Pailloux, directeur général de l'ANSSI, avait insisté sur la **mise en œuvre d'une hygiène au sein des systèmes d'information**. Je pense que cet appel demeure nécessaire. La capacité à faire des choses aussi simples que la **mise à jour des systèmes** ou la **mise en place de mots de passe convenables pour des comptes sensibles** doit être développée car ces prérequis ne sont pas toujours respectés, aujourd'hui encore. Il s'agit souvent d'une simple question de bon sens et il est vrai que la sécurité implique beaucoup de bon sens.

Plus largement, **un travail important de pédagogie reste à produire**, notamment auprès des entreprises (y compris les plus grandes) et des décideurs qui voient souvent la sécurité comme un mal nécessaire qui n'apporte pas grand-chose à l'entreprise.

Il faut aussi faire en sorte que nos concitoyens soient toujours au fait de ces enjeux car on ne peut considérer que la sécurité de l'Internet peut être approchée dans une logique de silo. **On peut en effet rendre inopérants des systèmes d'information extrêmement bien protégés du seul fait d'une**

sécurité insuffisante des postes de travail se trouvant à domicile. Ce sont des sujets vastes et il est nécessaire de mettre en œuvre un certain nombre de dispositifs de pédagogie, à l'école, au collège et dans les lycées. Il faut aussi dispenser une information plus systématique auprès de ces publics et de nos concitoyens, à l'image de ce qui existe par exemple en Grande-Bretagne, avec la diffusion de **programmes de sensibilisation sur la *BBC*, à des heures de grande écoute**. On ne trouve jamais cela en France : la sécurité informatique est un sujet qui fait peur et on va généralement faire peur à tout le monde sans avancer des solutions. J'insisterai sur ce fragile équilibre entre la sécurité, le respect de la vie privée et l'importance de la sensibilisation de tous ces acteurs.

M. Bruno Sido. – La parole est maintenant à M. Badi Ibrahim.

M. Badi Ibrahim, directeur des opérations, *P1 Security*. – Il y a un an, le 6 juin 2013, avec l'affaire Snowden on découvrait l'existence de *Prism*, système d'espionnage mis en place par la *NSA*. S'ensuivit un important volume de documents transmis progressivement au travers plusieurs titres de presse. On apprenait alors que l'agence de sécurité américaine surveillait des centaines de milliers d'ordinateurs à travers le monde mais aussi des téléphones portables, différents moyens de communication, et que les États-Unis d'Amérique auraient espionné plusieurs dirigeants européens, notamment des chefs d'État, des *leaders* mondiaux et des diplomates français.

La nécessité de renforcer la sécurité des réseaux s'impose au vu de l'ampleur de l'espionnage – y compris de la France – comme en témoignent les programmes *Prism*, l'espionnage de câbles sous-marins de télécommunications intercontinentales, le piratage de la filiale *BICS* de *Belgacom* ainsi que celui des entreprises chinoises de téléphonie mobile ; des documents détaillés attestent ces faits.

Depuis 1998, les experts de la société *P1 Security* ont mené des recherches appliquées dans le domaine de la sécurité des réseaux critiques, mobiles et de la télécommunication. Forte de son expertise technique et de son expérience internationale auprès des acteurs du secteur des télécommunications, notre société a réalisé de nombreuses études et audits qui ont permis d'identifier près de 800 vulnérabilités affectant de nombreux équipementiers tels que *Cisco*, *ZTE*, *Ericsson*, *Nokia Siemens Networks* ou encore *Alcatel-Lucent* ainsi bien sûr que de plus petits acteurs.

Les chercheurs de *P1 Security* ont depuis longtemps démontré que **les réseaux de signalisation téléphonique appelés 557 et *GRX* sont exposés à de multiples vulnérabilités permettant l'espionnage**, tel que dans l'affaire *BICS* de *Belgacom*.

Ce sont ces méthodes qui sont encore utilisées par la *NSA* et que nous avons communiquées lors de plusieurs conférences, en France comme à l'étranger, depuis plus de dix ans. Récemment encore, lors de la conférence « *Hackito Ergo Sum* », en avril 2014, ici à Paris, les chercheurs de *P1 Security*

ont présenté des études de sécurité des *HLR* (*Home Location Register*) et *HSS* (*Home Subscriber Server*) au sein des réseaux de téléphonie mobile et constaté qu'**un *HLR* ou *HSS* pouvait être mis hors service à l'aide de paquets créés par un attaquant. Ces *HLR* et *HSS* constituent le cœur des réseaux mobiles.** Ce sont les équipements du réseau responsables du stockage des données des utilisateurs, c'est-à-dire des bases de données comprenant les identifiants, la localisation de l'abonné, etc. Ils sont massivement interconnectés et s'appuient sur un grand nombre de services et applications internes.

À titre d'illustration, pour un réseau d'environ 20 millions d'abonnés, on trouvera 5 000 à 100 000 antennes radio pour seulement un à vingt *HLR*.

Dès lors, **il ne s'agit plus de s'attaquer à 100 000 équipements : il suffira parfois d'en compromettre un seul pour rendre le service indisponible**. Par exemple, après avoir réalisé une reconnaissance des différents équipements sur le réseau d'un opérateur, les chercheurs de *P1* ont été capables de localiser précisément la position des utilisateurs connectés à ce réseau téléphonique mobile. Ils ont en plus été capables d'émettre des appels et *SMS* depuis le numéro de leur choix, à l'échelle nationale et internationale.

Ces vulnérabilités soulèvent le problème de la disponibilité des réseaux des OIV mais aussi les possibilités qu'ont les attaquants de les compromettre ainsi que la confidentialité des informations, notamment pour les utilisateurs exerçant des responsabilités importantes, leurs contacts, les communications, leurs *SMS.* S'agit-il de faiblesses techniques inhérentes à ce type de réseau, le fait d'un manquement de la part des opérateurs ou des vendeurs ou encore de problématiques organisationnelles ? Y a-t-il un manque de régulation de la part des organisations internationales et/ou nationale ? Il faudra bien sûr trouver le moyen de répondre à ces interrogations et, à défaut de mettre un terme à ces agissements, apporter certains ajustements.

Tout d'abord, il faut rappeler que **les opérateurs de télécoms sont de plus en plus exposés à divers types d'attaques** allant de la fraude au déni de service. Pour ces raisons, les gouvernements de nombreux pays, y compris la France, ont intégré dans leur loi de programmation militaire un chapitre rappelant les enjeux de la sécurité et le besoin de sécuriser ces réseaux OIV. En effet, compte tenu du nombre d'abonnés utilisant ces services et des entreprises ou services de l'État directement impactés par un défaut de ces réseaux, il est clair que ces infrastructures font partie de la vie de nos concitoyens et n'appartiennent plus seulement aux opérateurs, dont la responsabilité est de veiller à leur bon fonctionnement. Dès lors, toute panne entraînant une perte de service exposerait ces opérateurs d'importance vitale à des poursuites ainsi qu'à des réparations financières importantes. On peut citer l'exemple d'*Orange* en 2012, qui a subi une

interruption de service de douze heures pour vingt-six millions d'abonnés. Le même cas de figure s'est produit pour l'opérateur britannique *O2*, avec plusieurs heures d'interruption de service pour 7 millions d'abonnés. Des problèmes similaires ont été recensés chez *Verizon* aux États-Unis, *T-Mobile* en Allemagne et chez de nombreux autres opérateurs. Tous ces problèmes étaient liés, entre autres, à une défaillance du *HLR HSS*. Au-delà de ces exemples qui font les gros titres de la presse, on entend rarement parler des problèmes touchant les opérateurs.

Il existe en effet un **manque de transparence de la part des vendeurs mais aussi des opérateurs** à ce sujet. Pour autant, je veux énumérer certains des problèmes fréquemment rencontrés par nos équipes lors des audits de sécurité qu'elles réalisent. En 2013, un opérateur japonais nous a contactés après quatre pannes massives qui ont impacté seize millions d'abonnés. Nos recherches ont montré que ces pannes provenaient de failles techniques sur des équipements *Nortel* récemment acquis par *Hitachi*. Il s'agissait vraisemblablement d'équipements d'ancienne génération peu ou pas maintenus après le rachat de cette ligne d'équipements *Nortel* qui entraient en conflit avec d'autres équipements du cœur de réseau.

Cet exemple montre le **risque d'accidents involontaires existant avec certaines technologies obsolètes**. Compte tenu des évolutions rapides dans le domaine des télécommunications, les opérateurs sont amenés à intégrer fréquemment de nouveaux systèmes tout en maintenant l'opérabilité avec les anciens équipements. C'est le cas notamment pour les équipements de deuxième ou de troisième génération qui cohabitent avec de nouveaux équipements de quatrième génération.

S'il est vrai que les nombreux problèmes identifiés touchent particulièrement les équipements de deuxième ou troisième génération, nous aurions tort de penser que ces réseaux seraient plus sécurisés du fait du déploiement de la 4G. Dans cette course aux nouvelles technologies, motivée par la volonté des opérateurs de proposer toujours plus de service à leurs abonnés mais aussi de concurrencer d'autres acteurs de l'Internet comme *Google*, *Skype*, *Facebook*, **ces développements sont rapides, parfois trop rapides pour avoir été testés**.

Par exemple, en 2013, lors du déploiement d'un nouveau réseau *LTE* pour un opérateur du Pacifique, nous avons prouvé qu'il était possible de mener plusieurs attaques (vol de données, fraude, intrusion) parfois simplement en utilisant un téléphone ou une clé 4G appartenant à un abonné du réseau.

De nombreux problèmes sont liés au manque de maturité des applications ou des équipements utilisés mais pas seulement. **De nombreux opérateurs désactivent volontairement les mécanismes de sécurité déjà peu nombreux parce qu'ils pourraient créer des latences sur les réseaux.** C'est notamment le cas concernant le chiffrement entre les antennes radio et le cœur du réseau. C'est tout particulièrement critique lorsqu'on sait qu'**il**

suffit de se brancher à la place d'une de ces antennes radio pour être directement connecté au cœur du réseau. Ces antennes, nombreuses, sont situées en haut des immeubles, parfois en pleine campagne et donc particulièrement exposées. D'autre part, plusieurs audits réalisés en Europe en 2014 ont montré un état critique de la sécurité, tant pour les réseaux de téléphonie fixe que pour les réseaux mobiles (2G, 3G, 4G). **Nous avons pu mettre hors service tout ou partie des équipements de cœur de réseau dans de nombreux pays en l'espace de quelques secondes ou encore pris le contrôle complet du réseau de téléphonie directement depuis des armoires de télécommunications dans la rue.**

Enfin, de nombreux cas de fraude ou d'intrusion recensés chez des opérateurs sont causés par des attaques internes provenant de réseaux amis ou partenaires. C'est là une des failles principales des réseaux de télécommunication. En effet, tout opérateur doit être interconnecté à un *cloud* privé qu'on appelle SS7 (système de signalisation # 7) dans le cas de la 2G/3G, *GRX/IPX* dans le cadre de la donnée mobile et donc peut adresser tout ou partie des équipements de cœur de réseau des autres opérateurs. **Il est impossible ou presque de se prémunir contre les attaques ciblant directement les routeurs ou les bases de données des autres opérateurs.**

Bien pire, **il est possible de se connecter à ces réseaux quand bien même on ne serait pas un opérateur**. C'est le cas de *P1 Security*, qui possède plusieurs interconnexions lui permettant de mener des audits à distance pour le compte de ses clients. D'ailleurs, il n'est pas indispensable d'être connecté à ces *cloud* privés pour avoir accès à des équipements de cœur de réseau. Comme expliqué par l'un des intervenants lors de l'audition publique de l'OPECST du jeudi 19 juin dernier, **certains outils *web* permettent de recenser sur Internet bon nombre d'équipements sensibles y compris des équipements de cœur de réseau** qui appartiennent aux opérateurs. Ces équipements qui ne devraient pas être connectés sur Internet le sont parfois par négligence. Il s'agit parfois d'équipements de tests ou encore d'équipements de production pour des besoins de maintenance.

Qu'il s'agisse de problèmes techniques liés aux technologies obsolètes, que ces problèmes soient posés par un empilement d'infrastructures (2G, 3G, 4G), auxquels il faut ajouter un grand nombre de périmètres voisins (réseaux *ADSL*, *Pay TV*, Internet, entreprises) ou encore les réseaux d'interconnexion (voix, *data*, etc.), de toute évidence, **les réseaux des opérateurs d'importance vitale, prétendus fermés, sont en réalité exposés à de multiples angles d'attaque**.

Il faut y ajouter trois grands problèmes spécifiques au monde des télécoms. Le premier est le **manque de sensibilisation à la sécurité des réseaux télécoms**. Souvent, les opérateurs ignorent les problèmes de sécurité, paradoxalement parce qu'ils craignent toute action susceptible d'avoir un impact négatif sur la disponibilité du réseau. On préfère donc ne rien

toucher tant que cela fonctionne. Le problème numéro deux est le **manque de contrôle ou de systèmes de détection dans les réseaux**.

Il est difficile de s'attaquer sérieusement aux problèmes de sécurité quand les opérateurs n'ont pas même de système d'alarme pour recenser le nombre ou le type d'attaques auxquelles ils sont exposés. Jusqu'à présent, seuls des systèmes de taxation réactive sont utilisés. Ils ne permettent de détecter les fraudes qu'*a posteriori*.

Alors que dans le monde IP, on trouve des pare-feu, des proxys, des anti-*spam* et qu'on s'interroge même sur les nouvelles méthodes qui ne soient plus périmétriques, il en est autrement **dans les réseaux télécoms**, où **les protections sont souvent bien faibles lorsqu'elles sont activées**.

Le problème numéro trois réside dans le manque de gouvernance qui relie des opérateurs peu nombreux (environ 50 opérateurs mobiles internationaux) et les équipementiers (sept ou huit équipementiers majeurs dans le monde). Les uns et les autres sont tentés de se rejeter la responsabilité de la sécurité et des failles lorsqu'elles sont identifiées, ce qui peut nécessiter parfois jusqu'à un an pour les résoudre. Ce problème de gouvernance est aussi à l'origine de **nombreuses failles de configuration** compte tenu des organisations complexes des opérateurs.

Nous avons observé trois nouvelles tendances dans les attaques menées contre les réseaux de télécoms. Le *big data* est important de même que les objets interconnectés. On parle dans les télécoms de technologies « *machine-to-machine* ». Les *femtocell,* équipement de relais radio présents à nos domiciles, fournissent un exemple d'équipements « *machine-to-machine* » que nous avons pu exploiter assez facilement. Grâce à de la rétroingénierie, il est possible de subtiliser des certificats présents dans ces *femtocell* et de les utiliser avec les cartes *SIM* qui accompagnent ces équipements pour se substituer à l'identité de ces équipements, ce qui offre un accès direct au cœur de réseau.

La deuxième tendance est bien sûr la cyberattaque. Il existe de multiples affaires dans ce domaine, par exemple *Telecom Italia* pour citer une des plus récentes. Cela met en jeu des agents motivés et compétents face auxquels les opérateurs sont souvent démunis. Cela ne doit pas servir d'excuse pour ne pas se prémunir contre ces acteurs du cyberterrorisme ni même livrer son réseau à la *NSA* comme l'a révélé récemment *Vodafone*.

Il existe enfin des attaques ciblant directement les vulnérabilités des équipementiers, ce qui constitue la dernière tendance en date que nous ayons observée. Il n'est pas rare de trouver des vulnérabilités suspectes qui ressemblent bien plus à des **portes dérobées** (*backdoors*) laissées volontairement. C'est, par exemple, le cas d'un certain nombre de commandes cachées par les opérateurs (notamment *Huawei*), qui permettent de réactiver ou de désactiver certaines fonctionnalités à distance.

Si ces problèmes inhérents aux infrastructures des réseaux télécoms sont nombreux et souvent critiques, des solutions existent. Elles sont d'une part techniques, par exemple en équipant ces réseaux de multiples mécanismes de sécurité, notamment du chiffrement avec des *Virtual Private Network (VPN)*, de la prévention (pare-feu, anti-*spam*) ou encore de la détection (sondes de sécurité). On peut aussi utiliser des solutions référencées qui excluent ou non certains vendeurs.

Il faudra privilégier la sécurité tout en préservant nos intérêts stratégiques. D'autres pays l'ont fait, notamment les États-Unis et la Chine. Il faut aussi **définir des guides de sécurisation technique à l'intention des opérateurs**. Enfin, il faut **auditer les réseaux télécoms**, pas seulement une fois par année civile comme le préconise le décret n° 2012-1266 du 15 novembre 2012 mais en définissant les vrais enjeux, les risques et les périmètres.

S'agissant des problématiques organisationnelles, il faudra surtout **sensibiliser les équipes de sécurité (y compris les équipes dirigeantes) et demander davantage de transparence aux opérateurs et aux équipementiers**, par exemple à l'aide d'une **certification spécifique des équipements et des réseaux**.

Aucune certification de ce type n'existe à ce jour et les vendeurs, ainsi que les opérateurs, suivent principalement les recommandations des organismes de normalisation ainsi que celles des organisations telles que la *GSMA* ou encore des critères communs. Malheureusement, ces recommandations de haut niveau ne sont pas suffisamment détaillées pour garantir un niveau de sécurité efficace.

D'une manière générale, nous préconisons plusieurs initiatives et notamment :

- l'organisation de nouveaux **consortiums et forums de recherche en sécurité**, pour une meilleure coordination de la sécurité télécoms ;

- une cartographie active des acteurs et réseaux télécoms et mobiles ;

- une **relation avec les chercheurs en sécurité** pour rester indépendants face aux groupes de pression et normalisateurs, qu'ils soient influencés ou influenceurs.

Comme l'expliquait M. Pascal Chauve, conseiller du secrétaire général de la défense et de la sécurité nationale (SGDSN) la semaine dernière lors de son audition publique par l'OPECST au Sénat, certaines mesures sont en cours de finalisation en France. Il s'agit, par exemple, de l'audit conduit par des prestataires de contrôle qualifiés par l'État, de l'obligation pour les opérateurs d'alerter l'ANSSI en cas de problème ou encore de la constitution d'une base de données de signature d'attaques. Malheureusement, ces mesures réactives sont encore trop timides et tardives pour avoir un réel

impact sur les opérateurs et les vendeurs. Ceux-ci sont déjà dans une logique trop lourde et insuffisamment orientés vers des solutions innovantes.

En Europe de l'Est, nous avons travaillé avec un opérateur qui a développé sa propre solution de détection d'attaques, de façon très intéressante. Nous encourageons l'ANSSI à collaborer davantage avec les sociétés du domaine pour ne pas appauvrir le tissu innovant des sociétés. Il faudra d'ailleurs que ces mesures soient appliquées à une plus grande échelle et avec le concours de nos partenaires européens si l'on veut éviter que nos concitoyens ne soient exposés dès lors qu'ils se déplacent à l'étranger.

M. Bruno Sido. – Je donne la parole à M. Stéphane Lenco, du GITSIS.

M. Stéphane Lenco, membre du bureau, Groupement interprofessionnel pour les techniques de sécurité des informations sensibles (GITSIS). – Je représente ici le GITSIS. Je suis par ailleurs officier central de sécurité des systèmes d'information du groupe *Airbus*.

Le GITSIS regroupe un certain nombre d'acteurs qui sont des opérateurs d'importance vitale. À ce titre, ces acteurs sont tous sensibilisés au risque numérique et ont une perception des menaces qui les entourent.

Pour la plupart des acteurs du GITSIS, la problématique de la sécurité numérique est aussi celle d'un marché international. La souveraineté s'entend au plan national. Pourquoi une solution souveraine française serait-elle plus légitime qu'une solution souveraine allemande ou britannique ? C'est une problématique réelle. Au-delà de la souveraineté, il faut la confiance, avalisée par l'État, sous quelque forme que ce soit. L'*open source* est à la fois intéressant et terrible car il est placé sous le regard de tous. Nous avons vu avec la faille *SSL*, qui a été largement médiatisée, qu'un produit libre et gratuit pouvait présenter de longue date des vulnérabilités – intentionnelles ou non.

On retrouve chez tous ces acteurs avec lesquels la France agit de nombreuses solutions technologiques curieusement similaires sans concertation préalable. La plupart de **ces solutions sont d'origine étrangère au sens large, en particulier américaines**. Cela constitue un profil de risque qu'il peut être intéressant d'identifier du point de vue des enjeux économiques pour l'État.

Enfin, notre secteur, qui regroupe principalement des acteurs de l'aéronautique et de l'espace, montre qu'on ne peut plus agir seul. On travaille dans une dynamique d'entreprise étendue avec des partenariats européens et souvent internationaux. Nous travaillons ainsi avec d'autres acteurs qui n'ont pas nécessairement le même degré de perception du risque. *Lockheed Martin* a été attaqué il y a quelque temps, de notoriété publique, à tel point que **le gouvernement américain considérait que la totalité du**

programme d'avion de chasse avait été perdu, à l'exception de quelques îlots qui avaient été extrêmement protégés.

Cet acteur a opéré un revirement complet du point de vue de sa *supply chain*, **en révisant le comportement à adopter vis-à-vis de PME conventionnées** qui n'ont évidemment pas les moyens de grands groupes ni toujours la maturité requise sur ces sujets.

Je voudrais enfin évoquer la ligne floue qui sépare la vie privée de la vie en entreprise. Certains voient cela sous l'angle du travail à domicile, sur les ordinateurs personnels. Il existe aujourd'hui des scénarios d'attaque qui ne relèvent pas de la science-fiction, dans lesquels l'individu est attaqué car il est beaucoup plus vulnérable et va transporter cette vulnérabilité dans son entreprise, qui peut être mieux protégée. On a, par exemple, fait entrer, dans un cas connu, **un virus *via* une clé *USB*** au sein d'un environnement qui était, en principe, totalement isolé.

S'agissant du risque numérique d'une façon générale, j'aime renverser la logique pour étudier la menace plutôt que le risque. Celui-ci est intéressant pour savoir ce que l'entreprise va assumer en tant que risque résiduel. Certaines personnes réagissent vivement à la notion de risque technique ou scientifique. Un risque est aussi une opportunité. C'est parce qu'on prend des risques qu'on est capable d'aller de l'avant. Si nous n'avions pas lancé le programme A300 avec l'idée folle de créer un avion commercial en concurrençant les Américains, *Airbus* ne serait pas là où il est aujourd'hui.

Le métier d'officier de sécurité en entreprise, qui est complexe, vise à sensibiliser tous les acteurs de l'entreprise à la réalité du risque. Les medias matérialisent en ce moment les rêves les plus fous de paranoïa qui existent dans la majeure partie du public avec tout de même un certain degré de crédibilité. Nous pouvons aussi être perçus comme des ayatollahs et comme des gens qui recherchent le risque zéro, même si bien entendu le risque « zéro » n'existe pas. Notre objectif est d'identifier un équilibre acceptable pour les dirigeants, en particulier, dans le fonctionnement quotidien de l'entreprise.

Le risque principal contre lequel nous luttons n'est pas nécessairement le déni de service ni l'altération du site *web*. C'est plutôt un enjeu d'intelligence économique, c'est-à-dire le risque de **fuite de notre savoir-faire et de notre capital intellectuel**. Nos appareils sont le fruit de dizaines d'années de recherche et développement. Si ce travail est annihilé parce qu'un concurrent se l'approprie, nous aurons perdu tout l'investissement réalisé durant des années, voire des décennies, parfois conjointement avec des États.

Notre travail est facilité lorsque nous bénéficions du soutien de l'État. Les informations protégées de défense sont entourées par un corpus de règles, de lois et de sanctions (y compris des peines de prison). La situation est plus délicate lorsqu'on doit composer avec un risque

matérialisé pour l'entreprise dans vingt ou trente ans, avec des dirigeants qui se soucient surtout du cours de la bourse. Si nous dépensons 100 000 euros pour telle ou telle « brique » de sécurité supplémentaire, le gain que nous allons en tirer sera-t-il supérieur à cet investissement ? C'est sur ces aspects que nous focalisons principalement notre attention.

La défense en profondeur, qui fait aujourd'hui figure de « tarte à la crème », désigne la démarche consistant à protéger les éléments les plus importants dans la durée pour l'entreprise. Encore faut-il avoir identifié ces éléments. Il s'agit souvent d'éléments diffus, notamment dans le *cloud*. On parvient tout de même à savoir où sont ces informations critiques qui doivent faire partie de la défense en profondeur.

Avant même cette défense en profondeur, certains acteurs n'appliquent pas les règles d'hygiène de base et ont leurs portes ouvertes sur Internet, avec un taux de survie de leurs informations ridiculement bas. En tant que grands groupes, dans les contrats que nous passons avec eux, nous prévoyons toujours une phase préalable d'audit pour mesurer le risque que nous allons prendre en nous connectant à leur système. Ces audits se concluent souvent par des appréciations et recommandations. Nous leur disons finalement « *vous mettez en danger notre entreprise, vous devez vous améliorer* ». Malgré tout cela, la situation ne s'améliore pas toujours.

La France est un pays qui a beaucoup de créativité et de nombreux atouts. On ne peut pas se permettre d'être partout. Des pays comme les États-Unis et la Chine ont des ressources financières beaucoup plus importantes. L'enjeu consiste à savoir sur quelles innovations technologiques nous allons mettre l'accent pour les pousser à l'échelle française et européenne. La France est d'autant plus efficace lorsqu'elle a le soutien de ses partenaires européens. Le plan 33 pour une Nouvelle France industrielle s'efforce d'identifier ces éléments, ce qui est positif. Nous devons nous concentrer sur ces éléments et cesser des « guéguerres » entre un certain nombre de sociétés très innovantes qui passent leur temps à se bagarrer entre elles à l'échelle franco-française alors que l'enjeu réside dans l'acquisition d'une crédibilité à l'échelle internationale.

M. Bruno Sido. – Je donne la parole à M. Jean-Marc Grémy, vice-président du Club de la sécurité de l'information français *(*CLUSIF*)*.

M. Jean-Marc Grémy, vice-président du Club de la sécurité de l'information français *(CLUSIF)*. – Je représente effectivement le CLUSIF, association née il y a trente ans de la volonté des compagnies d'assurance de comprendre le risque immatériel qui était alors moins bien appréhendé par les assureurs. On parle aujourd'hui du cyberrisque.

Nous fédérons 600 personnes et 270 entreprises de tous secteurs (secteur privé, secteur public) et de toutes tailles. Nous avons publié hier soir une étude qui nous rappelle qu'**une grande partie des incidents de sécurité liés aux technologies de l'information résultent essentiellement**

d'incidents internes liés au mauvais usage de certains éléments. La presse se fait l'écho d'attaques malveillantes venant de pirates de tous genres au plan international mais il ne faut pas oublier cette origine interne, plus banale, de nombreux problèmes.

Mme Anne-Yvonne Le Dain évoquait la nécessité d'être impertinent. J'observe à cet égard qu'aucun représentant du patronat français n'est présent aujourd'hui. J'aurais aimé débattre avec ses représentants pour savoir de quelle façon ils perçoivent la notion de risque, l'investissement dans la sécurité numérique et les enjeux dont nous discutons aujourd'hui.

Pour de nombreuses entreprises, le risque signifie l'absence de mise en danger. Pour certaines d'entre elles, tout risque est aussi synonyme d'opportunités. C'est grâce à cet opportunisme, notamment, que nous avons un champion de l'aéronautique en France. Lorsqu'on est patron de la sécurité d'une grande entreprise, on veut plutôt éviter les risques qui sont synonymes de danger. La vérité est sans doute entre ces deux appréhensions de la notion de risque. **Il ne faut pas imaginer que les entreprises vont externaliser l'ensemble de leur système d'information dans le *cloud*, ne serait-ce que pour des raisons sociales et parce qu'elles souhaitent conserver leur souveraineté.** On peut aussi avoir une méfiance vis-à-vis de son propre gouvernement lorsqu'on opère dans le monde industriel. Il est important de ne pas oublier qu'un certain nombre d'entreprises ont de grandes peurs face au risque d'attaques de leur système d'information.

Nous avons interrogé 350 entreprises de plus de 200 collaborateurs et 99 % d'entre elles nous disent qu'elles ne peuvent se passer de leur système d'information plus de quarante-huit heures. Ce constat rejoint la problématique à laquelle sont confrontés les opérateurs d'importance vitale qui doivent avant tout être en mesure de délivrer leur service qui fonde leur raison d'être. Il faut d'abord être en mesure de remplir sa mission et ses obligations. Par ailleurs, on voit que **34 % des entreprises interrogées n'ont pas encore nommé de responsable de la sécurité**. Je sais que le RSSI ne peut pas tout et n'est en aucun cas un « homme providentiel » pour la sécurité des entreprises. Cependant, lorsqu'on n'a désigné aucun responsable de la sécurité, personne ne peut porter ce discours, comprendre les risques et être force de proposition vis-à-vis de la direction de l'entreprise.

Je remercie toujours M. Snowden car certains ont découvert l'été dernier que des États se livraient à l'espionnage. Sans rouvrir ce débat, on voit aujourd'hui que 31 % des entreprises sensibilisent leur personnel, contre 18 % aujourd'hui. On lui explique ce qu'est le risque numérique, terme parfois confondu avec celui d'informatique (lequel est assimilé à la technique, là où le numérique embrasse un contexte plus large). **66 % des entreprises refusent aujourd'hui le *Bring Your Own Device* (*BYOD* ou** AVEC en français), c'est-à-dire **l'utilisation dans le périmètre de l'entreprise, en tant qu'outil professionnel, d'un équipement personnel**,

par exemple son *smartphone* ou sa tablette). Le discours de certaines institutions, comme l'ANSSI, commence donc à porter ses fruits dans des entreprises où l'on refuse de céder à l'envie d'être avant-gardiste.

En termes de sinistralité, le plus gros problème porte sur la perte des services essentiels, pour 40 % des entreprises interrogées. La notion de vol d'informations ou de matériels physiques vient en deuxième position et est citée par 35 % des entreprises.

On voit aussi que **de nombreuses entreprises n'ont pas encore défini un plan de continuité de l'activité (PCA)**. Ce n'est pas parce qu'on gère les risques qu'il ne se produira jamais rien. Il existe toujours une part de risque. En France, on maintient une armée car on n'a pas totalement écarté l'hypothèse selon laquelle un autre État aurait l'idée saugrenue de nous envahir. C'est cette notion de risque résiduel. Ce n'est pas parce qu'on ne veut pas qu'un élément se produise qu'il ne se produira jamais. Des entreprises n'ont pas encore pris en considération cette dimension, par exemple les risques de perte d'alimentation en énergie de leur *data center*.

Nous voyons que **nous manquons encore de personnes en mesure de porter cette sécurité dans les entreprises, au sein de la Direction générale et vers les directions « métier »** qui sont demandeuses d'une amélioration de la sécurité des systèmes d'information pour atteindre leurs objectifs et garantir leurs revenus, en établissant un pont avec l'outil informatique. Il s'agit aussi de faire en sorte que les équipes informatiques comprennent leur rôle et que les utilisateurs le comprennent aussi pour que la sensibilisation de tous les acteurs de l'entreprise soit plus forte. L'actualité est parfois déformée par la façon dont elle est rapportée par les journalistes mais cela nous donne de belles opportunités de sensibilisation pour faire écho à ce que relate la presse en expliquant que la perte de données personnelles, comme l'a subi *Domino's Pizza* la semaine dernière, n'arrive pas qu'aux autres. Cela se produit dans tous les secteurs d'activité. Même une entreprise qui livre des pizzas durant les matches de football n'est pas à l'abri.

Nous avons des groupes de travail et invitons les opérateurs d'importance vitale à rejoindre le CLUSIF pour débattre entre eux dans un espace privé et personnel. Ils peuvent y trouver ensemble non des solutions mais des axes d'amélioration pour une meilleure prise en compte de la sécurité dans leur environnement.

M. Bruno Sido. – Pour conclure, je voudrais que M. Christian Daviot nous livre le point de vue de l'ANSSI sur tout ce qui s'est dit cet après-midi.

M. Christian Daviot, chargé de la stratégie auprès du directeur général, Agence nationale de la sécurité des systèmes d'information (ANSSI). – Je voudrais tout d'abord souligner la bonne réactivité des industriels français. On vient de le voir dans le cadre de la loi de programmation militaire puisqu'on a mis au défi les industriels présents ici,

notamment, de sortir en dix-huit mois les premières versions d'équipements de détection d'attaques informatiques avec nos spécifications qui évoluent dans le temps. Il faut une certaine agilité intellectuelle et en matière de R&D pour répondre à nos exigences, parfois élevées. Cela dénote donc une grande agilité et une compétence certaine. J'espère que nous aurons rapidement, une fois les arrêtés parus, en fin d'année ou en début d'année prochaine, des équipements informatiques de détection d'attaques informatiques au sein des opérateurs d'importance vitale, ce qui n'empêchera pas d'accueillir des équipements de détection dans d'autres systèmes critiques ni de maintenir l'ouverture de certains marchés à nos amis et concurrents américains.

Nous avons d'ailleurs une très bonne coopération avec les grands acteurs de différents pays, américains mais aussi anglais et allemands, tant il est vrai qu'il faut, en matière de défense des systèmes d'information, collaborer avec nos alliés qui sont en même temps nos concurrents. Nous échangeons aussi des informations avec certains pays d'où viennent des attaques parce que nous avons des ennemis communs, sans doute à l'image de ce qui existe dans le renseignement. Nous avons une excellente coopération avec des entreprises étrangères dont certaines sont présentes ici. Sans les compétences de *Microsoft*, par exemple, nous n'aurions jamais sorti Bercy de la situation dans laquelle s'est trouvé le ministère.

Je voudrais également évoquer la réflexion stratégique. M. Luc Renouil soulignait qu'il fallait savoir ce qui doit être protégé. C'est fait, tant du point de vue des équipements que des services. Au sein de l'État, la stratégie, en matière de cybersécurité, est assez claire. En revanche, elle ne peut être définie dans un horizon plus long que deux ou trois ans. Il m'est impossible de savoir ce qui peut se produire dans un horizon plus long en matière d'attaques informatiques. Le Livre blanc sur la défense et la sécurité nationale paru en 2008 évoquait le grand risque de DDoS. L'ANSSI a adopté en conséquence une stratégie en 2010. On a découvert quelques mois plus tard que les attaques les plus importantes relevaient d'*Advanced Persistent Threats (APT)*. Nous avons alors dû changer de fusil d'épaule et faire évoluer notre stratégie. Je ne suis pas sûr que nous ayons suffisamment de visibilité, au-delà de deux ou trois ans, pour lancer les programmes industriels permettant de savoir ce que les attaquants vont faire dans deux ou trois ou quatre ans.

La France est souvent brocardée pour son incapacité à travailler avec l'Europe. Elle a pourtant largement inspiré la directive dite « Nice », votée par le Parlement européen en mars 2014, qui constitue en quelque sorte l'équivalent d'une loi de programmation militaire à l'échelle européenne. Nous avons déjà transposé ces principes dans notre droit, d'une certaine manière.

Je terminerai par les PME. Nous avons un tissu industriel de 600 PME très innovantes, selon le recensement que nous avons effectué. Elles commencent à se regrouper et *Hexatrust* en est un très bon exemple.

M. Bruno Sido. – Merci à tous d'avoir apporté vos témoignages au cours de l'ensemble de cette journée extrêmement instructive ; d'autant plus que vous avez pu réagir aux propos tenus par les uns et les autres.

Cette table ronde sera particulièrement utile aux rapporteurs que nous sommes. Mme Anne-Yvonne Le Dain s'associe à mes remerciements.

LISTE DES PERSONNES ENTENDUES PAR LES RAPPORTEURS

A

M. Serge **Abiteboul**, membre du Conseil national du numérique *p. 69*

M. Alexandre **Archambault**, responsable des affaires réglementaires, en charge des obligations légales, *Free* *p. 360*

B

M. Gilles **Babinet**, responsable des enjeux de l'économie numérique pour la France (*French Digital Champion*), Commission européenne *p. 247*

Mme Catherine **Becchetti-Bizot**, inspecteur général de l'éducation nationale, directrice du projet stratégie numérique, Ministère de l'éducation nationale, de l'enseignement supérieur et de la recherche *p. 193*

M. Ahmed **Bennour**, directeur des systèmes d'information, *Areva* *p. 346*

Mme Pascale **Bernal**, directeur du système d'information, *Gaz réseau distribution France (GrDF)* *p. 357*

M. Jean-Luc **Beylat**, président du Pôle Systematic Paris-Région *p. 386*

M. Jean-Marie **Bockel**, sénateur, membre de la commission des affaires étrangères, de la défense et des forces armées du Sénat *p. 9*

M. Éric **Bruni**, chef du service de la sécurité de défense et des systèmes d'information, Direction générale de l'armement (DGA) *p. 111*

Mme Agnieszka **Bruyère**, directrice de services de sécurité, *IBM France* *p. 388*

C

Me Éric **Caprioli**, docteur en droit, avocat à la Cour d'appel de Paris, vice-président du Club des experts de la sécurité de l'information et du numérique (CESIN) *p. 325*

M. Pascal **Chauve**, conseiller du secrétaire général de la défense et de la sécurité nationale (SGDSN) *p. 257*

M. Jean-Marie **Chesneaux**, vice-président de la Conférence des directeurs des écoles françaises d'ingénieurs (CDEFI) et directeur de Polytech'Paris-UPMC *p. 146, p. 211*

M. Maxime **Chipoy**, responsable des études, *UFC-Que-Choisir* *p. 298*

D

M. Lionel **Darasse**, chef du service de protection des activités classées et des informations (SPACI), direction centrale de la sécurité, Commissariat à l'énergie atomique et aux énergies alternatives (CEA) *p. 349*

M. Christian **Daviot**, chargé de la stratégie auprès du directeur général, Agence nationale de la sécurité des systèmes d'information (ANSSI) *p. 365, p. 406*

M. Éric **Delbecque**, chef du département de sécurité économique, Institut national des hautes études de la sécurité et de la justice (INHESJ) *p. 221*

Mme Mireille **Delmas-Marty**, membre de l'Institut de France (Académie des sciences morales et politiques), professeur honoraire au Collège de France (études juridiques comparatives et internationalisation du droit) *p. 263*

Me Pierre **Desmarais**, avocat à la Cour d'appel de Paris, correspondant informatique et libertés, spécialisé dans les questions de sécurité numérique *p. 329*

M. Gilles **Dowek**, directeur de recherche à l'Institut national de recherche en informatique et en automatique (INRIA), responsable du secrétariat du groupe de travail sur le rapport de l'Académie des sciences « *L'enseignement de l'informatique en France, Il est urgent de ne plus attendre* » *p. 211, p. 223*

Mme Cécile **Dubarry**, chef du service des technologies de l'information et de la communication à la Direction générale de la compétitivité, de l'industrie et des services (DGCIS) *p. 159*

E

M. Réza **El Galai**, ingénieur projet cybersécurité, Conférence des directeurs des écoles françaises d'ingénieurs (CDEFI) *p. 145*

F

Mme Anne-Florence **Fagès**, directrice de mission « *Économie numérique* » à la direction de la recherche et de l'innovation, MEDEF *p. 163*

Mme Isabelle **Falque-Pierrotin**, présidente de la Commission nationale de l'informatique et des libertés (CNIL) *p. 241*

Me Christiane **Féral-Schuhl**, avocat spécialisé en droit de l'informatique et des technologies, ancien bâtonnier du Barreau de Paris *p. 276*

M. Éric **Filiol**, directeur du laboratoire de cryptologie et de virologie opérationnelles, École supérieure d'informatique électronique automatique (ESIEA) Ouest *p. 181*

M. Thierry **Floriani**, responsable de la sécurité des systèmes d'information, *Numergy* *p. 376*

Colonel Éric **Freyssinet**, coordinateur du plateau d'investigation Cybercriminalité & Analyses Numériques (PI CyAN) - Pôle judiciaire de la gendarmerie nationale *p. 103*

G

M. Michel **Gagneux**, président de l'Agence des systèmes d'information partagés de santé (ASIP Santé) *p. 151*

M. François **Germinet**, président de l'Université de Cergy-Pontoise, président du comité numérique à la Conférence des présidents d'université (CPU) *p. 215*

M. Lionel **Gervais**, directeur de la stratégie, *Airbus Defence & Space - CyberSecurity* *p. 373*

M. Jean-Marc **Grémy**, vice-président du Club de la sécurité de l'information français (CLUSIF) *p. 404*

M. Hervé **Guillou**, président du Conseil des industries de confiance et de sécurité (CICS) *p. 47*

H

M. Patrick **Hereng**, directeur des systèmes d'information et télécommunications, *Total* p. 95

M. Laurent **Heslault**, directeur des stratégies de sécurité, *Symantec en France* p. 382

M. Charles **Huot**, président d'*Aproged*, président du comité éditorial du portail *Alliance Big Data* p. 272

I

M. Badi **Ibrahim**, directeur des opérations, *P1 Security* *p. 396*

J

M. Alain **Juillet**, président du Club des directeurs de sécurité des entreprises (CDSE) *p. 131*

K

Mme Sophie **Kwasny**, chef de l'unité de protection des données personnelles, Conseil de l'Europe *p. 15*

M. Daniel **Kofman**, professeur à Telecom ParisTech, directeur du LINCS, membre du Conseil scientifique de l'OPECST *p. 193*

L

M. Pierre **Lasbordes**, ancien député, ancien membre de l'OPECST *p. 288*

Lieutenant-colonel Philippe **Le Bouil**, chef de bureau, Direction de la protection et de la sécurité de la défense (DPSD) *p. 119*

M. Gwendal **Le Grand**, directeur des technologies et de l'innovation, Commission nationale de l'informatique et des libertés (CNIL) *p. 25*

Mme Axelle **Lemaire**, Secrétaire d'Etat chargée du numérique, auprès du ministre de l'économie, du redressement productif et du numérique *p. 314*

M. Pierre **Léna**, professeur émérite, membre de l'Académie des sciences, président et cofondateur de la Fondation de coopération scientifique pour l'éducation à la science « *La main à la pâte* » *p. 197*

M. Stéphane **Lenco**, membre du Bureau, Groupement interprofessionnel pour les techniques de sécurité des informations sensibles (GITSIS) *p. 402*

M. Yves **Le Mouël**, directeur général de la Fédération française des télécoms (FFT) *p. 79*

M. Christian **Lerminiaux**, président de la Conférence des directeurs des écoles françaises d'ingénieurs (CDEFI) *p. 146*

M. Pierre **Louette**, président du comité « *Transformation du numérique* », MEDEF *p. 163*

M

Mme Valérie **Maldonado**, chef de service, Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) *p. 332*

M. Philippe **Marquet**, vice-président, Société informatique de France (SIF) *p. 213*

M. Stanislas **de Maupeou**, directeur du secteur conseil en sécurité et évaluation, *Thales* *p. 371*

M. Thiébaut **Meyer**, responsable de la sécurité des systèmes d'information, Présidence de la République *p. 87*

M. Jean-Luc **Moliner**, président de la commission sécurité de la Fédération française des télécoms (FFT) *p. 81*

N

Lieutenant-colonel Jean-Dominique **Nollet** de la Gendarmerie nationale, chef d'unité de laboratoire de recherche, Centre européen de lutte contre la cybercriminalité (EC3) à Europol *p. 268*

M. Jérôme **Notin**, président de *Nov'IT* *p. 39*

O

M. Bernard **Ourghanlian**, directeur technique et sécurité, *Microsoft France*, administrateur, *Syntec-numérique* *p. 393*

P

M. Jean-François **Parguet**, directeur du pôle technique et sécurité de l'Agence des systèmes d'information partagés de santé (ASIP Santé) *p. 153*

M. Lazaro **Pejsachowicz**, président du Club de la sécurité de l'information français (CLUSIF) *p. 55*

Mme Sophie **Pène**, professeur en sciences de l'information et de la communication, Université Paris Descartes, membre du Conseil national du numérique *p. 201*

M. Guillaume **Poupard**, directeur général, Agence nationale de la sécurité des systèmes d'information (ANSSI) *p. 220*

M. Cédric **Prévost**, directeur sécurité et de la qualité des programmes, *Cloudwatt* *p. 61, p. 380*

M. Louis **Pouzin**, président d'*Open-root* *p. 139*

Q

M. Jean-Pierre **Quémard**, vice-président *security and technology communication intelligence and security* (*Airbus Defence and Space*), président de la commission de normalisation SSI et chef de délégation française à l'*ISO/IEC* JTC1/SC27 *p. 50, p. 303*

Mme Myriam **Quéméner**, magistrat, spécialiste des problèmes de la cybersécurité *p. 229*

R

M. Luc **Renouil**, directeur du développement et de la communication, *Bertin Technologies*, vice-président de l'association *Hexatrust* d'éditeurs français de la confiance numérique *p. 391*

Mme Claude **Revel**, déléguée interministérielle à l'intelligence économique *p. 171*

M. Gérard **Roucairol**, président de l'Académie des technologies, membre du Conseil scientifique de l'OPECST *p. 206*

M. Pierre **Ricono**, chef du département Campus technologique, direction des éditions et du transmédia, Universcience *p. 203*

S

M. Éric **Sadin**, écrivain et philosophe *p. 21*

M. Jean-Baptiste **Soufron**, secrétaire général, Conseil national du numérique *p. 70*

M. Bernard **Stiegler**, philosophe, directeur de l'Institut de recherche et d'innovation du Centre Georges Pompidou (IRI), membre du Conseil national du numérique *p. 288*

T

M. Jean-Jacques **Tourre**, responsable de la sécurité des systèmes d'information, *Total* *p. 353*

V

M. Benoît **Virole**, docteur en psychopathologie, docteur en sciences du langage, membre de l'Observatoire des mondes numériques en sciences humaines (OMNSH) *p. 336*

V

M. Philippe **Wolf**, ingénieur général de l'armement, auteur de nombreux articles et ouvrages sur le numérique *p. 309, p. 320*