N° 663

SÉNAT

SESSION ORDINAIRE DE 2013-2014

Enregistré à la Présidence du Sénat le 27 juin 2014

RAPPORT D´INFORMATION

FAIT

au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) sur le **numérique***, le* **renseignement** *et la* **vie privée** *: de* **nouveaux défis** *pour le* **droit***,*

Par M. Jean-Pierre SUEUR,

Sénateur.

(1) Cette commission est composée de : M. Jean-Pierre Sueur*, président ;* MM. Jean-Pierre Michel, Patrice Gélard, Mme Catherine Tasca, M. Bernard Saugey, Mme Esther Benbassa, MM. François Pillet, Yves Détraigne, Mme Éliane Assassi, M. Nicolas Alfonsi, Mlle Sophie Joissains*, vice-présidents ;* Mme Nicole Bonnefoy, MM. Christian Cointat, Christophe-André Frassa, Mme Virginie Klès*, secrétaires ;* MM. Alain Anziani, Philippe Bas, Christophe Béchu, François-Noël Buffet, Vincent Capo-Canellas, Luc Carvounas, Gérard Collomb, Pierre-Yves Collombat, Jean-Patrick Courtois, Mme Cécile Cukierman, MM. Michel Delebarre, Félix Desplan, Christian Favier, René Garrec, Mme Jacqueline Gourault, MM. François Grosdidier, Jean-Jacques Hyest, Philippe Kaltenbach, Mme Isabelle Lajoux, MM. Jean-René Lecerf, Jean-Yves Leconte, Antoine Lefèvre, Roger Madec, Jean Louis Masson, Jacques Mézard, Thani Mohamed Soilihi, Hugues Portelli, André Reichardt, Alain Richard, Simon Sutour, Mme Catherine Troendlé, MM. René Vandierendonck, Jean-Pierre Vial, François Zocchetto.

S O M M A I R E

Pages

PRÉFACE 5

OUVERTURE 7

PREMIÈRE TABLE RONDE - Les nouvelles technologies, une menace pour la vie privée ? 11

DEUXIÈME TABLE RONDE - Entreprises de la nouvelle économie et vie privée 21

TROISIÈME TABLE RONDE - Prévention/répression de la criminalité et atteintes à la vie privée 33

QUATRIÈME TABLE RONDE - Quelles règles de droit pour les nouvelles technologies ? 49

CONCLUSION 59

ANNEXE 1 - Programme du colloque 67

ANNEXE 2 - Glossaire 69

PRÉFACE

UNE JOURNÉE D'ÉTUDES SUR LE « NUMÉRIQUE, RENSEIGNEMENT ET VIE PRIVÉE »

LE 22 MAI 2014 AU SÉNAT

Il est souvent reproché au législateur de légiférer en réaction à des événements qui ont suscité une intense émotion, dans l'urgence et sans vision d'ensemble. Toutefois, les parlementaires prennent aussi le temps de la réflexion sur les grandes évolutions qui traversent notre société.

C'est ainsi que la commission des lois du Sénat a mené plusieurs travaux d'information sur l'effet **des nouvelles technologies sur la vie privée et sur les autres droits fondamentaux**. En 2008, elle adoptait un rapport d'information présenté par Mme Anne-Marie Escoffier et M. Yves Détraigne intitulé : « *La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information* ». Plus récemment, en mars 2012, elle a apporté une contribution importante à l'élaboration de la loi relative à la protection de l'identité. Par ailleurs, en avril 2014, la commission des lois a confié à Gaëtan Gorce et François Pillet une mission d'information consacrée à l'« *Open data et protection de la vie privée* ».

La journée d'étude du 22 mai, organisée à l'initiative de la commission des lois, a permis à une grande diversité d'intervenants de poursuivre ces réflexions : représentants des administrations, chefs d'entreprises, chercheurs, élus ont ainsi tenté de clarifier les termes du débat, et notamment de définir le statut actuel de la vie privée, entre droit fondamental, legs historique en pleine transformation, voire objet de négociation entre individus éclairés. Le débat s'est également focalisé sur la gestion des données personnelles et leur utilisation par les entreprises à des fins commerciales et a permis, en écartant les analyses trop simples, de prendre la mesure de la créativité juridique qui sera nécessaire pour concilier les intérêts divergents dans ce domaine. La dimension internationale de ces questions, de la négociation des projets de Règlement de la commission européenne à l'accord « Transatlantic Free Trade Area » (TAFTA), a également été traitée par les intervenants.

En second lieu, à l'occasion de l'examen de différents textes intéressant la sécurité, en particulier le projet de loi de programmation militaire pour la période 2014-2019, le Sénat a contribué à définir **le cadre et les limites des interventions des services de police et de renseignement susceptibles de constituer des intrusions dans la vie privée dans les seuls cas où ces services interviennent en matière de lutte contre la criminalité et le terrorisme.**

Cette question a pris une acuité toute particulière à la suite des révélations d'Edward Snowden sur les pratiques de la National security agency (NSA), qui ont déclenché un grand débat sur les nécessaires garde-fous qui, dans une société démocratique, doivent empêcher la légitime recherche d'information sur les agissements des criminels de se transformer en surveillance indifférenciée et généralisée. Là encore, les différents intervenants de la journée du 22 mai, défenseurs des libertés, membres des instances de contrôle des activités des services de renseignement et parlementaires, ont tracé des perspectives pour une rénovation du cadre juridique de la lutte contre la criminalité organisée et contre le terrorisme.

Mme Axelle Lemaire, secrétaire d'État chargée du numérique, a conclu la journée d'étude en annonçant la présentation d'un projet de loi relatif à la question de la protection des données personnelles et de la vie privée.

OUVERTURE

M. Jean-Pierre Sueur, président de la commission des lois. – Je vous souhaite, à tous, au nom de Jean-Pierre Bel et de tous nos collègues de la commission des lois – car ce colloque procède de l'initiative de cette commission – la bienvenue au Sénat.

Nous avons vécu un certain nombre d'événements marquants au cours des derniers mois. D'abord, la loi de programmation militaire. Son article 13, devenu article 20, a été voté par de larges majorités au Sénat puis à l'Assemblée nationale. Notre objectif était de mettre en œuvre des avancées en termes de contrôle et de liberté par rapport à la loi de 1991. Pendant un mois après le vote de la loi, rien ne s'est produit. Et puis l'Association des services Internet communautaires (ASIC), qui rassemble les majors du net comme Google, Yahoo ou Facebook, publie un communiqué prétendant que cette loi menaçait les libertés. Or le débat avait eu lieu dans les deux chambres sans soulever aucune critique de cette nature – vous direz que je récris l'histoire… Ce communiqué a été suivi par un autre, et encore un autre... La télévision et la radio ont organisé des débats ; la Ligue des droits de l'homme, dont je suis membre depuis quarante ans, s'est alarnée à son tour.

Or dans cette loi, nous n'avons fait qu'accroître les protections. Je précise que l'article 20 traite du contenant et non du contenu. En outre, les critiques confondent les écoutes administratives et judiciaires.

Il faut que les services de renseignement soient efficaces dans la lutte contre le terrorisme. Nous y sommes attentifs. Mais nous sommes aussi les gardiens des libertés et de la vie privée. Il y a là deux exigences auxquelles nous tenons. Et nous tenons autant à l'une et à l'autre.

On nous reproche d'étendre le champ des interceptions administratives à l'action économique. Ceux qui s'en émeuvent devraient se replonger dans la loi de 1991 qui le prévoyait déjà. Les fadettes ne demeurent accessibles qu'après autorisation écrite du Premier ministre. Et la géolocalisation est conditionnée – innovation ! – à une demande écrite et motivée faite au Premier ministre. Nous sortons ainsi de la loi de 2006, qui était une loi de circonstance, pour stabiliser le dispositif. Rien donc dans ce que nous avons voté ne porte atteinte aux libertés, tout au contraire.

Cette loi a été suivie par celle relative à la géolocalisation, rendue nécessaire par deux décisions de la Cour de cassation. À nouveau nous avons travaillé et avons eu le sentiment de renforcer la protection des libertés. Nous avons décidé que la géolocalisation ne serait possible que pour les infractions punies de cinq ans d'emprisonnement parce que la Cour européenne des droits de l'homme (CEDH) la limite aux infractions « d'une particulière gravité ». Nous avons rendu, en outre, le contrôle du juge obligatoire sous quinze jours – tout cela procède de l'arrêt Uzun de la CEDH.

Nous avons autorisé l'Officier de police judiciaire (OPJ) à procéder à un géolocalisation en cas de risque de disparition des preuves. Nous avons renforcé considérablement les garanties en ce qui concerne les intrusions dans le domicile privé en exigeant l'accord du procureur et du juge des libertés et de la détention pour que la géolocalisation puisse y être possible. Enfin, nous avons trouvé une formulation raisonnable sur le « double dossier ».

La loi sur la géolocalisation renforce donc les contrôles et les pouvoirs du juge, et protège mieux les libertés. Nous avons, en outre, voté la semaine dernière un nouveau projet de loi qui conforte les droits de la désense.

La délégation parlementaire au renseignement, qui travaille beaucoup, s'est penchée sur l'affaire Snowden et ses conséquences. Le président de la République, que nous sommes allés voir, s'est engagé à ce que la coopération entre les services français et américains ne porte que sur ce qui concerne la lutte contre le terrorisme et la violence organisée ainsi que la défense des intégrités territoriales. Nous avons remis au président de la République un rapport. Son contenu n'est pas intégralement public, secret défense oblige, mais l'un de ses paragraphes mérite l'attention. Je le lis : « Notre pays ne dispose pas à ce jour d'un véritable régime juridique complet définissant avec précision les missions et les activités des services de renseignements ainsi que les moyens dont ils disposent, et prévoyant les modalités de leur encadrement et de leur contrôle ». Cela veut dire que notre activité de renseignement nous avons salué les agents des services qui se dévouent sans relâche et avec courage, dans des conditions souvent périlleuses n'est pas suffisamment encadrée. Soyons clairs : le dispositif législatif actuel est insuffisant. Nous avons besoin d'une nouvelle loi.

Notre logique diffère de celles des services américains : nous refusons la captation massive et indifférenciée de données et nous considérons que la recherche du renseignement doit être ciblée.

J'ajoute que les interceptions administratives sont contrôlées par la Commission nationale de contrôle des interceptions de sécurité (CNCIS), dont les moyens sont notoirement insuffisants. De son côté, le rapport Urvoas-Verchère préconise la création d'une inspection. Il faut, indiscutablement, faire plus et mieux.

Je le répète : Le législateur doit avoir deux soucis majeurs : lutter contre la menace terroriste, la violence organisée, les atteintes à l'intégrité territoriale, les autres atteintes à la Nation, et protéger les libertés, le respect dû à la vie privée et les données personnelles. Ce sont deux impératifs majeurs.

Vous avez suivi l'actualité, vous savez les travaux de la CNIL, le débat relatif au droit à l'oubli – de récentes décisions de justice ont fait avancer les choses – qu'il faut concilier avec la conservation nécessaire de traces historiques, etc.

En un mot, sur toutes ces questions, les débats sont multiples. Et il faut absolument faire évoluer notre législation et nos textes réglementaires afin de prendre en compte les évolutions considérables que nous connaissons dans tous ces domaines en gardant toujours les mêmes objectifs : lutter contre le terrorisme ET protéger les libertés.

Cette journée d'étude a pour objet d'aborder ces problèmes avec tous les acteurs et partenaires concernés, dans leur grande diversité, de vous écouter et de réfléchir ensemble aux nouvelles législations nécessaires.

Je vous remercie sincèrement d'avoir bien voulu accepter d'y participer.

PREMIÈRE TABLE RONDE
Les nouvelles technologies, une menace pour la vie privée ?

Mme Christiane Féral-Schuhl, ancien bâtonnier du barreau de Paris

M. Philippe Aigrain, Quadrature du net

M. Antonio Casilli, maître de conférence en humanités numériques à Telecom Paris Tech et chercheur au Centre Edgar-Morin de l'EHESS

M. Benoît Tabaka, directeur des politiques publiques de Google France

(de gauche à droite : Mme Christiane Féral-Schuhl, M. Philippe Aigrain, Mme Éliane Assassi, M. Benoît Tabaka, M. Antonio Casilli, M. Jean-Pierre Sueur)

Mme Éliane Assassi, présidente. – Je veux remercier Jean-Pierre Sueur, qui a planté le décor avec le talent et la franchise qui lui sont coutumiers. Rentrons dans le vif du sujet : les technologies ont-elles un effet sur la vie privée, les représentations que l'on s'en fait et sur les pratiques juridiques ? D'aucuns considèrent à l'inverse qu'il n'y a plus de vie privée à défendre…

Mme Christiane Féral-Schul, ancien bâtonnier du barreau de Paris. – Je m'adresse à une assemblée de citoyens du XXIe siècle, forcément composée de personnes connectées aux réseaux sociaux, aboutissement de l'évolution technologique depuis 1992-1993. Les adolescents ont désormais troqué leurs carnets secrets contre des pages Facebook. J'y vois un bouleversement culturel profond.

Quelques chiffres : 2,4 milliards d'internautes dans le monde, 54 millions en France (+ 566% depuis 2000) ; 68 % des Français sont inscrits sur un réseau social. Chacun passe quatre heures par jour devant son ordinateur, une heure sur son mobile. Chaque minute, dans le monde, deux millions de requêtes sont faites sur Google, 571 nouveaux sites, 2 000 nouvelles photos sont postées sur Tumblr, 204 millions d'e-mails sont envoyés ; 90% de nos données numériques ont été créées ces deux dernières années.

L'internaute est schizophrène, qui exige simultanément liberté de s'exprimer sans entrave et protection de son intimité. Souvenez-vous des débats suscités par la localisation rendue possible par la carte Navigo… Les victimes d'agression dans le métro s'étonnent pourtant qu'on ne puisse retrouver les coupables ! Autres exemples : la vidéosurveillance dans les halls d'immeuble ou le déshabillage numérique dans les aéroports : on ne comprendrait pas qu'il n'y ait pas de contrôles. À la vérité, nous passons sans cesse d'une revendication à l'autre.

Les réseaux sociaux fonctionnent précisément sur le dévoilement, la fourniture libre de données personnelles, qui finissent par cerner les personnes. Cela commence par les bulletins de promotion dans les boutiques : nous sommes des victimes consentantes. Sur le réseau, la dichotomie espace privé-espace professionnel fait débat. Dans l'esprit de beaucoup, privé signifie confidentiel. Or l'espace privé n'est pas compatible avec le modèle économique de ces réseaux. C'est un problème culturel.

Peut-on retirer les données fournies librement ? L'Internet a une mémoire d'éléphant. Rien ne s'y perd. En outre, tout préjudice a un écho planétaire. On comprend la demande d'effacement d'une vidéo compromettante de la part de celui qui craint d'en souffrir, mais qui va être juge de l'histoire ? Nous en reparlerons en évoquant la décision de la Cour de justice de l'Union européenne du 13 mai 2014.

Il n'y a pas de prescription légale sur Internet. La photographie d'une personne suspectée d'infraction restera sur le réseau, qu'elle ait été finalement blanchie ou qu'elle ait payé sa peine. Dès que chaque internaute s'improvise diffuseur d'information sans avoir l'éthique d'un journaliste, l'on mesure les dégâts. Les informations mélangent vrai, vraisemblable et mensonge, injure et diffamation ; elles posent la question des atteintes à la vie privée, à la protection de laquelle nous avons tous droit.

Nous défendons le respect de ce principe sans prêter attention à nos propres responsabilités. Ouvrir un compte sur Gmail, c'est accepter de voir ses informations livrées à l'administration américaine si elle en fait la demande. Les données ne se perdent pas, et les préjudices ne sont guère réparables. Renforçons l'autocontrôle, changeons de culture.

Internet n'en demeure pas moins un formidable outil de partage et de promotion de valeurs fortes. Trouvons un point d'équilibre et laissons l'Etat jouer son rôle et apporter de la sécurité au citoyen. *(Applaudissements)*

M. Antonio Casilli, maître de conférences en humanités numériques à Telecom ParisTech et chercheur au Centre Edgar-Morin de l'EHESS. – Je veux questionner l'idée selon laquelle la vie privée serait vouée à disparaître du fait de l'évolution technologique. Le 6 juin 2014, nous fêterons le premier anniversaire des révélations d'Edward Snowden, événement fondateur de nouvelles relations entre les individus et les administrations.

De nouveaux usages ont émergé. En 2013, un rapport de l'Information Technology and Innovation Foundation (ITIF) * a révélé que les pertes enregistrées par les sociétés américaines du *cloud* en raison de l'érosion de la confiance des utilisateurs ont atteint entre 22 et 35 milliards de dollars. Des applications anonymes ou éphémères, comme *Snapchat*, sont plébiscitées – au point que c'est devenu une stratégie commerciale. J'y vois un changement de discours important. Les GAFA* (Google, Apple, Facebook et Amazon) sont contraints de s'adapter.

Scott McNealy, président de Sun Microsystems déclarait en 1999 : « Vous n'avez aucune vie privée. Tournez la page ». Mark Zuckerberg a repris ses propos en 2010, estimant que la vie en public était la nouvelle norme. En 2011, Paul Hermelin, de Capgemini ne disait rien d'autre. Vint Cerf, évangéliste en chef chez Google, a assuré en 2013 que la vie privée était une anomalie de l'histoire. La vie privée, qui s'était affirmée avec la bourgeoisie urbaine, refluait devant de nouvelles formes de vie communautaire.

La vie privée était nulle parce que non avenue… les discours masquent en fait une véritable guerre culturelle entre utilisateurs de grandes plateformes sociales, États, acteurs de l'économie traditionnelle, entreprises innovantes. Il faut sortir de ce cadre idéologique.

La vie privée n'a pas disparu, elle s'est transformée : elle n'est plus une sphère susceptible d'être pénétrée, mais un espace de négociation avec les autres acteurs. La première conception est héritée de la tradition libérale, fondée sur le droit à être laissé en paix, comme le définissaient Samuel Warren et Louis Brandeis dans un article paru en 1890 dans la Harvard Law

* *Cf. glossaire, p. 69*

Review. Pourtant l'internaute surfe sur Internet non pour être laissé en paix mais pour développer ses relations sociales, dont il négocie les codes et les paramètres, tout en en gardant la maîtrise. Il ne s'agit plus seulement de contrôler ce que l'on divulgue, mais de contrôler ce que les autres publient sur nous, dans une négociation permanente. Or nos pouvoirs de négociation sont faibles et doivent être renforcés.

Il ne s'agit pas d'une négociation au sens commercial, même si certaines *start-up* comme Yesprofile.com proposent de monétiser la protection des données personnelles. Il s'agit d'une négociation collective pour renouveler le cadre légal, changer de paradigme ; car nous passons d'un web de publication à un web d'émission de données. *(Applaudissements)*

M. Philippe Aigrain, Quadrature du net. – Nous sommes ici car une personne a sacrifié une partie de sa vie pour nous révéler le fonctionnement des services de renseignement et la contribution – non contrainte et forcée – des géants de l'Internet.

Notre premier devoir est d'aider M. Snowden. En juillet, l'asile temporaire qui lui a été accordé par la Russie prendra fin. Nous avons un devoir absolu. Conformément à l'article 53-1 de la Constitution, « *les autorités de la République ont toujours le droit de donner asile à tout étranger persécuté en raison de son action en faveur de la liberté ou qui sollicite la protection de la France pour un autre motif* ».

Le Parlement européen a mené un travail d'enquête à la suite de ces révélations. Son rapport a recommandé la suspension du *Safe Harbor Agreement*, qui permet aux opérateurs américains de transférer aux États-Unis des données collectives en Europe pour les retraiter. La captation des données n'a cessé de s'accroître. Pour vous en convaincre, lisez *Liberté et sûreté dans un monde dangereux* de Mireille Delmas-Marty. Ce modèle ne repose plus sur le consentement, mais sur des abus. A l'issue d'une réunion organisée par Peter Fletcher, de Google, les représentants des internautes ont refusé de s'opposer à des approches règlementaires de la CNIL, parce qu'il était impossible de faire confiance à une société dont les revenus reposent sur une utilisation abusive des données.

Pourquoi invoquer la sécurité ? Dans ce pays, le seul attentat récent a été mené par une personne dénoncée par sa famille, surveillée pendant des années, mais qui avait échappé aux radars. Le responsable de la NSA a reconnu avoir menti au Congrès en indiquant que le modèle de collectivisme des données a évité des attentats. Il est essentiel que les lois nous donnent un nouveau pouvoir de négociation, selon le terme de M. Casilli, face aux entreprises et aux États.

Ce n'est pas une vue de l'esprit. Les adolescents américains fuient désormais massivement les réseaux sociaux traditionnels comme Facebook au profit de médias sociaux comme Tumblr, par désillusion, afin de retrouver des relations authentiques sur le net. Le système Échelon reposait sur la captation des flux de données. Les services secrets disposent grâce à

Internet, non seulement des flux mais des moyens nécessaires à leur interprétation. Les données du web se sont centralisées à la fin des années 2000. Ce n'est pas le modèle original du web, fondé sur la décentralisation des contenus. Or, la centralisation n'est pas une loi de nature. Avant d'être un média de communication, le web est un moyen d'expression : il y a 180 millions de blogs.

La loi numérique devra protéger davantage les citoyens face aux autorités administratives qui agissent comme des bulldozers. Dans le même temps, il incombera au politique de favoriser la décentralisation : dans la nouvelle négociation collective, les utilisateurs qui possèdent les données, sont au cœur du processus. Espérons que ce mouvement aboutira à des avancées législatives. *(Applaudissements)*

M. Benoît Tabaka, directeur des politiques publiques de Google France. – La question essentielle est celle de l'usage. Nous vivons dans une société du partage. Les acteurs d'Internet sont tenus de répondre aux nouvelles demandes. La première est celle de mieux informer.

Google a une activité liée aux régies publicitaires. La publicité peut être personnalisée. Notre devoir est d'en informer l'internaute et de lui donner les moyens de gérer ses paramètres et de désactiver ce service. De même, il nous incombe d'informer les personnes qui ont été « flaguées », ou d'offrir aux usagers la possibilité de retirer une vidéo. Chacun doit pouvoir choisir avec qui il partage ses données. L'émergence sur le réseau des communautés privées en découle.

La confiance est essentielle. Si l'usager d'un service n'a plus confiance en celui-ci, il doit pouvoir en sortir. C'est pourquoi Google s'efforce de développer la portabilité des données.

Le deuxième aspect est la sécurité des données. Les attaques informatiques, les piratages se multiplient. Le *phishing*, ou l'hameçonnage, consiste à dérober les données personnelles pour s'emparer de certains éléments de la vie privée d'un individu. Nous essayons de développer les outils pour protéger les internautes, par exemple en les avertissant des connexions suspectes.

Autre danger, les interceptions. Elles ne sont pas seulement judiciaires ou administratives, elles concernent aussi l'utilisateur d'un réseau wifi public – celui d'un café par exemple. Le fournisseur de services internet doit, là aussi, veiller à renforcer la sécurité, grâce à des chiffrements – le SSL notamment, dont les révélations de Snowden ont montré la nécessité. Chez Google, depuis plusieurs mois, le chiffrement des données e-mails n'est plus désactivable par l'utilisateur et celui des requêtes faites dans le moteur de recherche est automatique.

Des autorités publiques peuvent demander à accéder aux données d'identification si une adresse IP a une activité illicite. Le régime de l'interception suppose une intervention préalable du juge. Enfin, les services de renseignement s'efforcent d'accéder aux données dans un cadre a-légal par la collecte massive de données sur les réseaux. Nous veillons à la

transparence et au respect des cadres juridiques. Nous examinons chaque demande, quitte à la contester en justice. Il faut renforcer les garde-fous.

L'Asic qui compte aussi des sociétés françaises, a exprimé des craintes à propos de la loi de programmation militaire, car elle laisse entendre que les services de renseignement ont, par des interceptions administratives, accès à toutes les données stockées sur Internet. Ce cadre n'est pas clair. Or quand il y a un flou, il y a un loup. L'accès à des documents, contrairement aux écoutes téléphoniques, est pérenne et rend inefficace le contrôle *a posteriori :* les documents ont été interceptés. De même, la loi sur la géolocalisation ne précise pas le concept d'objet pouvant être géolocalisé : ce peut être une automobile comme une brosse à dent connectée, puisque la chose existe désormais. Nous attendons plus de transparence et de garde-fous du cadre juridique car les technologies évoluent très vite. *(Applaudissements)*

M. Philippe Aigrain, Quadrature du net. – Aucun intervenant n'a dit que la Cour de justice de l'Union européenne (CJUE) avait invalidé la directive de 2006 sur la rétention des données pour atteinte aux droits fondamentaux – ce n'est pas banal. Une grande partie des textes qui ont été mentionnés ce matin n'ont plus de base juridique.

M. Jean-Pierre Sueur, président de la commission des lois. – L'ASIC regroupe de très grandes entreprises mondiales. Oserai-je l'appeler à faire preuve d'humilité ? Elle a publié un communiqué un mois après le vote de la loi. Or la géolocalisation suppose une demande motivée au Premier ministre et une réponse motivée ; ensuite le concours des opérateurs est sollicité. Le paradoxe est que ceux qui dénoncent un risque sont ceux qui ont livré des milliards de données à la National security agency (NSA) ! *(Applaudissements)*

(Échanges avec la salle)

M. Gilles Trouessim. – Ancien du CNRS, je suis consultant en sécurité informatique. Ne doit-on pas privilégier le droit à l'oubli *a priori*, la séclusion : ce n'est pas parce que j'ai rien à cacher que je n'ai rien à cacher… Une donnée publiée reste stockée à jamais. À titre personnel je n'ai pas de page Facebook, ni de page Linkedin. Au-delà de la cryptographie, il est possible de développer des techniques en amont, comme la carte blanche à l'anonymat provisoire.

M. Antoine Lefébure. – Je suis l'auteur d'un livre sur l'affaire Snowden…

M. Jean-Pierre Sueur, président de la commission des lois. – Bravo !

M. Antoine Lefébure. – M. Tabaka m'a déçu. Plutôt que de nous expliquer vos tentatives de chiffrage, pourquoi ne pas avouer que vous n'avez pas les moyens techniques et juridiques de nous protéger contre les services de renseignements ? La vérité, c'est que vous devriez vous tourner vers le législateur, seul légitime à intervenir, car notre modèle économique souffre de l'érosion de la confiance des utilisateurs.

M. André Alix. – Où vont les données ? On ne le sait pas. Je suis pour leur effacement. L'usurpation d'identité est un fléau qui se développe.

Les *smartphones* et les tablettes se multiplient ; Google en profite avec son Play Store, qui n'offre pas de protection contre les *malwares*[*]. Pourquoi la France, qui en est friande, ne créerait-elle pas un label en fonction de la sécurité ?

De même, il serait bon de savoir où sont stockées les données. Le droit du pays d'ouverture du compte Gmail devrait s'appliquer. En France, nous avons la chance d'avoir la Commission nationale de l'informatique et des libertés (CNIL), qui réalise un excellent travail.

M. Daniel Latrémolière. – Informer les personnes non accusées qu'elles ont été écoutées contribuerait largement à la confiance.

M. Sylvain Cabot. – Pourquoi ne pas sensibiliser les utilisateurs des réseaux sociaux dans un souci de prévention ? Toute donnée mise en ligne n'appartient plus vraiment à celui qui l'a publiée. Quant aux labels, ils existent déjà. Le Play Store de Google en contient. Rendons-les plus visibles.

M. Benoît Tabaka, directeur des politiques publiques de Google France. – Nos efforts en matière de sécurité ne sont pas de la poudre aux yeux, mais procèdent d'une obligation légale. Chez Google, 400 ingénieurs travaillent en permanence à améliorer la sécurité : en novembre, la clef de cryptage SSL est passée de 1 084 à 2 048 kbits. Nous sommes les seuls à l'avoir fait ! De même, nous cherchons à protéger les utilisateurs contre les interceptions – d'origine gouvernementale parfois, dirigées contre des journalistes – et à les prévenir, et les conseiller. Le cadre juridique n'est pas illusoire.

Dans les systèmes d'utilisation ouverts comme Android les utilisateurs peuvent télécharger les applications sur tous les sites. La protection dépend des systèmes d'exploitation, mais aussi des développeurs d'applications, et des sites qui en proposent le téléchargement.

Notre site indique où sont situés nos *data centers*. Pour des raisons de sécurité, nous fragmentons les données et les stockons sur différents serveurs. L'aspect juridique l'emporte même sur l'aspect technique. Les autorités locales peuvent intervenir où que soient stockées les données.

[*] *Cf. glossaire, p. 69*

Enfin, l'ASIC s'est emparée tardivement de la loi de programmation militaire, parce qu'elle travaillait sur d'autres textes. En outre, cette loi ne concernait pas initialement les acteurs de l'Internet.

M. Jean-Pierre Sueur, président de la commission des lois. – Merci pour votre grande modestie. Il a fallu 31 jours pour que de grandes entreprises mondiales implantées en France découvrent que le Sénat avait débattu de la loi de programmation militaire. Cela rend à ces sociétés un aspect humain, éminemment sympathique.

M. Benoît Tabaka, directeur des politiques publiques de Google France. – S'agissant des révélations de M. Snowden, les informations captées par la NSA ont été interceptées sur le réseau, et non puisées chez les acteurs de l'Internet, comme l'a montré le schéma publié en septembre. Nous avons donné les informations sur l'accès parcellaire autorisé par la règlementation. Quasiment tous les acteurs qui en ont été victimes ont décidé d'augmenter le chiffrement des données.

M. Philippe Aigrain, Quadrature du net. – A ma connaissance, deux campagnes ont été lancées : l'une à l'initiative de la CNIL, l'autre par Quadrature du net : Contrôle tes données.net ou reclaim your data.eu. Celle-ci insiste sur le coût de la captation indue des données, celle-là souligne les dangers du net mais, en la matière, les pré-ados pourraient apprendre comment faire à ceux qui veulent leur donner des leçons. Au demeurant, les sociologues ont montré que les internautes ont appris à se protéger, parfois à leurs dépens.

Nous avons un grand besoin de faire campagne sur le chiffrement. Je souris à l'évocation du 2048 : la sécurité commence au 4096 avec un chiffrement de bout en bout. L'anonymat est profondément mis en danger. Or je n'ai pas plus entendu le gouvernement français dire qu'il allait soutenir massivement Tor* ou TED.

Les systèmes d'exploitation sont importants, en effet. Android est un système ouvert, oui, mais la *playstore*[*] de Google ne comporte plus l'application facilitant le passage vers CyanogenMod. Qui a véritablement besoin de données de géolocalisation ? L'usager, et non les opérateurs ! Pour ne pas se perdre dans les villes, le meilleur outil reste encore la carte.

Mme Christiane Féral-Schuhl ancien bâtonnier du barreau de Paris. – L'heure de la fin de la vie privée a-t-elle sonné ? Cette question nous oblige à repenser tous les fondamentaux de nos sociétés. Constatons que le droit tient plutôt bien et maintenons le respect de la vie privée comme un droit constitutionnel. Pourquoi cet affrontement permanent entre la liberté d'expression et le respect de la vie privée ? Nous ne travaillons pas pour des obsessionnels ! Il nous revient de maintenir par des moyens sécurisants le

[*] *Cf. glossaire, p. 69*

formidable outil que constitue Internet. Peut-on admettre que la liberté d'expression s'abrite derrière l'anonymat ? De même pas de droit à l'effacement sans juge de l'historique : le devoir de mémoire impose de conserver les archives de l'histoire comme de nos histoires personnelles.

J'ai trouvé significative la récente mobilisation autour de la vidéo du chaton. J'aimerais que cette autorégulation contre les dérives soit plus fréquente. Les valeurs existent sur Internet, à nous de les rassembler.

Mme Carole Miko. – Tout le monde sait que je suis là aujourd'hui car je l'ai indiqué sur Facebook ce matin… Les technologies auront toujours une longueur d'avance sur le droit. C'est pourquoi nous devons enseigner la protection de la liberté d'expression à nos enfants. La cause est peut-être perdue pour nous, à 40 ou 50 ans, mais pas pour eux.

Mme Éliane Assassi, **présidente**. – Merci pour vos interventions.

DEUXIÈME TABLE RONDE
Entreprises de la nouvelle économie et vie privée

M. Yves le Mouël, directeur général de la Fédération française des Télécoms

M. Alain Bazot, président de l'UFC Que Choisir

M. Marc Mossé, directeur des affaires publiques et juridiques de Microsoft France et membre de l'Association des services Internet communautaires (ASIC)

M. Loïc Rivière, délégué général de l'Association française des éditeurs de logiciels et solutions internet (AFDEL)

Mme Isabelle Falque-Pierrotin, présidente de la Commission nationale de l'informatique et des libertés (CNIL)

(de gauche à droite : Mme Isabelle Falque-Pierrotin, M. Yves le Mouël, M. Marc Mossé, Mme Anne-Marie Escoffier, M. Loïc Rivière, M. Alain Bazot)

Mme Anne-Marie Escoffier, présidente. – Je veux d'abord remercier M. Sueur de m'avoir demandé de présider cette table ronde. En 2009-2010,

j'avais, avec d'autres collègues, commis le premier rapport sur le droit à la vie privée, puis une proposition de loi sur celle-ci à l'ère du numérique. Le débat sur l'*homo numericus* a depuis beaucoup évolué depuis.

Mme Féral-Schul a eu raison d'insister sur les valeurs en jeu dans ces affaires : le besoin de commercialiser des marchandises heurte l'attachement à la vie privée. Nos sociétés sont marquées par l'instantanéité, le besoin d'aller vite et, simultanément mais non sans tension, celui de protection. Comment concilier ces aspirations contradictoires ?

M. Yves Le Mouël, directeur général de la Fédération française des Télécoms. – Internet – faut-il le rappeler ? – est un outil mondial. Cet outil collecte et expose des données de toute nature, dont le volume augmente avec le nombre de ses utilisateurs.

Des milliards d'objets connectés vont envahir notre quotidien. Cette révolution change notre vie, et pas seulement d'une manière diabolique : quelle formidable opportunité pour la planète ! Voyez l'évolution du bien-être individuel : par un simple bracelet, on améliore sa santé et ses performances ; l'on apprend à gérer une ville, à réaliser des économies d'énergie ; *e-call* gèrera plus efficacement les secours en cas d'accident automobile…

Ne nous voilons pas la face, nous sommes là dans un modèle marchand. Ces données sont une monnaie d'échange : information contre service. Les valeurs morales n'en sont pas pour autant exclues : les informations que l'on dissémine sont chargées d'aspects intimes. Il faut trouver un équilibre, éviter de construire des abris anti-numérique et se garder de toute naïveté. L'immédiateté et l'universalité priment.

De plus, nous sommes passés d'un monde de consommateurs s'en remettant à des sachants à un monde de producto-consommateurs aux attentes sensiblement différentes. Nous voulons tous créer un monde de confiance, de sécurité, mais laissant une large place à l'innovation. Nous autres opérateurs essayons de contribuer à ces évolutions, notamment en sécurisant les échanges. Nous ne sommes bien sûr pas seuls à lutter contre la cybercriminalité : nous agissons suivant les orientations des pouvoirs publics. C'est ainsi que le Premier ministre a récemment demandé que les serveurs d'accès aux systèmes de messagerie soient sécurisés pour les FAI, les fournisseurs d'accès à Internet ; ce chantier aboutira avant la fin de l'année. Nous collaborons avec l'administration pour le mener à bien.

Nous travaillons également en lien avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI) à sécuriser les réseaux eux-mêmes, les équipements, ainsi que les communications. Nous sommes aussi des acteurs pour les interceptions, qu'elles interviennent sur réquisition judiciaire ou selon des processus d'exception.

Le cadre dans lequel nous évoluons n'est pas seulement national : il est européen. Un projet de règlement des données personnelles est en cours

d'élaboration, pour réformer la directive de 1995. Tous les acteurs de la chaîne du numérique sont concernés, car tous ont une activité internationale. Ce projet de texte bute au moins sur deux choses. D'une part, le consentement de l'utilisateur devient illusoire quand l'internaute doit compulser d'innombrables pages et cliquer de trop nombreuses coches. Veillons à ne pas complexifier les choses à l'excès. D'autre part, attention à ne pas handicaper le développement de nos entreprises en les corsetant par nos lois. Internet est un média mondial.

Restons souples : privilégions des codes de bonne conduite plutôt que de graver dans le marbre de la loi des normes, sans cesse à préciser pour tenir compte des évolutions fulgurantes du secteur. Vivons avec notre temps, au rythme échevelé de l'Internet.

Il n'y pas de raison que nous ne bénéficions pas des mêmes possibilités de développement que d'autre acteurs, implantés sur des territoires plus larges. Une grande zone de libre-échange est en négociation avec les États-Unis. Le *Safe Harbor Agreement* doit faire partie des discussions. Il serait très dommageable que les acteurs ne soient pas soumis aux mêmes règles de part et d'autre de l'Atlantique.

Une proposition de loi relative à la biométrie a été récemment examinée par la commission des lois du Sénat. C'est un secteur porteur. Certes, il importe de préserver la sécurité des biens et des personnes, mais il s'agit aussi d'un enjeu du développement pour les entreprises françaises, particulièrement innovantes et qui comptent parmi les leaders mondiaux.

Soyons prudents : trop réglementer serait contreproductif. Soyons également avertis et développons la formation, car l'État n'est pas le seul à agir : le consommateur doit également prendre ses responsabilités. Aidons-le à le faire. (*Applaudissements*)

M. Alain Bazot, président de l'UFC-Que Choisir. – UFC-Que Choisir entend rester une vigie pour les consommateurs. Internet et le *big-bang* numérique nous invitent à tout reconsidérer sous un œil neuf. A commencer par la science économique, parce que les données personnelles apparaissent comme une matière nouvelle. Leur exploitation est de plus en plus fine, de plus en plus massive, de plus en plus valorisée économiquement. Les informations personnelles fournies par les usagers eux-mêmes font vivre certaines entreprises à titre exclusif, un comme cela se passe pour les déchets – le parallèle s'arrête là…

Devant cette révolution, la digue juridique est sur le point de céder. Il est temps de l'adapter, de revenir aux fondamentaux et de repenser ce que l'on construit sur leur base. Ayant fait des études de droit – nul n'est parfait –, j'ai encore souvenir de l'article 9 du code civil, qui proclame le droit à l'intimité de la vie privée. À l'époque, le débat se focalisait sur la vie privée des personnes publiques – pouvait-on photographier Jean Gabin sur

son lit de mort ? Le corollaire c'était l'inviolabilité du domicile, le secret des correspondances.

Les consommateurs prennent conscience que l'usage de ces données peut être abusif. La conscientisation reste assez intuitive. En 2011, l'une de nos enquêtes a révélé que le respect de la vie privée était désormais une préoccupation majeure des consommateurs. La prise de conscience porte en germe un sentiment de méfiance. Celui-ci, à son tour, peut avoir des conséquences économiques – voyez les scandales alimentaires. Il faut restaurer la confiance.

La clef est que les internautes maîtrisent leurs données. Les consommateurs, bien avertis, prendront les bonnes décisions. Voilà le point d'équilibre. Faisons-en des gens capables et responsables. Ne les traitons pas avec condescendance sous prétexte de les protéger.

L'enjeu est le consentement éclairé. Pour qu'il y ait contrôle des données, il faut que le consommateur soit informé. À défaut, pas de contrôle effectif de sa part. Avez-vous déjà cherché à comprendre les conditions générales d'utilisation de Facebook, de Google+ ou de Twitter ? Nous nous y sommes essayés pendant six mois avec des juristes : c'est impossible ! Les conditions générales ne sont pas toujours traduites, et quand c'est le cas, elles sont à la fois pléthoriques et elliptiques. Vous pouvez ouvrir un profil Facebook sans donner votre consentement… Il faut un *dashboard*[*], donnant à tout moment accès à une page sécurisée destinée à informer l'utilisateur de l'usage qui est fait de ses données, celles qui sont nécessaires au service, celles qui contribuent à sa qualité, et celles qui seront cédées, étant entendu qu'à tout moment le consommateur peut dire non. Ne partons pas du principe qu'il est nu ; à lui de choisir de se déshabiller ou non.

La sécurisation des données repose sur des dispositifs techniques : une norme ou une certification mondiale est souhaitable. Elle passe aussi par un contrôle. Enfin, il faut informer les intéressés de l'éventuel piratage de leurs données personnelles. Le projet de règlement en cours nous satisfait plutôt. L'information des autorités de contrôle sous 72 heures va dans le bon sens ; en revanche, il faut le faire « sans retard indu » pour le consommateur, ce qui nous laisse dubitatif.

Restera à savoir quel régulateur sera compétent géographiquement. Je ne suis pas sûr que l'autorité de régulation irlandaise, par exemple, dispose de moyens suffisants. Pour éviter le forum shopping, nous appelons de nos vœux une procédure associant la CNIL, si un Français est en cause.

Nous sommes bien sûr attachés à la bonne santé économique du secteur. Les limites à un usage débridé du profilage doivent venir de la libre volonté des consommateurs. (*Applaudissements*)

[*] *Cf. glossaire, p. 69*

M. Marc Mossé, directeur des Affaires publiques et juridiques de Microsoft France et membre de l'Association des services Internet communautaires (ASIC). – « Je m'intéresse à l'avenir car c'est là que j'ai décidé de passer le restant de mes jours », disait Woody Allen. Nous parlons de 2,5 hexa-octets collectés chaque jour. Ce phénomène colossal est déjà là, il se produit sous nos yeux. Inutile de regarder dans le rétroviseur.

Nous sommes à l'époque des opportunités. La Commission européenne a bien montré, dans son rapport de septembre 2012 sur le *cloud computing*[*], les enjeux de ces évolutions : 1,5 point de PIB d'ici 2020, 2,5 millions d'emplois en Europe grâce à la création de nouveaux usages. L'on estime à 54 milliards la valeur supplémentaire dégagée par les nouveaux modèles économiques. Les applications sont innombrables : en santé par exemple, l'on parvient à prévenir les risques d'infections nosocomiales grâce au *big data*. C'est aussi l'occasion de renouer avec l'adaptabilité, l'égalité des services publics et de réformer l'Etat.

Les motifs d'enthousiasme sont réels. Toutefois, le big data semble fragiliser les droits fondamentaux. Contrairement à d'autres, je ne crois pas que la protection des droits fondamentaux menace l'innovation, au contraire. Celle-ci, *by design*, dans sa conception, doit veiller sur ceux-là.

La question de la confiance est centrale, qui suppose la transparence à l'égard des utilisateurs. La régulation, qui forme le premier volet du triptyque, n'est pas du ressort des entreprises. Le droit à la vie privée est un droit fondamental, et je ne crois pas qu'il ait succédé, historiquement et philosophiquement, à la liberté d'expression. Nous avons l'habitude de concilier les droits fondamentaux. Il ne revient pas à la technologie de décider quels principes font sens dans notre société : la régulation incombe au politique. Nous avons besoin à cet égard de principes clairs, simples, efficients, à partir desquels construire des réponses adaptées.

Deuxième volet du triptyque, la co-régulation, par un dialogue entre parties prenantes, y compris le régulateur et le juge. Nous avons au terme d'un travail de plusieurs mois avec la CNIL et les autres régulateurs européens intégré dans nos contrats de *cloud computing* les clauses contractuelles type européennes.

[*] *Cf. glossaire, p. 69*

Enfin, le troisième volet du triptyque est celui de l'autorégulation. Résultant d'un choix volontaire des industriels, elle ne nous dispense pas de la régulation mais, au contraire, va plus loin qu'elle, à l'instar du principe de faveur en droit social. Il est possible de développer des technologies de protection : le *dashboard*, le *do not track by default*[*], le non-stockage des adresses IP au-delà de six mois.

En fonctionnant sur ces trois plans, nous réaliserons les promesses du numérique dans le respect des valeurs de notre société. Nous sommes confrontés à un enjeu de civilisation. Il n'est pas franco-français. Voyez l'intensité des débats en Allemagne, et la tribune publiée par Sigmar Gabriel. Aux Etats-Unis, les associations de protection des droits civils sont mobilisées. Un rapport sur le *big data* remis il y a quelques jours à M. Obama propose d'interdire la collecte des données à l'école, et réfléchit aux risques de discrimination liés à la capacité de prédiction facilitée par le croisement des données.

Il ne s'agit pas d'un conflit entre les Anciens et les Modernes. Tous les points de vue existent : les craintifs du numérique, les ravis de la crèche numérique, heureux *by design*, et les progressistes. Dans *Le Prisonnier*, série culte des années 60, le héros cherche à s'évader d'un village où tout le monde dit « Bonjour chez vous ! », un lieu trop parfait car déserté par le politique. Ce héros, c'est nous. Les libertés abandonnées sont celles auxquelles nous avons renoncé. Ne renonçons pas et saisissons-nous de ce débat. *(Applaudissements)*

M. Loïc Rivière, délégué général de l'Association française des éditeurs de logiciels et solutions internet (AFDEL). – Nous ne faisons pas partie des ravis du numérique, mais espérons être de ses promoteurs éclairés. La notion de vie privée a évolué au cours de l'histoire. En Grèce antique, elle concernait ce qui ne relevait pas de la sphère publique, c'était peu. Maintenant, les conceptions latines et anglo-saxonnes s'opposent mais le numérique fait exploser les frontières. Quand on a 400 amis sur Facebook et 10 000 *followers*, est-on dans la vie privée ? La vie publique de beaucoup sur Internet consiste dans ce qu'ils exposent ou surexposent de leur vie privée.

Il y a un échange entre le fournisseur de service et l'utilisateur. Ne nous étonnons pas que les entreprises d'Internet qui offrent un service gratuit collectent et traitent des données. C'est leur *business model*. Si ce modèle est modifié, l'usage des réseaux sociaux deviendra-t-il payant ? On parle de travail gratuit, mais une recherche sur Google ou Bing s'apparente-t-elle au *tripalium*, à la souffrance ?

[*] *Cf. glossaire, p. 69*

La confiance numérique a été ébranlée par l'affaire Snowden, qui a suscité des soupçons de connivence entre Google et les services de renseignements. Ces soupçons n'ont pas été corroborés ; au contraire le branchement sur le réseau a été opéré à l'insu des industriels. Internet ne saurait échapper à la surveillance des autorités de contrôle, parce qu'il décuple en même temps les possibilités d'échanger et de commercer, et celles de commettre des crimes.

Si le cadre règlementaire doit garantir les libertés, les industriels ont des progrès à accomplir en matière de transparence. Nos conditions générales d'utilisation (CGU) sont-elles longues ? Nous voulons noyer le poisson. Sont-elles courtes ? Nous ne traitons pas tous les cas ! Reste que l'internaute veut consommer le service le plus rapidement possible. C'est pourquoi l'essentiel réside dans l'éducation à la protection de la vie privée. Des applications sont dépourvues de CGU, ainsi que l'a révélé une étude de la CNIL : Internet ne sera jamais un espace totalement sain. Ce n'est en tout cas pas en rendant le cadre toujours plus coercitif que l'on favorisera la sécurité.

L'on a balayé trop vite les techniques d'anonymisation. Le navigateur est le meilleur outil, à travers la gestion des *cookies**, pour protéger la vie privée. Le cadre réglementaire se révèle déterminant à cet égard. Cependant, il s'applique à la PME du quartier comme à la multinationale. Comme Alain Bazot, je crois qu'il ne faut pas céder à la tentation de créer de nouvelles lois pour résoudre toutes les questions.

Le droit à l'oubli existe déjà depuis la loi « Informatique et Libertés », avec le droit à l'effacement. La décision de la CJUE du 14 mai ne promeut d'ailleurs pas un nouveau droit mais fait entrer les moteurs de recherche dans le cadre applicable aux opérateurs de traitement et les rend responsables des atteintes à la vie privée, car ils ont la faculté de déréférencer certaines données. Mais qui est compétent ? Les juges ont résolu un problème en en créant un autre. Les vidéos de l'Institut national de l'audiovisuel (INA) seront-elles concernées par ce type de décision? À nous de trouver, collectivement, les réponses. (*Applaudissements*)

Mme Isabelle Falque-Pierrotin, présidente de la Commission nationale de l'informatique et des libertés (CNIL) – Nous en convenons tous, nous sommes face à un changement absolu d'univers. Les données personnelles sont au centre de notre économie, ce qui apporte des bénéfices indéniables. Dans le même temps, les possibilités de ciblage, voire de surveillance des individus, s'accroissent et doivent être contrôlées. Les révélations sur le programme PRISM* ont permis de dévoiler un écosystème opaque et illustré les mauvais côtés d'Internet. Au fond, dans cette affaire, les remparts juridiques comme le *Safe Harbor,* n'ont pas fonctionné. Rétablir la confiance n'est pas simple. Il n'y a pas de réponse univoque et cela appelle une action simultanée auprès de tous les acteurs concernés. Il faut répondre

aux attentes exprimées autour de deux notions : plus de transparence et plus de possibilités de maîtriser de façon individuelle le système.

S'agissant, en premier lieu, des acteurs économiques, les entreprises plaident pour l'autorégulation. Le projet de règlement européen, qui mise sur l'*accountability*[*], répond en partie à cette démarche de responsabilisation des entreprises pour intégrer les préoccupations Informatique et Libertés. La CNIL, d'ailleurs, est active à leurs côtés, en ce domaine, depuis plusieurs années. Encore faut-il qu'elles jouent le jeu de la transparence. Or, on rencontre encore beaucoup de conditions générales d'utilisation (CGU) opaques. Il reste beaucoup à faire en matière de *privacy by design*[*]. De même, la culture de la sécurité des données personnelles est insuffisante.

De plus, il faut que les entreprises contribuent à rendre effectifs les droits des particuliers à l'accès, à la rectification ou à l'oubli. C'est pourquoi la CNIL propose, dans le cadre du projet de loi sur le numérique en préparation, que ces droits puissent s'exercer en ligne et que les particuliers obtiennent une preuve de cet exercice (récépissé, accusé de réception...).

Faut-il instaurer un droit de propriété sur les données personnelles pour éviter leur captation par les entreprises ? Je ne le crois pas. Ce serait une rupture avec la conception française selon laquelle les données sont une composante des droits fondamentaux et non un élément de patrimoine. De plus, même si les données sont détenues par des tiers, le particulier conserve des droits ; à l'inverse, dès que vous les aurez cédés, ces droits disparaîtront avec la perte liée au droit de propriété.

À l'égard, en second lieu, des acteurs publics, la CNIL propose que les fichiers de souveraineté puissent faire l'objet d'un contrôle externe, comme elle le fait déjà pour les fichiers de police – il ne s'agit pas de contrôler le contenu des fichiers de Renseignement mais de s'assurer que les outils mis en place par l'autorité compétente respectent le droit. Le cadre juridique, autre élément de transparence, doit être clarifié. L'invalidation de la directive sur la conservation des données de connexion, par un arrêt important de la CJUE rendu le 8 avril dernier, l'a montré. La CNIL avait attiré l'attention sur la nécessaire proportionnalité entre l'obligation de conservation qui pèse sur les opérateurs de télécommunication et la préservation des libertés. Les acteurs de marché nous interrogent pour savoir comment conserver les données. Il est indispensable que le législateur clarifie le champ de l'article 34-1 du Code des postes et des communications électroniques.

[*] *Cf. glossaire, p. 69*

Enfin, s'agissant du rôle du régulateur, dans le domaine du conseil aux pouvoirs publics, la transparence doit également être renforcée. Les avis rendus par la CNIL sur les projets de loi devraient être rendus publics et les possibilités de saisine de la CNIL devraient être étendues aux propositions de loi. Le projet de règlement européen s'efforce d'améliorer la gouvernance et la coopération entre autorités de protection ; notre proposition concilie simplicité et compétence nationale. Nous proposons d'augmenter la maîtrise du régulateur national et d'ajuster le niveau des sanctions. *(Applaudissements)*

M. Jean-Pierre Sueur, président de la commission des lois. – La commission des lois est déterminée à soutenir la CNIL face au projet de Mme Reding. L'instance compétente en cas de litige ne doit pas être l'instance du pays d'implantation de l'entreprise ; les citoyens ont le droit de s'adresser à l'autorité de régulation de leur pays. Nous espérons que vous gagnerez.

Merci d'avoir conforté notre idée selon laquelle une loi sur le renseignement est nécessaire. Quand la Direction générale de la sécurité extérieure (DGSE) s'efforce de retrouver un otage ou lutte contre le terrorisme, elle s'appuie sur un faisceau d'indices. Faut-il avertir toutes les personnes qu'elle a soupçonnées ? Une instance de contrôle serait nécessaire.

(Échanges avec la salle)

Mme Nathalie Launay. – Une donnée personnelle n'est pas un élément de patrimoine. Le *Safe Harbor Agreement** ne devrait-il pas être totalement exclu du Traité transatlantique, si la négociation de celui-ci se poursuivait après les élections européennes?

M. Daniel Latrémolière. – La CNIL a-t-elle étudié s'il est pertinent de conserver les données de connexion ? Il y a des précédents auxquels comparer cela : livrets ouvriers au XIX^e^, livrets de circulation pour les Roms, registres hôteliers…

Un intervenant. – Armer la France avec des outils de droit national est une chose, renforcer la dimension extérieure en est une autre. Le *do not track** n'a pas marché. Le rapport Obama évoque la remobilisation du *Privacy Bill* que les républicains empêcheront. La question de la territorialité est essentielle…

Mme Chantal Rubin. – Quelles sanctions prévoir à l'égard des gros acteurs d'Internet pour faire respecter les droits sur Internet ?

* *Cf. glossaire, p. 69*

M. Yves Le Mouël, directeur général de la Fédération française des Télécoms. – Le débat sur le *Safe Harbour Agreement** a partie liée avec la souveraineté. Les Européens en débattent. Des juges américains prolongent son application. Il faut mettre le sujet sur la table de négociation.

Mme Isabelle Falque-Pierrotin, présidente de la Commission nationale de l'informatique et des libertés (CNIL). – Le bon niveau de réponse est européen. Il s'agit de créer un rapport de force pour peser sur les autorités et les entreprises américaines. Si nous dénonçons le *Safe Harbor*, les flux d'informations entre l'Europe et les Etats-Unis s'interrompent. La Commission négocie pied à pied des améliorations. Nous avons la main pour être exigeants. En outre, l'Europe peut se donner, dans son règlement, des instruments de contrôle, comme le fameux article 43 qui soumet à autorisation l'accès d'une autorité publique étrangère aux données d'un citoyen européen.

Nous sommes inquiets sur le TTIP*. Que sont les données commerciales qui font l'objet des négociations, sinon des données personnelles, puisqu'elles servent au profilage des consommateurs ? Soyons vigilants pour que la négociation ne sacrifie pas la vie privée à la banane ou à tel autre produit. Les parlementaires ne peuvent-ils aider à dévoiler le mandat de négociation ?

M. Marc Mossé, directeur des affaires publiques et juridiques de Microsoft France et membre de l'Association des services Internet communautaires (ASIC). – La réponse européenne est indispensable, tant dans les négociations internationales, que pour sécuriser et harmoniser le cadre juridique. Le règlement rendra la norme accessible par tout le monde, des multinationales aux PME. Encore l'harmonisation doit-elle se réaliser autour des standards les plus élevés.

L'enjeu n'est pas seulement la collecte, mais sa finalité, car elle sert de base à l'élaboration de nouveaux produits et services, comme en matière de prédictibilité des comportements. Face à ces questions nouvelles, il faut répondre par l'*accountability*. Le droit, c'est bien ; un droit efficace, c'est mieux.

Mme Isabelle Falque-Pierrotin, présidente de la Commission nationale de l'informatique et des libertés (CNIL). – Les sanctions s'inscrivent dans un *continuum*. La nôtre n'était pas la première et ne sera pas la dernière, parce qu'une communauté de régulateurs travaillent ensemble. N'oublions pas en outre que la sanction affecte l'image d'une société : lorsque la CNIL a sanctionné Google, celle-ci a dû publier la décision sur sa page d'accueil, ce qui n'est pas en sa faveur ! Cela n'empêche pas de rendre les sanctions plus dissuasives. Quant aux métadonnées, peut-être des chercheurs détiennent-ils la réponse. Il faut en tout cas être attentif au respect de la proportionnalité.

* *Cf. glossaire, p. 69*

M. Alain Bazot, président de l'UFC Que Choisir. – La publicité des manquements aux règles fonctionne. Les professionnels tiennent à leur e-reputation. Un indicateur de taux de fraude serait dissuasif. Nous partageons l'inquiétude sur l'opacité du mandat de négociation du TTIP. Les visions européenne et américaine ne sont pas nécessairement antagonistes ; nos homologues d'outre-Atlantique sont très remontés.

Ne négligeons pas le droit national qui rend des procès possibles. Celui que nous avons engagé s'apparente peut-être au combat de David contre Goliath, mais il démontre l'intérêt d'agir à ce niveau. Nous sommes confiants sur l'issue tout en sachant que le chemin de l'application de la décision sera long.

M. Loïc Rivière, délégué général de l'Association française des éditeurs de logiciels et solutions internet (AFDEL). – Il est dans l'intérêt des entreprises américaines que le Safe Harbor crée de la confiance. L'Europe est évidemment le bon niveau. Une entreprise peut être prise dans une contradiction, née des obligations divergentes imposées aux niveaux national et international. Pour éviter des obstacles insurmontables, nous avons besoin de davantage de coopération.

Mme Anne-Marie Escoffier, présidente. – Merci à tous de la qualité de vos interventions, et à l'assemblée pour son attention ainsi que pour la pertinence de ses questions.

TROISIÈME TABLE RONDE
Prévention/répression de la criminalité et atteintes à la vie privée

M. Alain Zabulon, coordonnateur national du renseignement

M. Jean-Jacques Hyest, sénateur, membre et ancien président de la commission des lois du Sénat, membre de la Commission nationale de contrôle des interceptions de sécurité (CNCIS)

M. Jean-Jacques Urvoas, député, président de la commission des lois de l'Assemblée nationale, membre de la CNCIS

M. OlivierGuérin, délégué général de la CNCIS

M. Dominique Guibert, vice-président de la Ligue des droits de l'homme (LDH)

Mme Valérie Maldonado, chef de service de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC)

(de gauche à droit : M. Alain Zabulon, M. Jean-Jacques Hyest, M. Jean-Jacques Urvoas, M. Yves Détraigne, M. Olivier Guérin, M. Dominique Guibert, Mme Valérie Maldonado)

M. Jean-Pierre Sueur, président de la commission des lois. – Les tables rondes de ce matin ont été très riches. Celles à venir ne le seront pas moins. La première est présidée par M. Détraigne, vice-président de la commission des lois.

M. Yves Détraigne, président. – Le terme de criminalité qui figure dans le titre de cette table ronde est à entendre au sens le plus général, en y ajoutant l'ensemble des atteintes à la sécurité de l'État contre lesquelles les services de renseignement ont pour mission de lutter.

Les moyens employés à cette fin portent nécessairement atteinte à la vie privée. Le sujet a toutefois pris une ampleur nouvelle avec l'évolution technologique, comme l'ont montré les révélations d'Edward Snowden. La France n'y échappe pas, qui s'est saisie promptement de ces questions.

La loi sur la géolocalisation a fait naître un débat sur le suivi par la police et la justice des objets connectés.

M. Jean-Jacques Hyest, sénateur, membre et ancien président de la commission des lois du Sénat, membre de la Commission nationale de contrôle des interceptions de sécurité (CNCIS). – Je laisserai le soin à MM. Guérin et Urvoas, plus experts que je ne le suis, d'approfondir ces questions, et me bornerai à quelques remarques.

C'est en 1990 que la question des interceptions administratives, alors illégales, s'est posée. Il y avait pourtant des écoutes tous azimuts ; il fallait y mettre fin. C'était l'objet du rapport Schmelck. La loi du 10 juillet 1991 a créé le groupement interministériel de contrôle (GIC), et une Autorité administrative indépendante (AAI), la CNCIS, composée de trois membres, dont un parlementaire de la majorité, et un de l'opposition. J'ai été celui-là ; je suis désormais celui-ci. La commission ne donnait alors, aux termes de la loi, qu'un avis *a posteriori*. Il fallait revenir sur ce point : le gouvernement a souhaité que cet avis soit rendu *a priori*. Telle est, depuis lors, notre pratique, qui n'a pas varié. Le Premier ministre pourrait en théorie passer outre, mais il ne l'a jamais fait.

L'avis *a priori* a forcé l'administration à être plus rigoureuse dans ses demandes. Le code de la sécurité intérieure rend les interceptions possibles dans un certain nombre de cas, notamment la recherche de renseignements intéressant la sécurité nationale, la sauvegarde d'éléments essentiels du potentiel économique et scientifique de la France, la protection du patrimoine national, etc. Aucun problème, depuis 1991, ne s'est produit dans l'application de ces dispositions.

Les cas de la géolocalisation et des données techniques de communication, lesquelles sont devenues, aujourd'hui, souvent plus importantes que le contenu de l'interception lui-même, n'avaient toutefois pas été prévus par le législateur de l'époque… Qu'il me suffise de prononcer le mot magique : « fadette » !

Rappelons également que la loi du 23 janvier 2006 a prévu, dans le cadre de la lutte contre le terrorisme, une procédure spécifique, sous le contrôle d'une personnalité qualifiée, elle-même placée sous le contrôle de la CNCIS.

La CNCIS est une institution extrêmement originale. À sa tête, un magistrat administratif ou judiciaire. Aux côtés de celui-ci, un délégué général et des adjoints, également magistrats. C'est une bonne solution, parce que ceux-ci ont la charge de protéger les libertés publiques et que ces écoutes relèvent aussi parfois d'une phase pré-judiciaire.

Dans d'autres pays, les parlementaires sont plus nombreux. Je pense qu'il nefaut pas que les parlementaires se dispersent trop. En France, la présence des parlementaires – limitée normalement à trois ans non renouvelables - est utile ; elle a permis à la commission de remplir ses missions. Je n'ai jamais entendu la moindre critique sur les avis rendus. De même, je me réjouis du fonctionnement de la délégation parlementaire au renseignement. Il ne convient pas, je le répète, que les parlementaires soient trop nombreux. En dehors du champ d'action de la CNCIS, qui ne concerne que les écoutes dites administratives, il revient à la chaîne judiciaire de remplir son office pour les écoutes judiciaires.

Cet outil, indispensable, évoluera sans doute. Je voulais toutefois lui rendre l'hommage qu'il mérite. *(Applaudissements)*

M. Olivier Guérin, délégué général de la CNCIS. – Je m'en tiendrai aux éléments juridiques et techniques de l'activité quotidienne de la CNCIS, deuxième AAI créée, treize ans après la CNIL, et premier organisme de contrôle légal d'activités spécifiques au renseignement.

La CNCIS illustre la recherche constante de l'équilibre entre sécurité nationale et protection des libertés, dont le récent rapport Urvoas rappelle qu'elle exige des efforts toujours renouvelés.

Les « oreilles indiscrètes » sont une question sensible et ancienne. L'interception est presqu'aussi vieille que le téléphone : si la première conversation entre Graham Bell et son assistant date du 10 mars 1876, la première interception téléphonique fut inventée dès mars 1915, lorsqu'une prise de terre fut posée par le lieutenant André Delavie près des lignes allemandes, dans les tranchées de la forêt d'Apremont, pour écouter leurs téléphones de combat. C'est après la seconde guerre mondiale que les services des ministères de l'intérieur et de la défense se partagent les quelque 5 000 m² dédiés aux écoutes téléphoniques dans les égouts de Paris par la police secrète allemande.

Le 28 mars 1960, M. Debré ordonne la centralisation des outils d'interception et crée le GIC. En 1970, lors du débat sur le projet de loi renforçant la garantie des droits individuels des citoyens, le garde des Sceaux René Pleven admet pour la première fois la réalité de la pratique des interceptions de sécurité, en annonçant qu'elle sera encadrée et qu'un

organisme extérieur au gouvernement devra, un jour ou l'autre, se charger de ce contrôle. Le rapport de la commission Marcilhacy introduit une première distinction entre écoutes administratives et judiciaires, distinction fondamentale en France. Dans la plupart des États voisins, l'intégralité des écoutes relèvent de l'autorité judiciaire.

Après le rapport de la commission Schmelck, évoquée par le président Hyest, la loi du 10 juillet 1991 marque une étape importante, qui établit un équilibre entre l'intérêt national et la protection des libertés publiques. Quatre arrêts de la Cour européenne des droits de l'homme (CEDH), dont l'arrêt *Huvig et Kruslin contre France*, du 24 avril 1990, ont assurément influé sur cette évolution. La loi confiant les autorisations des interceptions à la CNCIS a été qualifiée de « modèle abouti » par un rapport parlementaire de 2013.

Au regard de l'augmentation des menaces, de l'émergence de problématiques juridiques transversales, des nouveaux enjeux de la protection des communications et des données personnelles et des développements technologiques, ce modèle pourrait toutefois avoir atteint ses limites.

Les garanties sont nombreuses. Autorité judiciaire et autorité administrative sont strictement séparées. La primauté de l'autorité judiciaire, rappelée par le Conseil constitutionnel en 2006, se traduit par la cessation automatique des interceptions administratives, sur l'ensemble des réseaux nationaux, dès lors qu'une information judiciaire est ouverte. Ce dispositif est observé avec attention par certaines délégations étrangères qui nous rendent visite. D'autres cloisonnements séparent les services de renseignements, en charge de l'enquête, et les services techniques qui exécutent les mesures ou encore l'exécutif demandeur -ministères de l'intérieur, de la défense, du budget- et l'exécutif décideur : le Premier ministre. L'intervention d'une autorité administrative indépendante évite une boucle réservée à l'exécutif et permet l'examen des requêtes des citoyens.

Autres garanties : le nombre limité des administrations habilitées à demander une interception ; l'obligation de validation par l'autorité de tutelle ministérielle, avec un nombre restreint de signataires (deux seulement en plus du ministre) ; le nombre limité de motifs pour autoriser une écoute ; le faible nombre d'écoutes autorisées ; la limitation à quatre mois de leur durée (il en va autrement des écoutes judiciaires) ; l'obligation de transcription, donc de traçabilité ; la limitation à dix jours de la durée de conservation des enregistrements ; la classification secret défense (ce qui constitue une protection pour ceux qui ont fait l'objet d'une surveillance) ; la nécessité d'un faisceau de présomptions graves et concordantes, d'implication personnelle dans des projets d'atteinte aux intérêts fondamentaux de la Nation, déclinés en cinq motifs légaux, encadrés par le

code pénal et les engagements européens et internationaux de la France, comme la convention de Palerme sur la criminalité organisée, par exemple. Le Conseil constitutionnel, le 2 mars 2004, a validé ces critères.

L'intervention d'un organe extérieur et indépendant, comme la CNCIS, où sont présents des parlementaires, ainsi que l'intervention technique d'opérateurs privés, requis par les autorités administratives ou judiciaires, constituent des garanties.

Le mécanisme en vigueur est toutefois remis en cause. D'abord, par l'émergence de nouveaux acteurs de la communication, multiples, internationaux, en trois couches. En premier lieu, les propriétaires de réseaux : ces infrastructures physiques sont variées, renvoyant à différentes textes – la convention de Montego Bay renvoie, pour les câbles sous-marins, au régime international des communications ; les vecteurs hertziens et satellitaires sont visés par des dispositifs spécifiques non pris en compte par les conventions européennes…Ensuite, les hébergeurs de contenus, les fournisseurs d'accès ; enfin, la multiplicité des sociétés disséminées à travers le globe qui produisent les contenus échangés, dont les sièges et les outils sont situés à l'étranger.

Les acteurs classiques ne sont plus incontournables, de nombreuses sociétés proposant des services, des outils d'interception ou de captation de données, hors du cadre défini pour les réquisitions administratives ou judiciaires adressées aux opérateurs. Ils sont aussi vulnérables aux diverses attaques, non explicitement visées dans les dispositifs légaux, telles que les usurpations d'identité, piratages, actes de cybercriminalité…

S'y ajoutent des contraintes techniques nouvelles, avec la dissociation complète entre la ligne, l'abonné et la communication. Question essentielle : la corrélation entre l'objectif et la personne qui communique, étant donné la difficulté de l'identification des internautes. L'anonymisation est devenue un obstacle. Il faut parfois croiser plusieurs types de données pour identifier quelqu'un. L'anonymisation peut être volontaire ou non – cybercafés, wifi gratuit, usage groupé de moyens de communication, outils spécifiques : une vingtaine de mesures distinctes sont parfois nécessaires pour parvenir à l'identification…Les outils de cryptologie ont été libéralisés et les entraves à l'interception se multiplient.

La plupart des outils de communication électroniques servent également, de manière croissante, à connecter des machines entre elles et non plus seulement à communiquer. La question de la compétence territoriale de la loi se pose parfois. Les modalités du contrôle doivent par conséquent changer. La liberté de la correspondance n'est plus le seul principe à protéger. Quel contrôle ? *Ab initio*, *a posteriori* ? Les sondages révèlent que 57 % des Français trouvent les outils de surveillance sur internet justifiés dans le cadre de la lutte contre la criminalité. *(Applaudissements)*

M. Jean-Jacques Urvoas, député, président de la commission des lois de l'Assemblée nationale, membre de la CNCIS. – Je serai plutôt empirique, n'ayant pas l'expertise des deux précédents orateurs. À partir de mon expérience de membre de la CNCIS, mais aussi de président de la délégation parlementaire au renseignement (DPR), j'aborderai la question de la responsabilité de l'État au XXIème siècle et des moyens dont il doit se doter pour protéger personnes et citoyens dans le respect des libertés.

La menace est de plus en plus atomisée et difficile à détecter. Elle progresse en intensité. Elle est plus virulente que jamais. De surcroît, elle se modernise. En 1991, tous les outils de communication actuels n'existaient pas. La menace est dans la technologie. Ses buts restent classiques ; déstabiliser, attaquer, tuer. Face à cette menace, du terrorisme, de la déstabilisation, du pillage de nos secrets industriels, etc., nous estimons que les moyens de nos services sont notablement insuffisants. Nos six services administratifs ont trois moyens : les écoutes d'abord. Elles sont peu nombreuses : pendant très longtemps il y en eut 1840, puis, depuis un décret pris par Jean-Marc Ayrault il y a quelques semaines, 2 150 chaque année, soit *epsilon* par rapport aux interceptions judiciaires, qui se comptent en dizaines de milliers. Ensuite, les fichiers sont ridiculement peu utilisés, sans interconnexion possible. Troisième moyen : le recueil des données de connexion s'opère dans un cadre lui aussi très contraint.

Je précise que les débats qui ont entouré la loi de programmation militaire ne portent pas sur la situation actuelle puisque cette loi ne sera applicable qu'en 2015.

Le rôle de l'État est de protéger les personnes, dans le respect des droits et libertés individuels. Nous sommes bien loin des caricatures orwelliennes.

Pour les remplir, l'État dispose de la prévention, de la détection et du monopole de la sanction. Que faire ? D'abord, accroître les moyens des services. La mutation de la DCRI (Direction centrale du renseignement intérieur), en DGSI (Direction générale de la sécurité intérieure), permettra de recruter les compétences utiles : informatique, cryptologie, ingénierie bancaire, etc. La DGSI, s'émancipe donc utilement du cadre normatif de la DGPN, la logique des compétences supplante celle du statut.

Ensuite, il faut doter l'administration des outils existant dans le domaine judiciaire : capacité de sonorisation, de captation d'images…Marc Trévidic, juge antiterroriste bien connu, le dit à qui veut l'entendre : 100 % de ses dossiers impliquent Internet, désormais. Or le droit va toujours moins vite que la technique. Il faut assurer un contrôle de responsabilité accru. Les services n'étaient contrôlés par personne. La création de la délégation parlementaire au renseignement (DPR) est une avancée majeure : grâce soit rendue – pour une fois ! – à Nicolas Sarkozy… Les parlementaires ont appris à connaître les services. Les agents du renseignement ne sont pas des

barbouzes, des Pieds nickelés, des *losers*, les enfants naturels de Ben Barka et du *Rainbow Warrior*, mais des fonctionnaires courageux qui servent – parfois au prix de leur vie – l'État, l'intérêt général, dans le respect des valeurs de la République. Les services ont découvert que les parlementaires, bien qu'émanant d'un lieu dédié à la parole, ne sont pas pour autant des bavards impénitents. Le Parlement a décidé de conférer à la DPR le contrôle des politiques de renseignement, non des opérations de terrain. Les services de renseignements doivent être contrôlés par le Parlement en tant que services de l'État, car ce ne sont pas des officines privées au service d'intérêts particuliers.

Deuxième type de contrôle, essentiel : celui de légalité et de proportionnalité, c'est-à-dire de l'usage des moyens. Contrôle du quotidien, constant, pointilleux, il ne peut être exercé par le Parlement. Dès lors, deux possibilités : le confier à un juge – l'Espagne le fait. Nous pourrions suivre cette voie, aux termes de l'article 66 de la Constitution. Autre hypothèse : le modèle de l'AAI, fondé sur vingt décisions du Conseil constitutionnel depuis 1991. J'appelle de mes vœux la transformation de la CNCIS en ce sens. Les parlementaires n'auraient pas à y siéger, et là-dessus je suis en désaccord avec Jean-Jacques Hyest. Son pouvoir de rendre un avis *a priori* doit être introduit dans la loi, qui ne relève pour l'heure que de la pratique de la CNCIS. Ainsi nous aurons un modèle qui ouvrira aux citoyens des possibilités d'appel et fonctionnera efficacement. *(Applaudissements)*

M. Alain Zabulon, coordonnateur national du renseignement. – Je me propose de vous exposer la position de la communauté du renseignement sur tous les sujets évoqués par les intervenants précédents. Mais tout d'abord de quoi parlons-nous ? Il ne s'agit pas de services secrets, contrairement à ce que l'on entend souvent. La communauté du renseignement est un ensemble d'hommes et de femmes qui sont des agents publics, ont un statut, agissent conformément aux orientations données par le gouvernement. Des six services qui la constituent, deux ont une vocation généraliste, relative à la sécurité intérieure et extérieure. La DGSI (ex-DCRI) lutte contre le terrorisme, l'espionnage et protège notre patrimoine technologique, industriel et scientifique. Elle vise à sanctuariser notre territoire national contre toutes les agressions à l'encontre de nos intérêts fondamentaux.

La Direction générale de la sécurité extérieure (DGSE) agit, elle, en dehors du territoire, pour collecter des renseignements destinés à informer le gouvernement sur les grandes affaires stratégiques internationales. Membre permanent du Conseil de sécurité des Nations unies, la France participe au maintien de la paix dans le monde et a besoin à ce titre, être renseignée. La DGSE exerce aussi une fonction d'entrave aux risques d'atteinte aux intérêts français à l'étranger.

Il existe quatre autres services spécialisés. Deux d'entre eux relèvent du ministère de la défense : la direction de la sécurité et de la protection de la défense (DPSD) est chargée de protéger le personnel, les emprises physiques et le périmètre du ministère de la défense nationale, y compris des entreprises qui travaillent avec lui ; la direction du renseignement militaire (DRM) fournit des informations opérationnelles à nos forces armées pour leur permettre d'intervenir dans les meilleures conditions d'efficacité et de sécurité. Deux autres services relèvent du ministère de l'économie et des finances : la direction nationale du renseignement douanier (DNRD) lutte contre la criminalité organisée, les trafics en tous genres, la contrefaçon, y compris dans le domaine de la sécurité sanitaire ; la cellule Tracfin lutte contre le blanchiment d'argent, le financement du terrorisme et l'utilisation frauduleuse des flux financiers qui servent à la criminalité organisée.

Ces services œuvrent ensemble et forment une communauté. Que faut-il entendre par là ? Soyons concrets : juste avant l'attentat du 11 septembre 2001, la CIA, chargée de la sécurité extérieure, avait repéré des mouvements d'individus suspects sur le territoire américain, mais cette information n'a pas été partagée avec le service chargé de la sécurité intérieure.

On connait le résultat. La leçon en a été tirée : les démocraties ont pris conscience de leur extrême vulnérabilité ; un service de renseignement ne peut travailler seul, il doit échanger en permanence avec les autres services placés sous l'autorité de son gouvernement et avec les services étrangers des pays amis. Nous collaborons quotidiennement, dans la lutte antiterroriste, avec les Britanniques, les Américains, les Allemands, les Belges, parce que nous sommes confrontés, comme l'a souligné le président Urvoas, à des menaces de plus en plus individualisées et atomisées.

La principale menace réside actuellement dans la présence de 300 jeunes gens détectés enrôlés en Syrie dans des groupes qui combattent le régime d'Assad et ont pour projet de revenir dans leur pays sous la bannière du djihad. Songez à cette effroyable vidéo montrant de jeunes Français ricanant, traînant, à l'arrière de leur véhicule, des cadavres décapités. Ils participent en Syrie à des égorgements, des décapitations et des crucifixions et ont pour ordre de répandre ce combat à leur retour, sur le territoire national, dans les pays occidentaux. Il faut se donner les moyens de suivre cette multitude d'individus, qui ne sont pas forcément regroupés dans des unités structurées.

Aussi l'action des services doit-elle évoluer, en utilisant les moyens techniques d'accès à l'information, dans le respect des libertés. La communauté du renseignement est consciente que l'acceptation du contrôle est une nécessité et un rempart contre la suspicion. Le cadre juridique des interceptions de sécurité est très rigoureux et c'est tant mieux. Les services de renseignement doivent relever le défi démocratique. La technologie

permet de collecter chaque jour des milliards de données : belle prouesse technique, mais pour quoi faire ? Ce que l'on peut faire ne doit pas être nécessairement ce que l'on doit faire.

Quelques mots sur le contrôle qui pèse sur les services

Le quota d'interceptions de communications autorisé est fixé à 6 000 interceptions, ce qui est très faible, en comparaison du nombre des interceptions judiciaires et de nos 60 millions d'habitants.

S'agissant du contrôle démocratique évoqué par le président Urvoas, la délégation parlementaire au renseignement, composée de parlementaires de la majorité et de l'opposition est un véritable progrès. Elle peut auditionner les ministres, les services ; elle remet un rapport annuel au président de la République, facteur de transparence. C'est un fait nouveau. Ce n'était pourtant pas dans la culture du monde du renseignement, mais son existence, qui n'allait sans doute pas de soi, est un atout, voire un relais pour améliorer l'efficacité de notre action.

La communauté du renseignement est une entité vivante. Elle évolue et accepte le changement. Elle souhaite bénéficier de la confiance de la Nation, pour mieux participer à la sécurité du pays et au maintien du rang de la France dans le concert des Nations. (*Applaudissements*)

M. Yves Détraigne, président. – Merci pour cette démonstration de l'utilité des services de renseignement.

Mme Valérie Maldonado, chef de service de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC). – L'OCLCTIC relève d'activités judiciaires, au sein de la sous-direction de la lutte contre la cybercriminalité de la DCPJ. Nous travaillons avec Europol, notamment l'unité « EC3 » spécialisé contre la cybercriminalité, et Interpol.

Nous luttons contre la cybercriminalité, à la fois de manière préventive et répressive, dans le cadre des procédures pénales, sous le contrôle des magistrats, du parquet ou de l'instruction.

Nous privilégions la coopération internationale, et cherchons à faire évoluer nos outils sans cesse. Il nous appartient, sous le contrôle des magistrats, de rechercher les éléments constitutifs d'une infraction pénale, dont les technologies numériques ont rendu la commission plus aisée.

L'usage généralisé des technologies de l'information et de la communication (TIC) concerne tous types de trafics et d'infractions : comme les narcotrafics (opération Silkroad, menée en collaboration avec le FBI, ayant abouti au démantèlement d'un site de vente en ligne de stupéfiants) ou la pédopornographie, contre laquelle la coopération internationale est nécessaire pour faire tomber les serveurs utilisés pour la diffusion des images illicites.

Les criminels recourent de plus en plus aux logiciels d'anonymisation, ou à la monnaie virtuelle. Les cyberattaques sont de plus en plus performantes et virulentes, comme l'illustre dernièrement l'affaire Blackshades, du nom d'un malware, logiciel malveillant qui permet de prendre le contrôle à distance d'un ordinateur, et de subtiliser les identifiants qui y sont stockés, en activer la webcam ou de lancer des attaques en déni de service, destinées à saturer des serveurs ciblés. Une action coordonnée des services de l'État est nécessaire. Les citoyens et les PME sont des cibles de choix de ces attaques qui causent des préjudices importants, notamment en cas d'usurpation d'identité numérique. C'est pourquoi nous développons la prévention et mettons à disposition un point de contact national.

Nous disposons des moyens traditionnels d'enquête. Nous souhaitons augmenter la durée de conservation des données techniques : ces éléments sont essentiels pour démontrer l'infraction pénale et l'administration de la preuve. La cyber-infiltration, très encadrée, constitue un outil essentiel pour les services spécialisés.

Autre dispositif majeur : la captation des données à distance, des frappes sur le clavier ou d'images d'écran, qui, seule, permet efficacement de contourner le cryptage.

Enfin, nous souhaitons des instruments de coopération judiciaire plus rapides, car la criminalité n'attend pas la délivrance de commissions rogatoires internationales.

L'enjeu est de veiller à l'équilibre entre l'usage ces outils perfectionnés, aux mains également des délinquants, et le contrôle de l'autorité judiciaire, garante du respect des libertés. (*Applaudissements*)

M. Yves Détraigne, président. – L'enjeu est de concilier le respect de la vie privée et la captation des données pour lutter contre la criminalité.

M. Dominique Guibert, vice-président de la Ligue des droits de l'homme (LDH). – Un moment, je me suis demandé ce que je faisais là, seul défenseur des droits de l'homme face à cinq représentants de l'administration et des institutions. La LDH n'a pas compétence pour juger l'action de la CNCIS, ni celle des services de renseignement, mais de veiller à la défense des libertés publiques, non pas de la vie privée.

Je déplore certains effets de tribune faciles : un intervenant a fait une comparaison avec la Corée du Nord. Je préfère me référer au modèle français. Pour évaluer notre système, il ne faut pas l'évaluer à cette aune...

Le titre même de la table ronde est ambigu. Prévention/répression de la criminalité « et » atteintes à la vie privée : « et » signifie-t-il « au risque de » ?

Pour lutter contre la criminalité faut-il accepter de réduire les droits ? On peut faire de la politique au mépris des droits ; on ne fait de bonne politique qu'avec ces droits, qu'en les respectant. Comment distinguer assurément la surveillance généralisée du contrôle nécessaire ? Où est la limite ? Quand la surveillance devient-elle invasive ? La question est ancienne. Le contrôle des populations est apparu avec les déserteurs de l'armée de Louis XIV, qui parcouraient les campagnes entre 1700 et 1715 et auxquels l'on reprochait beaucoup de crimes, de vols : pour protéger les villageois, on a créé des papiers d'identité militaires, étendus ensuite à toute la population. L'idée d'une surveillance générale était née.

La question des sans-papiers était née ! L'efficacité des services de police a été augmentée, accréditant l'idée que la surveillance était un outil contre la criminalité. Les fichiers se sont multipliés ; ils ne sont pas toujours utiles : le Système de traitement des infractions constatées (STIC) fiche des personnes non encore condamnées, le Fichier national des empreintes digitales (FNAED) a valu à la France d'être condamnée par la CEDH…

Surgit alors la question du rapport entre la technique et la politique. Les techniques sont contingentes et secondes par rapport à la décision politique. Ce n'est pas parce qu'une technique existe, qu'elle doit être utilisée ! On court toujours après la technique, certes. Mais il faut poser d'abord le cadre juridique, celui des politiques publiques. Dans tous les cas, le respect des droits et des libertés des individus est premier. En l'absence de normes et de réglementation, on se laisse distancer par la technique, réduite à en appeler à de simples codes de bonne conduite.

D'où l'importance des AAI. Le groupe des 29 « DPA » (*data protection agencies*) existe en Europe. De même qu'existe un corpus de droits, reconnus au niveau international. La déclaration universelle des droits de l'homme, les pactes de 1966, la convention européenne des droits de l'homme, la charte européenne des droits fondamentaux sont des garde-fous. La LDH et la FIDH ont déposé en juillet dernier une plainte contre X visant la NSA, le FBI et la CIA, sur la base d'articles du code pénal français, pour dénoncer la captation des données personnelles. Les Allemands, les Belges, les Hollandais et les Anglais ont fait de même sur le fondement de leur droit national.

Lorsque nous jugeons l'action des services de renseignement, au regard des libertés publiques, il faut se poser quatre questions : comment résoudre ou corriger l'asymétrie d'information avec les citoyens ? Doit-on considérer que toute technique est utilisable ou peut-on, à l'image de la législation française, résister à son invasion ? Est-il pertinent de constituer d'énormes bases de données ? Doit-on, enfin, toujours soumettre le respect des libertés publiques à l'efficacité de la lutte contre la criminalité, au risque d'ouvrir la voie à Guantanamo ? Cette question ne peut être éludée au Parlement.

De même, la centralisation en matière de renseignement n'est-elle pas excessive ? À quoi sert-elle ? N'oublions pas aussi que le juge doit être compétent. C'est lui qui décide en dernier recours. N'étendons pas le champ de l'extra-judiciaire, sous peine d'amoindrir l'efficacité de la lutte contre la criminalité.

J'aurais préféré que cette table ronde soit intitulée « Libertés publiques et lutte contre la criminalité ». L'équilibre est essentiel. Sinon la légitimité même de la police et des services de renseignement sera remise en cause, l'efficacité de leur action sera amoindrie, car celle-ci repose sur la confiance des citoyens en leur respect absolu des droits de l'homme. (*Applaudissements*)

M. Yves Détraigne, président. – Merci pour votre franchise. Vous avez posé beaucoup de questions qui ne manqueront pas de faire réagir vos interlocuteurs, notamment les parlementaires présents parmi nous.

M. Jean-Jacques Hyest, sénateur, membre de la commission des lois du Sénat, membre de la Commission nationale de contrôle des interceptions de sécurité (CNCIS). – Vos questions anticipent largement sur la dernière table ronde. Le renseignement a pour objet de veiller à prévenir les atteintes aux intérêts de la Nation. Si les criminels utilisent les nouvelles technologies, il faut bien s'adapter, sans renoncer au contrôle. Tel est l'objet de la CNIL ou de la DPR.

M. Jean-Pierre Sueur, président de la commission des lois. – Je suis membre de la LDH depuis environ 30 ans. J'ai été rapporteur de la LPM. Or j'eusse aimé, comme je l'ai dit amicalement, que la LDH, avant d'émettre un communiqué me condamnant, m'ait entendu. La semaine prochaine, sa section du Loiret m'auditionnera, à ma demande. Je plaide pour le dialogue le plus approfondi entre nous. Je l'indique ici en toute amitié.

M. Dominique Guibert, vice-président de la Ligue des droits de l'homme (LDH). – je vous réponds non moins amicalement. Nous avons des désaccords à ce sujet, ce qui prouve que la Ligue est un organisme démocratique, où des points de vue différents peuvent s'exprimer librement… J'avais d'ailleurs rédigé une lettre à votre intention, pour que nous nous rencontrions avant…

M. Jean-Pierre Sueur, président de la commission des lois. – Elle a dû être interceptée !

(*Échanges avec la salle*)

Mme Virginie Dumas, des services du Premier ministre.- Le CNCIS fonctionne bien ; sa transformation en AAI a été évoquée. Quand aura-t-elle lieu ?

M. Jean-Jacques Urvoas, député, président de la commission des lois de l'Assemblée nationale, membre de la CNCIS. – Le calendrier parlementaire est touffu. Certainement avant la fin de la législature ; probablement avant la fin de l'année.

M. Jean-Pierre Sueur, président de la commission des lois. – Il faudrait en parler au Premier ministre…

M. César Armand.- Je suis journaliste au magazine Europe parlementaire. Monsieur Urvoas, dans le rapport avec M. Verchère sur l'organisation des services de renseignement, publié l'an dernier, vous déplorez le faible nombre d'interceptions simultanées, ainsi que le fait que l'on ne pourrait écouter Skype. Qu'en est-il aujourd'hui ? Est-ce possible désormais?

M. Jean-Jacques Urvoas, député, président de la commission des lois de l'Assemblée nationale, membre de la CNCIS. – Le nombre d'écoutes simultanées est passé de 1 840 à 2 150, ce qui n'est pas colossal. Mais une écoute est une cible. Cela peut représenter dix portables. Quant à Skype, rien n'a changé pour des raisons juridiques.

M. Antoine Lefébure.- M. Zabulon a été éloquent, mais a évoqué une menace terroriste à la fois diffuse et individuelle : ne risque-t-on pas de céder, comme aux États-Unis, à la tentation de la surveillance généralisée, dont on a constaté les piètres résultats ? Quid de la menace intérieure ? Que se passerait-il si la presse internationale – souvent mal relayée par la presse française – révélait que la DGSE, dans le cadre de ses rapports avec le Government Communications Headquarters (GCHQ) britannique s'est livrée, en 2012, à des activités considérées comme criminelles ? Y aurait-il prescription ?

M. Alain Zabulon, coordonnateur national du renseignement. – Je ne reprendrai pas la comparaison avec la Corée du Nord, mais j'évoquerai la parabole du chalut et du harpon. Les moyens techniques existants permettent à tel grand pays, ami de la France, de collecter des milliards de données par jour. Est-ce un modèle à suivre ? C'est une prouesse technique, sans doute, mais faut-il être capable de trouver « la » bonne information ! Or ce modèle du chalut n'a pas empêché le 11 septembre, ni l'attentat sanglant de Boston ! Telle n'est pas la voie choisie en France.

Aussi, nous préférons la pêche au harpon dans la collecte des informations. Créer un tel système en France serait illégal, inutile et coûteux. Les services du renseignement ne sont pas demandeurs ! Ils préfèrent un système d'analyse intelligent des menaces. Nous suivons une poignée d'individus. Le rapport public de la CNCIS en rend compte. Une politique du renseignement généralisée ne servirait à rien.

Question de la salle. – La présidente de la CNIL défendait un contrôle externe des services de renseignement ce matin. Quand verra-t-il le jour ?

Nous sommes tous plus favorables au harpon qu'au chalut. Pourquoi donner à une grande entreprise privée, dont l'État est actionnaire minoritaire, comme Thalès, la fonction d'écoute ?

M. Alain Zabulon, coordonnateur national du renseignement. – Je n'ai pas d'informations sur ce dernier point. La doctrine de l'État en matière d'interception est de ne pas sous-traiter une action qui relève de ses prérogatives. Le contrôle, je le répète, répond aux risques de suspicion. Il s'est étoffé grâce à la loi de programmation militaire. Outre la DPR et la CNCIS, aurons bientôt, un service d'inspection des services de renseignement constitué à partir des grands corps d'inspection de l'Etat et doté de pouvoirs d'investigation sur pièces et sur place au sein des services. Il y a enfin un contrôle hiérarchique sur les services. Les directeurs des services de renseignement sont placés sous l'autorité de leur ministre. Je ne suis pas le super-chef des services. Nous assumons en revanche que, pour la sécurité du pays, certaines actions de renseignement menées à l'extérieur soient secrètes et clandestines.

M. Guy Batard.- Les interventions sont depuis ce matin de haut niveau. Je regrette toutefois l'absence de l'ANSSI, qui aurait pu nous éclairer sur la réalité de la cybermenace, qui est planétaire, hors du microcosme français. Les câbles sous-marins sont ainsi des lieux de captation d'informations potentiellement constitutives de renseignements. Arriver après les événements, c'est du journalisme : c'est trop tard. Le renseignement suppose d'aller chercher les choses là où elles sont, en amont, pour anticiper. J'ajoute que Thalès est une entreprise française de confiance.

Question de la salle. – Pouvez-vous, Monsieur Guibert, revenir sur la composition de la future commission de contrôle annoncée par M. Urvoas ?

M. Dominique Guibert, vice-président de la Ligue des droits de l'homme (LDH). – Je serais ravi de donner l'avis de la LDH sur la composition d'une telle AAI, si on le lui demandait…

M. Jean-Jacques Hyest, sénateur, membre de la commission des lois du Sénat, membre de la Commission nationale de contrôle des interceptions de sécurité (CNCIS). – Tous les membres de cette commission sont soumis au respect du secret de la défense nationale.

Question de la salle. – De quelle manière vos services nous protègent-ils nous, citoyens et entreprises, des interceptions d'autres pays ou du crime organisé ? N'est-il légitime de se prémunir contre ces risques-là ? Quels mécanismes institutionnels, spécifiques à la France, permettent d'éviter une affaire Snowden à la française ?

Mme Valérie Maldonado, chef de service de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC). – Les outils classiques sont ceux du dépôt de plainte. Mon service a de plus créé une division spécialisée pour recevoir les demandes des particuliers et des entreprises, les conseiller et les renseigner utilement. Nous en avons discuté avec l'ANSSI, dont les guides de bonnes pratiques sont très intéressants.

M. Yves Détraigne, président. – Je remercie l'ensemble des intervenants. Cette table ronde a répondu, manifestement, à la plupart des attentes de chacun.

M. Jean-Pierre Sueur, **président de la commission des lois.** – Je vous remercie à mon tour, ainsi que les intervenants pour la richesse de leurs propos**.**

QUATRIÈME TABLE RONDE
Quelles règles de droit pour les nouvelles technologies ?

M. Gaëtan Gorce, sénateur,
membre de la commission des lois du Sénat, membre de la CNIL

M. François Pillet, sénateur, membre de la commission des lois du Sénat

Mme Meryem Marzouki, chercheure au CNRS

Me Alain Bensoussan, avocat spécialiste des nouvelles technologies de l'information et de la communication

Mme Nathalie Metallinos, responsable de l'atelier « protection des données personnelles » de l'Association pour le développement de l'informatique juridique (ADIJ)

(de gauche à droit : M. Gaëtan Gorce, M. François Pillet, Mme Esther Benbassa, Me Alain Bensoussan, Mme Meryem Marzouki, Mme Nathalie Metallinos, Jean-Pierre Sueur)

Mme Esther Benbassa, présidente. – Nous nous réjouissons de faire face à une aussi vaste assemblée, et d'être entourés de personnes aussi savantes.

Les nouvelles technologies effacent les frontières entre vie publique et privée. Comment gérer cet espace de liberté ? Nous pouvons éduquer les plus jeunes à son utilisation, sans passer pour des censeurs. Ne devrait-on pas enseigner l'usage des nouvelles technologies dès le plus jeune âge, à l'école ? La démarche est ambitieuse. Avec Mme Goulet, nous nous y étions engagées. L'on nous a alors accusées de vouloir créer des limites là où il n'y en a pas.

Pour clore cette journée, nous recevons M. Gaëtan Gorce, auteur d'un rapport sénatorial remarqué sur la protection des données personnelles et l'*open data*, ainsi que d'une proposition de loi tendant à limiter l'usage des données biométriques, président de la mission commune d'information « Nouveau rôle et nouvelle stratégie pour l'UE dans la gouvernance de l'internet » ; M. François Pillet, co-auteur avec M. Gorce du rapport précité et rapporteur de la proposition de loi sur la biométrie ; Mme Meryem Marzouki, chercheure au CNRS, spécialiste des relations entre TIC, politiques publiques et espace public ; Me Alain Bensoussan, avocat spécialisé dans les nouvelles technologies de l'information et de la communication et Mme Nathalie Metallinos, responsable de l'atelier « protection des données personnelles » de l'Association pour le développement de l'informatique juridique (ADIJ). Ouvrons le débat !

M. Gaëtan Gorce, **sénateur, membre de la commission des lois du Sénat, membre de la CNIL.** – Je ne sais si l'on pourra ajouter des choses nouvelles, tant les précédentes tables rondes ont été riches. On n'aime guère que le législateur se mêle de ces questions : Internet, c'est en effet la liberté. Légiférer, c'est risquer d'être à contretemps et de bloquer les évolutions que l'on veut encourager. Le législateur a néanmoins une responsabilité, au-delà du fonctionnement des marchés et des technologies : dire la norme, c'est fixer l'acceptable et l'inacceptable, en fonction de valeurs collectivement définies. Le numérique bouscule ces valeurs.

La vie privée est une notion relativement récente. Âgée de deux siècles tout au plus, elle n'est protégée que depuis peu. Or ce qui compte aujourd'hui, c'est moins ce que l'on est que la position occupée, au carrefour de tels ou tels réseaux, la circulation des informations que l'on détient. Il s'agit de questions civilisationnelles. Il faut commencer, pour certains interlocuteurs, par redéfinir les valeurs que l'on entend protéger.

Que deviennent la vie privée, l'intimité, quand la téléréalité, par exemple, survalorise des éléments du quotidien, en transformant la sphère privée en spectacle ?

La technologie ne demeurera-t-elle qu'un outil ?

Selon le point de vue dominant aujourd'hui, la technologie facilite la vie quotidienne, améliore la santé et la sécurité des individus. Selon un autre point de vue, la technologie instrumentalise l'individu - voyez l'utilisation de la biométrie, du contour de la main, pour l'accès à des cantines scolaires ou à des équipements sportifs et culturels.

Le législateur doit rester le garant d'une certaine conception de la personne humaine, donc limiter l'usage de la technologie au strict nécessaire : assurer la sécurité indispensable de locaux, lutter contre les usurpations d'identité…Ce point de vue n'est plus une évidence. Tel est l'objet de la proposition de loi que j'ai déposée, qui limite l'usage de la biométrie aux situations dans lesquelles la sécurité est en jeu.

J'ai osé critiquer l'*open data* – ce qui m'a valu de voir mon blog piraté, curieuse conception du débat ! L'*open data* ne concernerait pas les données personnelles, dit-on, or, par recoupement, on reconstitue aisément le profil d'un individu. Le respect de l'intimité, du corps humain, n'est pas un principe désuet, mais un élément du respect de l'autonomie de la personne, qui ne se réduit pas à un rouage de la machine technologique et économique.

En provoquant le débat sur ces questions, nous encourageons le Parlement à jouer son rôle. N'ayons pas une confiance aveugle dans la technologie qui, loin d'être neutre, bouleverse la société et ses valeurs. Il est normal qu'elle les rappelle, quitte à les reformuler. C'est l'homme qui contrôle la technologie, non le contraire. *(Applaudissements)*

M. François Pillet, **sénateur, membre de la commission des lois**. – Je me bornerai à deux exemples empruntés aux possibilités biométriques, qui illustrent les questions posées au législateur. Le droit, pour être fort, doit être stable ; comment peut-il dès lors encadrer des technologies qui vont plus vite que lui ? D'aucuns répondent : par des procédures de labellisation, de certification. N'abdiquerait-il pas ainsi sa compétence normative, au profit de spécialistes de la technologie ?

Le législateur joue, selon moi, un rôle primordial : celui de garant du pacte social, que la technologie peut modifier en profondeur. Ne péchons pas par pusillanimité en refusant de prendre la mesure des nouveaux enjeux. Certaines innovations, comme les nanotechnologies ou l'utilisation massive des données personnelles, sont peut-être irréversibles. Ne tombons pas non plus dans un prohibitionnisme obscurantiste, ne serait-ce que parce que la technologie n'a pas de frontières.

Premier exemple : la proposition de loi destinée à lutter contre l'usurpation d'identité. La sécurisation proposée passait par l'enregistrement dans un fichier central de données biométriques de chaque français, afin de les associer définitivement à son identité, et *via* un titre d'identité biométrique également. Il s'agissait de ficher 60 millions de Français. Un tel fichier aurait méconnu le principe de proportionnalité entre l'objectif (lutter

contre l'usurpation d'identité) et les atteintes aux libertés publiques constituées par les moyens déployés, aboutissant à l'identification quasi parfaite de la totalité de la population française. Les garanties juridiques posées par ce texte étaient insuffisantes. Refuser purement et simplement l'usage de la biométrie pour les titres d'identité revenait à refuser un progrès incontestable dans la fiabilité de ces titres. Sur ma proposition, le Sénat a doublé les garanties juridiques par des garanties dans la constitution même de la base de données, rendant impossible l'identification d'une personne à partir d'une seule donnée biométrique, sans porter atteinte à l'objectif prioritaire du texte. La CMP a finalement échoué ; le point de vue de l'Assemblée nationale a prévalu et le Conseil constitutionnel a censuré le fichier central, comme l'avait annoncé le Sénat.

Deuxième exemple : la proposition de loi de Gaëtan Gorce, relative à la biométrie. Impossible d'ignorer les avancées de cette technologie, désormais largement répandue, qui pénètre dans tous les domaines de la vie quotidienne, de l'accès aux locaux à la santé. La proposition complète l'article 25 de la loi Informatique et libertés et renforce les conditions d'autorisation par la CNIL de la constitution de tels systèmes biométriques. Le législateur est là indiscutablement dans son rôle.

Il fait écho à des préoccupations internationales, notamment dans le cadre du Conseil de l'Europe, dont le comité de réflexion sur la « convention 108 » a proposé d'intégrer les données biométriques parmi les données sensibles au sens de cette convention. Des évolutions de la réglementation en vigueur au sein de l'UE sont également en cours. La proposition de loi sera étudiée dès la semaine prochaine par le Sénat. J'ai voulu préciser la notion de « stricte nécessité de sécurité », qui conditionne la mise en place de la biométrie, afin qu'elle ne soit entendue de façon ni trop large, ni trop étroite. M'inspirant d'une communication de la CNIL de 2007, j'ai proposé de tracer la frontière le long des « intérêts excédant l'intérêt propre de l'entreprise », ce qui inclurait l'authentification pour les transactions financières, qui protège les intérêts du citoyen consommateur, au-delà de ceux des banques et des commerçants.

Le législateur n'intervient en ces matières que d'une main tremblante, en espérant contribuer à limiter les dérives portant atteinte à l'intérêt général. *(Applaudissements)*

Mme Meryem Marzouki, **chercheure au CNRS**. – La proposition de loi de M. Gorce est bienvenue. Je regrette toutefois sa timidité : elle se limite à la modification de l'article 25 de la loi de 1978. Or l'usage sécuritaire de la biométrie qui en est fait aujourd'hui exigeait d'aller plus loin ; de plus, je doute que les garde-fous soient suffisants. Nous y reviendrons sans doute. Alors, quel droit pour les nouvelles technologies ? Je suis tentée de répondre : un droit respectueux des droits fondamentaux.

Au-delà de la formule, saisissons l'occasion de la loi sur le numérique pour faire évoluer les choses. Les droits fondamentaux qu'il incombe au législateur de faire respecter sont le droit à la vie privée, le droit à la présomption d'innocence, le droit à un procès équitable, le droit à la dignité humaine, qui est sérieusement mis en cause par l'usage de la biométrie. Le principe de non-discrimination, quant à lui, est souvent enfreint par les dispositifs de vidéo-protection dans les rues et les quartiers – chacun en a des exemples en tête.

La protection de la vie privée et des données personnelles conditionne la liberté d'expression, car la surveillance nourrit l'autocensure. C'est une question démocratique, une question de contrat social.

Ces défis ne sont pas nouveaux. Depuis l'affaire Snowden, nous savons, grâce à une résolution des Nations unies que nous devons faire respecter nos droits, y compris sur le réseau. Les révélations d'Edward Snowden ont suscité une prise de conscience massive des citoyens. Leur énormité ne doit toutefois pas masquer les autres problèmes qui demeurent, dont la convergence des méthodes et outils des opérateurs privés, fournisseurs de services en ligne, des communautés de renseignement, des services de police judiciaire et des administrations soumises à une logique gestionnaire, à des objectifs chiffrés, depuis la présidence de Nicolas Sarkozy, notamment dans le cadre de la révision générale des politiques publiques (RGPP). Tous les arrêtés que nous avons contribué à contester, avec les associations de défense des droits de l'homme, devant le conseil d'État, se réfèrent à l'objectif de tenir des statistiques. Tous ces services procèdent en effet à des collectes massives et systématiques des données qui sont à leur portée. Tous se livrent à des opérations de profilage. Plus besoin de connaître l'identité des gens, il s'agit de cerner des profils, au moyen d'application informatiques : à des fins de publicité comportementale pour les entreprises ; à des fins de renseignement pour la lutte antiterroriste ; à des fins de lutte contre la criminalité, voire la simple délinquance, comme l'ont montré Delphine Batho et Jacques-Alain Benisti dans leur rapport parlementaire.

Certaines tâches relevant de l'administration sont également transférées à des tiers. La CJUE, le 13 mai, a estimé que les moteurs de recherche, Google en l'espèce, géraient bien des données personnelles au sens de la directive européenne sur la protection des données, et devraient garantir une forme de droit à l'oubli.

La surveillance qui guette peut faire craindre un recul de la liberté d'expression. *(Applaudissements)*

Me Alain Bensoussan, **avocat spécialiste des nouvelles technologies de l'information et de la communication.** – Cela fait vingt ans qu'on se bat pour le droit à l'oubli : on ne peut que se féliciter d'une victoire jurisprudentielle, qui sera sans doute suivie d'une réglementation.

Il me semble que la vie privée est devenue un concept sans pertinence. La loi de 1978 a été pertinente technologiquement… jusqu'à l'arrivée des nouvelles technologies, le 2.0, les réseaux sociaux ; du 3.0, l'internet des objets, du 4.0, celui des objets autonomes et du 5.0, qui fusionne l'informatique et les robots.

Je ne fais pas de procès à la vie privée, mais je m'interroge sur la vie publique virtuelle. La Cour de cassation a reconnu que son existence dépendait des circonstances.

Auparavant la vie privée avait un lieu : le domicile, étendu parfois à la voiture, voire à la chambre d'hôtel. Or la notion de vie privée virtuelle a été reconnue, nous l'avons obtenu en plaidoirie, dans l'ordinateur, où il y a bien plus de vie privée que dans ma voiture. Autre progrès jurisprudentiel !

Réintroduisons les valeurs intemporelles cachées derrière ces zones. La vie privée ne se résume pas à l'intimité. Nous sommes passés du droit à la protection de l'intitulé au droit à la vie privée. Depuis la loi de 1978, les lois ont développé les protections. Plus d'une cinquantaine jusqu'au droit à l'oubli ! Ce sont tous des droits à la personnalité. Nous avons besoin aujourd'hui d'un droit à la propriété. Facebook est une révolution pour un milliard de personnes dans le monde – il représente pourtant le Jurassique du numérique. L'article premier des conditions générales d'utilisation (CGU) de ce réseau, soit du contrat qui le lie à ses utilisateurs, valant loi entre les parties, indique que chacun d'entre nous donne une licence, non exclusive et gratuite à Facebook. C'est qu'il est locataire et que nous sommes propriétaires. Ce droit de propriété s'étend à la sphère des données. *Quid* du droit pénal, dans le contexte actuel de marchandisation des données ? On titre « vol de données chez Sony, chez Orange » etc. Pour qualifier un vol il faut une effraction pour s'approprier la chose d'autrui. Je me bats, avec d'autres, pour faire reconnaître le vol par réseau, virtuel. On n'en est pas tout à fait là. Le droit des biens est sûrement la solution au droit de la vie privée dans le monde virtuel.

Bien sûr, il faut faire respecter les valeurs. Les technologies sont neutres, ce sont les usages que les hommes en font qu'il faut réguler. Libérons la biométrie et les technologies ! Partons de l'idée que la création de valeur est saine et que c'est l'utilisation anormale qui est malsaine. La loi de 1978 est fondée sur la collecte des données et la notion de finalité. Mais celles-ci ne sont plus collectées, elles sont créées par des algorithmes prédictifs. Le concept finalité est absent du *big data*. Peu importe le nom des individus, seul compte leur comportement. Peut-on laisser les États-Unis créer seuls des entreprises de biens incorporels ? L'article 5C du règlement européen n'a aucun sens. N'imposons pas le principe de *minima* en Europe quand prévaut le principe de *maxima* aux États-Unis ! Et Google prospère… Libérez la technologie en Europe ! Nous ne cessons de plaider tous les jours devant les tribunaux les droits de l'homme numérique…

Oui, Snowden est un vrai défi, mais en trente-quatre ans, deux décisions importantes ont été rendues : l'arrêt Reno c/ACLU qui a placé Internet sous la protection du premier amendement de la Constitution américaine, et la décision de la Cour de justice de l'Union européenne de mai 2014 qui consacre le droit à l'oubli : nous sommes les archivistes de notre passé, notre passé ne mine pas notre futur. Voilà un droit de la personnalité !

Reste à reconnaître le droit à l'intimité, le droit à la souveraineté personnelle, à l'autodétermination dans l'utilisation des nouvelles technologies de l'information et de la communication.

Le bonheur est, dans le monde binaire, le droit de s'arrêter quand il ne protège pas les valeurs essentielles…*(Applaudissements)*

Mme Esther Benbassa, **présidente**. – Cher Maître, merci pour cette performance ! Je retiens la différence, importante aujourd'hui, entre vie privée et vie intime, ainsi que votre comparaison entre les États-Unis et la France…

Mme Nathalie Metallinos, **responsable de l'atelier « protection des données personnelles » de l'Association pour le développement de l'informatique juridique (ADIJ).** – L'ADIJ, réunit depuis quarante ans des juristes passionnés de nouvelles technologies de l'information et de la communication. Son président, Pascal Petitcollot, rédacteur en chef de Légifrance, est dans la salle. Je dirige l'atelier de protection des données personnelles.

Quelles perspectives ? Le tableau a été dressé : la mort annoncée de la vie privée, l'impasse de nos libertés publiques, face aux mesures sur la sécurité…

La réforme du règlement européen sur la protection des données personnelles est très attendue.

Les législations existantes trouvent leurs limites. Les principes de la loi de 1978, repris dans la directive de 1995, sont néanmoins pérennes. Même si la logique de la collecte s'estompe, le principe de proportionnalité demeure. En France, on estimait longtemps que la protection reposait sur la déclaration préalable à la CNIL. Il pose manifestement un problème d'effectivité. Il n'a pas suffi à prévenir les abus.

La réforme en cours du règlement européen change le paradigme en rétablissant la responsabilité des acteurs, publics et privés. Le contrôle *a priori* est transféré aux opérateurs, à charge pour eux de démontrer leur observation des règles, alors qu'aujourd'hui de nombreux manquements passent inaperçus : « pas vu, pas pris » !

Le rapport sur l'*open data* montre que seule la méthode d'élaboration des données et la traçabilité documentée de cette méthode, que les banques connaissent, est un garde-fou efficace.

Ensuite les données à caractère personnel constituent une notion plus vaste que la vie privée. Il s'agit désormais de tenir compte non seulement de la possession de données nominatives, mais aussi des conséquences du traitement des données, du profilage. La législation s'appuiera sur cette notion.

Enfin, pour pallier le manque d'effectivité de la réglementation, il faut renforcer le pouvoir de sanctions de la CNIL. La FTC américaine a condamné Google à une amende de 10 millions de dollars, pour avoir contourné la technologie censée empêcher le placement de *cookies* sur les postes Apple ; la CNIL ne peut prononcer des amendes supérieures de 150 000 euros. Le projet de règlement permet, en relevant ces sanctions, de remonter aux comités exécutifs des entreprises, au lieu d'en rester à celles traitées par leurs services juridiques. Je ne connais à ce jour aucune entreprise qui ait inscrit le respect des données personnelles de ses clients ou de ses salariés dans ses valeurs.

L'arrêt de la Cour de justice de l'Union européenne, selon moi, se fonde sur le droit existant et ne crée pas un nouveau droit à l'oubli numérique. Elle a ordonné la suppression des données qui ne répondaient plus à l'exigence de qualité posée par la législation actuelle car elles n'étaient plus à jour. Pour résoudre la question posée par la dissémination des données, il faut agir en amont. Une fois que les données sont parties sur internet, il est trop tard. La préservation des données privées doit devenir une option par défaut dans les dispositifs numériques. Tel est l'élément majeur de cette proposition de règlement. Il reste beaucoup de travail, mais nous espérons que cette réforme aboutira. *(Applaudissements)*

Mme Esther Benbassa, **présidente**. – Je note que vous évoquez aussi le droit à l'autodétermination. Il est vrai que les sanctions prononcées par la CNIL ne sont pas dissuasives. Je donne la parole à la salle.

(Échanges avec la salle)

Question de la salle. – Je représente la société Morpho. L'usage de la biométrie se développe, non en France car le droit y est strict, mais dans le monde. Une alliance, FIDO s'est créée, essentiellement autour d'entreprises américaines. Morpho et Oberthur l'ont rejointe. L'industrie française est novatrice. Nous travaillons avec la CNIL.

Votre proposition de loi nous inquiète. Ne risque-t-on pas de laisser la France à l'écart, d'autant que vous ne prévoyez pas d'exception pour la recherche scientifique ?

Mme Monique Pontier.- Je suis professeure émérite à l'Institut de mathématiques de Toulouse.

Personne n'a parlé du centre d'accès sécurisé aux données, sous l'égide de l'Insee, dans le cadre de l'établissement public « Genes » (groupe des écoles nationales d'économie et statistique), qui tient des bases de

données, provenant de la sécurité sociale, de ministères. Ces données sont consultables par tous à des fins de recherche et anonymes. La recherche scientifique n'a pas besoin de données nominales pour avancer. Nous pratiquons le *data mining* depuis longtemps. Je m'interroge donc sur la pertinence de la question précédente.

M. César Armand.- Je suis journaliste au magazine *Europe parlementaire*. Madame Marzouki, pensez-vous être objective ? Êtes-vous chercheure au CNRS ou militante ? N'auriez-vous pas dû intervenir lors de la table ronde de ce matin, où était présent un représentant de Google France, puisque vous critiquez Google qui n'est pas là pour vous répondre ?

Mme Esther Benbassa, **présidente. –** Les organisateurs sont libres. Il ne vous appartient pas de porter un jugement sur leurs choix de composition des tables rondes. J'ajoute que les intervenants sont libres d'exprimer leurs points de vue, sans qu'on ait à leur demander leur carte professionnelle…

Mme Meryem Marzouki, **chercheure au CNRS**. **–** Je ne vous demande pas si vous êtes journaliste ou partisan. Je n'ai pas attaqué Google, mais simplement rappelé une décision de la Cour de justice de l'Union européenne.

Question de la salle. – je représente une société active dans le domaine de l'information légale, financière et économique. Nous publions des données personnelles figurant dans le cadre de la publicité légale. Certains dirigeants d'entreprises cités nous interrogent à ce sujet. Des éclaircissements seraient bienvenus sur le statut de ces données.

Question de la salle. – Notre société travaille dans le secteur de la biométrie. Le problème de la biométrie ne réside pas dans la technologie même, mais dans la constitution de bases de données nominales biométriques. Il est possible de rendre anonymes ces bases de données. La loi limiterait les possibilités d'authentification. Actuellement, elle verrouille les applications. Certains États américains, comme la Floride, interdisent la biométrie pour l'accès aux cantines scolaires. Mais si la technologie biométrique est utilisée sur un *device* individuel, il n'y a pas de danger pour l'utilisateur, qui peut ainsi accéder à des services numériques intéressants.

M. Gaëtan Gorce, sénateur, membre de la commission des lois du Sénat, membre de la CNIL. – La proposition de loi ouvre un débat, qui se prolongera au-delà de son examen en séance publique au Sénat. Le corps humain bénéficie dans notre droit d'une protection particulière. Il faut l'étendre à ses prolongements, comme les données biométriques, dont l'utilisation est à mon sens choquante, non seulement pour les enfants, mais aussi pour les adultes. C'est un débat de société. Je considère que certains usages changent notre vision du corps humain et même l'idée qui est au fondement de notre civilisation. De plus, j'y vois un moyen de discipliner les individus. Cela me choque. C'est un débat politique, qui porte sur les valeurs. Nous aurons ce débat mardi. Je suis conscient des enjeux

économiques, industriels, mais le respect de la personne humaine est premier. M. Bensoussan appelait à libérer la technologie. Certes ! Mais n'oublions pas nos valeurs de base, faute de quoi nous nous réveillerions dans une société très différente de celle où s'est construite l'autonomie de l'individu.

M. François Pillet, sénateur, membre de la commission des lois du Sénat. – Cette proposition de loi ne nuit pas à la recherche, ce qui devra être précisé lors des débats, ni au développement de l'industrie française. Nous ne réglementons que les usages. Ce n'est pas parce qu'une société française découvrirait un procédé révolutionnaire, exportable, mais contraire à notre conception de la société, qu'il faudrait l'accepter *ipso facto* ! Nous ne voulons pas couper les ailes de l'*open data* mais émettre des recommandations, afin d'éviter la divulgation incontrôlée des données contre la volonté de leurs propriétaires. En effet, on ne dispose pas de techniques d'anonymisation totalement fiables. L'administration ne peut garantir qu'il n'y aura pas de dérapage. Même si les failles sont aujourd'hui peu nombreuses, il faut anticiper sur le développement de l'*open data*.

Mme Esther Benbassa, présidente. **–** Merci à vous tous. La notion de vie privée et de valeur fondamentale sont des concepts qui varient selon les civilisations, les pays et les époques. Il conviendra de les définir avec précision. Les lois s'adaptent et sont conjoncturelles.

M. Alain Bensoussan, avocat spécialiste des nouvelles technologies de l'information et de la communication. – Les civilisations et leur géographie évoluent. Bien malin celui qui peut affirmer que nos valeurs sont universelles, même s'il faut les défendre. Il y a plusieurs sortes de biométries : celle de l'organe, qui est une horreur ; celle du cyborg, qui peut être discutée, l'alliance du corps et de la technologie ; et la biométrie de l'image du corps humain, qu'il ne faut pas confondre avec le corps humain lui-même. L'empreinte digitale, la voix, l'iris, le système veineux ne sont que les images des doigts, de la parole, de l'œil, des veines ! À ce compte-là, faudra-t-il interdire la photographie ? Lorsque mon ordinateur me regardera, il saura m'identifier, sans que j'aie à retenir un code…Libérons la biométrie de la forme et de l'image, élément essentiel à la démocratie !

M. Gaëtan Gorce, sénateur, membre de la commission des lois du Sénat, membre de la CNIL. **–** Avec M. Bensoussan, il est clair que nous avons des conceptions différentes de l'amour !

Mme Esther Benbassa, présidente. **–** Merci pour vos interventions. Nous terminons en beauté ! *(Applaudissements)*

M. Jean-Pierre Sueur, président de la commission des lois. **–** Merci à tous les participants.

CONCLUSION

M. Jean-Pierre Sueur, président de la commission des lois. – Je remercie Mme la ministre Axelle Lemaire d'avoir accepté de conclure nos travaux. Je vous félicite pour votre nomination. Vous étiez très engagée à l'Assemblée nationale afin de faire adopter une proposition de loi que le Sénat a votée, qui donne au juge français la compétence pour intervenir dans le cadre du TPI. Espérons qu'elle sera examinée à l'Assemblée nationale ! Trop de propositions de loi d'origine sénatoriale s'égarent en chemin de l'Assemblée, ce qui représente un gâchis de temps et d'énergie.

Je remercie les 25 intervenants. En dépit de la complexité des sujets, nul n'a cédé à la polémique et le climat, tout au long de la journée, a été serein. Le sens de l'écoute a prévalu. Il est bon assurément que tous les acteurs concernés soient consultés avant le vote d'une loi.

Nous avons discuté des rapports entre la vie privée et l'intimité, sous de nombreux aspects, techniques, juridiques, scientifiques, civilisationnels. Sans doute faut-il une loi à ce sujet.

Je suis persuadé qu'une loi sur le renseignement est également nécessaire. Le contrôle de l'utilisation des données par les services de renseignement n'est pas assez poussé. Il ne faut pas céder pour autant à l'angélisme. Pour arrêter Mohamed Mérah, avant qu'il ne commette ses horreurs, il aurait fallu procéder à des écoutes ! Les mêmes qui déplorent les

écoutes réclament aux services de renseignement d'agir ! Certes, il ne faut harponner que ce qui est nécessaire, mais on ne sait pas toujours ce que l'on cherche ! C'est pourquoi il faut renforcer le cadre législatif du renseignement.

Il faut aussi une loi sur le numérique et le respect des droits. Je sais que vous préparez cette loi indispensable, mais complexe, car le numérique ne connaît pas de frontières. Qu'est-ce qu'une loi de la République française peut poser comme contraintes et obligations en ce domaine ? En attendant un cadre mondial, il faut que l'Europe agisse. En Europe, certaines idées ne doivent pas prévaloir, telles celles qui affirmeraient la seule compétence de l'instance de régulation du pays où l'opérateur a son siège. Défendons les prérogatives de la CNIL pour le citoyen français. Vous avez été choisie, parce que c'est une loi difficile à faire. Nos débats seront publiés. Votre propos va nous éclairer, Madame la Ministre. *(Applaudissements)*

Mme Axelle Lemaire, secrétaire d'état auprès du ministre de l'économie, du redressement productif et du numérique, chargée du numérique

Mme Axelle Lemaire, secrétaire d'État auprès du ministre de l'économie, du redressement productif et du numérique, chargée du numérique. – Vous venez de révéler mon ADN ! Il est vrai, que j'étais très engagée sur le texte sur la CPI, en effet. Je vois un point commun avec le sujet qui nous occupe aujourd'hui : il s'agit de protéger les droits de l'homme et les libertés fondamentales. Je défendrai l'inscription de ce texte à l'ordre du jour à l'Assemblée nationale.

Félicitations à tous, pour vos interventions riches – que j'ai suivies sur Twitter - et votre état d'esprit serein, même si je puis regretter que ce colloque n'ait pas pu avoir lieu avant l'examen de la LPM. Il importe de souligner les vertus du travail collectif, voire collaboratif, en amont du processus décisionnel.

Un scoop d'abord : dans un bureau, à Palo Alto, il a été décidé cet après-midi que le statut des nouveaux utilisateurs de Facebook ne serait plus visible par défaut, il ne serait donc consultable que pour leurs amis. Merci à Facebook ! Le politique ne servirait donc plus à rien ? Trêve de plaisanterie !

Quel est alors le rôle du politique dans un monde sans frontières ? La concurrence entre les systèmes de droit prévaut. La compétitivité dépend des choix du législateur. Faut-il accepter le sentiment de dépossession, bien réel, vécu par nombre de nos concitoyens ? Ou bien alors, comme je le crois, s'efforcer de définir au niveau européen des positions communes, centrales ? L'Europe a, à cet égard, un rôle crucial à jouer.

Ce dimanche se tiennent les prochaines élections européennes : c'est là que tout se joue.

Les choses ont évolué rapidement : la Cour de justice de l'Union européenne a censuré il y a quelques jours la directive relative à la conservation des données de connexion, qui l'eût cru ? Cette décision dont nous rêvions, c'est la Cour de justice de l'Union européenne qui l'a prise à notre place. C'est aussi cela, l'Europe concrète, où la France doit faire entendre sa voix. Nous attendons avec impatience les débats relatifs au nouveau projet de directive.

Le numérique entraîne un bouleversement potentiel de nos valeurs. Nous avons en Europe et en France une forte tradition de protection des droits. 1789 a inventé l'individu libre et souverain ; la France était également pionnière en 1978 ; elle a toujours su s'adapter aux évolutions technologiques. Je ne l'oublie pas, quand j'entends que la France serait en retard.

J'étais au Brésil lors de la ratification du Marco civil da Internet par la présidente Dilma Roussef : ce pays n'avait tout simplement pas de cadre législatif en la matière ! Il n'empêche que le droit français doit se moderniser : ce sera l'objet du projet de loi sur le numérique.

L'affaire Snowden, distillée semaine après semaine par les journalistes, a profondément changé les choses. Le modèle que nous avons construit est plus pertinent que celui de la notion anglo-saxonne du notice and consent, qui est celui de la NSA.

La loi de 1978 a instauré le contrôle par l'État des données personnelles des individus. L'étape suivante a introduit un contrôle partiel du secteur privé. L'échelle actuelle des grands traitements de données est tout autre. La quantité des informations échangées, avec les objets connectés, change complètement la donne.

Auparavant, les renseignements dépendaient du nombre d'hommes. Les taxis jouaient un rôle crucial ! Cette époque est révolue : les possibilités techniques sont devenues sans limites. Les États-Unis ont décidé de stocker tout internet, « au cas où »…

Les valeurs que nous voulons promouvoir font l'objet de débats depuis la nuit des temps. Il faut adapter ces questions, posées dès l'ère présocratique, à l'évolution des technologies. Benjamin Franklin disait qu'un peuple prêt à sacrifier un peu de sa liberté pour plus de sécurité finit par perdre l'une et l'autre.

Les Français ne sont pas ce peuple. Ils sont très attachés à leurs libertés et au débat public. Faut-il revoir ces valeurs ? Je ne le crois pas. Elles sont fondamentales. La liberté d'expression sur les réseaux sociaux doit-elle primer sur le droit à l'oubli ? Quelle égalité entre les usagers quand le numérique permet de rendre des services personnalisés ? Quel est le sens de l'ordre public lorsque l'État n'a plus le monopole de l'exercice de la violence légitime, face à des acteurs domiciliés fiscalement aux Bermudes, ou situés dans le cyberespace ? Les réponses à ces questions, nous les connaissons.

Le numérique est facteur de progrès ; il libère l'individu - il ne consiste pas à jouer à Candy Crush toute la journée…Je suis pour un numérique de l'inclusion, qui donne à chacun le pouvoir d'agir. Je ne crois pas à la dépossession. L'outil numérique est un levier d'autonomisation des individus et une force économique.

Oui, il faut moderniser le cadre juridique du renseignement. Donnons-nous les moyens de collecter des données viables, adaptées aux menaces qui pèsent sur notre pays. Point de transparence à tout prix, mais des outils efficaces, dans le cadre du droit. J'ai lu avec attention le rapport annuel de la délégation parlementaire au renseignement. Il est opportun de légiférer. La France doit compléter son arsenal législatif, sans mélanger toutefois le renseignement, la sécurité d'une part et le numérique, l'innovation, la protection des données personnelles, d'autre part, car cela ajouterait à la confusion, et je ne suis pas ministre de la défense.

Le contrôle du juge a été présenté, lors du débat sur la loi de programmation militaire, comme l'ultime rempart contre l'arbitraire. C'est une idée très anglo-saxonne. En France, nous avons la CNIL, que personne ne critique, en tant qu'autorité indépendante, sauf ceux qui l'ont qualifiée, l'année dernière « d'ennemi de la Nation ». Elle protège nos libertés. La CNCIS fonctionne aussi correctement. Tout n'est pas parfait, mais respectons notre tradition française. Ne nous lançons pas, par conséquent, dans un exercice de « copier-coller » législatif.

Que recherchons-nous ? L'essentiel, en matière de numérique, réside dans la confiance, qui passe par la connaissance du rôle de chacun. Qui fait usage de quelle donnée et à quelle fin ? Prenons le commerce électronique, qui rencontre un grand succès en France : la confiance des consommateurs a été gagnée par l'instauration légale de mécanismes efficaces, de statuts clairs, pour garantir la sécurité des transactions et éviter les fraudes. La certitude de ne pas être écouté, ébranlée par l'affaire Snowden, doit être retrouvée.

Dans le même esprit, le champ d'intervention de la puissance publique doit être renforcé, là où c'est nécessaire, afin de garantir l'application de la loi française aux acteurs français : c'est tout l'enjeu de la fiscalité applicable au numérique, de la territorialisation des dispositifs

relatifs aux données. Le cloud*, à cet égard, est un outil formidable, qui ne doit pas être dévoyé pour contourner la loi française, plus protectrice que d'autres pour les données personnelles.

État, CNIL, CNCIS : tel est le triangle institutionnel équilibré qui garantit les libertés en France, avec le législateur et le juge. M. Gorce plaide pour une réappropriation du politique.

Le débat aura lieu. Je serai heureuse de représenter le Gouvernement lors de la discussion de sa proposition de loi sur les données biométriques. Nous nous interrogeons sur les rôles respectifs des AAI, du juge et du politique.

Deuxième volet : la question technologique.

L'individu est souvent considéré comme un produit commercial par les grandes plateformes du numérique. Il faut casser ce monopole de l'information, permettre à chacun de s'approprier les outils, développer les architectures distribuées, soutenir les solutions libres, le marché des tiers intermédiaires de confiance où les Français occupent une bonne place. Oui, la protection à la française peut être source d'attractivité économique, d'innovation. Il existe en outre des modèles alternatifs, respectueux de la vie privée : celui de l'économie collaborative, fondée sur les prestations et non sur la vente d'espaces publicitaires par exemple.

Réfléchissons aux nouvelles façons d'exercer des droits, loin de l'utopie de la propriété individuelle des données privées. Celles-ci deviennent un bien commun, dont la valeur ne peut être captée au seul profit de quelques acteurs économiques : elles doivent être partagées, mais aussi maîtrisées par les individus.

L'open data est-il incompatible avec la protection de la vie privée ? Je ne le crois pas. Là aussi, il faut délimiter des frontières juridiques claires. L'open data n'est pas le big data. Il faudra un débat public : je plaide pour que la directive européenne soit transposée dans le projet de loi numérique. La commercialisation des données risque de flouter, à terme, la frontière entre données privées et données publiques.

Beaucoup ressentent, je l'ai dit, un climat de dépossession face au numérique. Creusons toutes les pistes de réappropriation de cet outil. Le débat perdure depuis la naissance de la République, car il pose au fond la question de l'idée que la France se fait d'elle-même, en tant que Nation ouverte sur le monde, ouverte à l'innovation.

Posons des questions. Le temps de la concertation viendra bientôt. La loi ne pourra pas tout : elle n'a vocation qu'à mobiliser l'éventail le plus large possible d'outils au service de tous, et de la croissance. (*Applaudissements*)

---

* *Cf. glossaire, p. 69*

M. Jean-Pierre Sueur, président de la commission des lois. – Merci pour votre propos. Nous sommes à votre disposition pour travailler avec vous. Il faudra en effet deux lois. Il faudra plaider auprès du Premier ministre pour leur inscription à l'ordre du jour. Nous aurons le temps d'y revenir. Merci à tous. (*Applaudissements*)

ANNEXE 1
Programme du colloque

OUVERTURE

M. Jean-Pierre Sueur, Président de la commission des lois du Sénat

TABLE RONDE N° 1

• Les nouvelles technologies, une menace pour la vie privée ?

Présidée par Éliane Assassi, vice-présidente de la commission des lois du Sénat

- **Mme Christiane Féral-Schuhl**, ancien bâtonnier du barreau de Paris
- **M. Philippe Aigrain**, Quadrature du net
- **M. Antonio Casilli**, maître de conférences en humanités numériques à Telecom ParisTech et chercheur au Centre Edgar-Morin de l'EHESS
- **M. Benoît Tabaka**, directeur des politiques publiques de Google France

TABLE RONDE N° 2

• Entreprises de la nouvelle économie et vie privée

Présidée par Anne-Marie Escoffier, ancienne ministre, sénatrice de l'Aveyron

- **M. Yves Le Mouël**, directeur général de la Fédération française des Télécoms
- **Mme Isabelle Falque-Pierrotin**, présidente de la commission nationale de l'informatique et des libertés (CNIL)
- **M. Alain Bazot**, président de l'UFC-Que Choisir
- **M. Marc Mossé**, directeur des affaires publiques et juridiques de de Microsoft France et membre de l'Association des services Internet communautaires (ASIC)
- **M. Loïc Rivière**, délégué général de l'Association Française des Editeurs de Logiciels et Solutions Internet (AFDEL).

TABLE RONDE N° 3

• Prévention/répression de la criminalité et atteintes à la vie privée

Présidée par Yves Détraigne, vice-président de la commission des lois du Sénat

- **M. Alain Zabulon**, coordonnateur national du renseignement
- **M. Dominique Guibert**, vice-président de la Ligue des droits de l'homme (LDH)
- **M. Jean-Jacques Hyest**, sénateur, membre de la commission des lois du Sénat, membre de la Commission nationale de contrôle des interceptions de sécurité (CNCIS)
- **M. Jean-Jacques Urvoas**, député, président de la commission des lois de l'Assemblée nationale, membre de la Commission nationale de contrôle des interceptions de sécurité (CNCIS)
- **M. Olivier Guérin**, délégué général de la Commission nationale de contrôle des interceptions de sécurité (CNCIS)
- **Mme Valérie Maldonado**, chef de service de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC)

TABLE RONDE N° 4

• Quelles règles de droit pour les nouvelles technologies ?

Présidée par Esther Benbassa, vice-présidente de la commission des lois du Sénat

- **Mme Meryem Marzouki**, chercheure au CNRS
- **Me Alain Bensoussan**, avocat spécialiste des nouvelles technologies de l'information et de la communication
- **M. Gaëtan Gorce**, sénateur, membre de la commission des lois du Sénat, membre de la CNIL
- **M. François Pillet**, sénateur, membre de la commission des lois du Sénat
- **Mme Nathalie Metallinos**, responsable de l'atelier « protection des données personnelles » de l'Association pour le développement de l'informatique juridique (ADIJ)

CONCLUSION

- **Mme Axelle Lemaire**, secrétaire d'État auprès du ministre de l'économie, du redressement productif et du numérique, chargée du numérique

ANNEXE 2
GLOSSAIRE

Accountability Obligation de rendre compte et d'expliquer, dans un souci de transparence et de traçabilité afin d'identifier et de documenter les mesures mises en œuvre pour se conformer aux exigences issues de la réglementation Informatique et libertés

Cloud (computing) Ensemble de processus consistant à utiliser la puissance de calcul et/ou de stockage de serveurs informatiques distants à travers un réseau, généralement Internet

Cookies En français, témoin de connexion. Fichier stocké sur le disque dur de l'utilisateur permettant au serveur web de le reconnaître d'une page web à l'autre. Les cookies sont notamment utilisés pour éviter à l'utilisateur de ressaisir des données

Dashboard Tableau de bord

Do not track Option des navigateurs internet permettant à l'utilisateur d'indiquer aux sites qu'il consulte qu'il ne veut pas être pisté à des fins publicitaires

Do not track by default Option précédemment décrite automatiquement activée

GAFA Acronyme de Google, Apple, Facebook, Amazon

ITIF (Information technology and innovation foundation) Fondation pour les Technologies de l'information et l'innovation

Malwares Logiciel malveillant

Playstore Boutique en ligne créée par Google, regroupant une boutique d'application, une boutique de location de films et de série télévisées, et une boutique d'achat de musique, de livres et de magazines

PRISM Programme américain de surveillance électronique, basé sur la collecte de renseignements à partir d'Internet et d'autres fournisseurs de services électroniques

Privacy by design Prise en compte du respect de la vie privée dès la conception du produit informatique

Safe Harbour Agreement
Accord sur la « sphère de sécurité », permettant à une entreprise américaine de certifier qu'elle respecte la législation de l'Espace économique européen (EEE) afin d'obtenir l'autorisation de transférer des données personnelles de l'EEE vers les États-Unis

TIC Technologies de l'information et de la communication

TTIP (*Transatlantic Trade and Investment Partnership*) : Partenariat transatlantique de commerce et d'investissement

Tor (*The Onion Router* : littéralement le « routeur oignon ») : Réseau informatique superposé mondial et décentralisé, Il est composé de routeurs organisés en couches, appelés « nœuds de l'oignon », qui transmettent de manière anonyme des flux répondant au protocole de transport « TCP ». Le réseau Tor peut ainsi rendre anonymes tous les échanges internet basés sur le protocole de communiation « TCP ».