N° 696

SÉNAT

SESSION EXTRAORDINAIRE DE 2013-2014

Enregistré à la Présidence du Sénat le 8 juillet 2014

RAPPORT D´INFORMATION

FAIT

au nom de la mission commune d'information « **Nouveau rôle** *et* **nouvelle stratégie** *pour l'***Union européenne** *dans la* **gouvernance mondiale** *de* **l'Internet** *» (1),*

Par Mme Catherine MORIN-DESAILLY,

Sénatrice.

Tome I : Rapport.

(1) Cette commission est composée de : M. Gaëtan Gorce*, président ;* Mme Catherine Morin-Desailly, *rapporteure ;* MM. Michel Billout, Jean Bizet, André Gattolin, Mme Françoise Laborde, M. Philippe Leroy et Mme Patricia Schillinger, *vice-présidents ;* M. Philippe Adnot, Mme Michèle André, M. Dominique Bailly, Mme Maryvonne Blondin, MM. Jean-Marie Bockel, Pierre Camani, Jacques Chiron, Philippe Dallier, Robert del Picchia, Mmes Michelle Demessine, Marie-Hélène Des Esgaulx, MM. Yves Détraigne, Claude Dilain, Jean-Jacques Filleul, Christophe-André Frassa, Mme Joëlle Garriaud-Maylam, M. Pierre Hérisson, Mme Sophie Joissains, MM. Jean-Yves Leconte, Jean-Pierre Leleux, Jacques-Bernard Magner, Philippe Marini, Rachel Mazuir, Jean-Pierre Plancade et Bruno Retailleau.

SOMMAIRE

SYNTHÈSE

C'est à partir de 1989, date à laquelle l'Organisation européenne pour la recherche nucléaire (CERN) met à disposition du public une application, le *World wide web*, que l'Internet, né dans les années 1960 aux États-Unis, a connu un succès grandissant, si bien que s'y connecte aujourd'hui près de 40 % de la population mondiale. Cet essor prend donc racine sur les deux rives de l'Atlantique, et pourtant l'Internet que nous, Européens, « consommons » en 2014 est très largement américain, le Vieux continent n'ayant pas pris la mesure des enjeux qui s'y attachent. Alors que cette technologie encore jeune s'apprête à déployer sa puissance transformatrice dans les pays en développement et à s'étendre aux objets, les révélations d'Edward Snowden en 2013 ont transformé l'Internet en un sujet politique : à l'initiative de son groupe UDI-UC, le Sénat a créé fin 2013 une mission rassemblant 33 sénateurs pour analyser, dans ce contexte, quel nouveau rôle et quelle nouvelle stratégie l'Union européenne pourrait avoir dans la gouvernance mondiale de l'Internet, que le Sommet mondial sur la société de l'information de 2005 a définie comme « *l'élaboration et l'application par les États, le secteur privé et la société civile, dans le cadre de leur rôle respectif, de principes, normes, règles, procédures de prise de décisions et programmes communs, propres à modeler l'évolution et l'utilisation de l'Internet, évolution dans le sens technologique, utilisation au sens des pratiques* ».

I. LA GOUVERNANCE DE L'INTERNET, UN NOUVEAU TERRAIN D'AFFRONTEMENT MONDIAL

1. L'Internet, la fin d'un mythe

• Porté à l'origine par le monde de la recherche avant d'être rapidement accaparé par les intérêts militaires et commerciaux américains, l'**Internet s'est d'emblée caractérisé par ses dimensions d'horizontalité et d'ouverture, en faisant un instrument technologique accessible par et pour tous** : l'architecture décentralisée, « de bout en bout », de ce réseau de réseaux permet à tout utilisateur de développer des innovations susceptibles de rencontrer un succès mondial et promettant des progrès immenses en matière de santé, d'énergie, d'éducation, de transport... Innovation de rupture, l'Internet révolutionne les modèles économiques et, plus globalement, les relations humaines et la relation de l'être au monde.

• L'Internet apparaît en fait comme un prolongement de la puissance par le droit et l'économie : dès le début des années 90, avant même la

généralisation du web, les États-Unis ont pris des dispositions législatives et fiscales pour acquérir le *leadership* sur cette technologie si bien que, sur les 50 premières entreprises de médias numériques, 36 sont aujourd'hui américaines. Dans les années 2000, la Chine s'est bâti un écosystème d'entreprises numériques parmi les plus importantes, comme la Russie désormais. Faute de volonté politique, l'Europe vit sous la domination commerciale des acteurs américains du net ; cette domination commerciale est le socle d'une domination juridique, de nombreux noms de domaine ressortissant des juridictions américaines, comme d'ailleurs les litiges relatifs aux conditions générales d'utilisation des grandes plateformes.

Du fait de l'effet de réseau, l'Internet évolue vers une hypercentralisation au profit de grands acteurs privés qui constituent des silos verticaux, notamment dans le mobile (terminal/système d'exploitation/ applications). Ces grands acteurs **défient les États**, sapant les moyens de l'action publique par l'optimisation fiscale, rivalisant avec leurs services publics, menaçant leurs modèles économique et culturel, et même frappant monnaie virtuelle.

L'Europe, « colonie du monde numérique », se trouve largement distancée dans cette redistribution des pouvoirs. Sa place est même en recul : seuls 8 groupes européens figurent désormais dans les 100 premiers groupes high-tech dans le monde, contre 12 il y a deux ans. De nombreux facteurs d'explication peuvent être avancés. Quoique dotée d'opérateurs télécoms solides, l'Europe se trouve de fait dépourvue d'acteurs de premier plan aux deux bouts de la chaîne de valeur numérique : les équipementiers et les fournisseurs de contenus et d'applications, également appelés *over the top* (OTT). Elle est ainsi menacée de ne plus avoir accès au savoir et à la connaissance que par la médiation d'acteurs non européens.

• **Par ailleurs**, l'évolution des technologies et des mentalités a transformé la promesse de liberté, que constituait l'**Internet**, en un **fantastique outil de surveillance**. En facilitant le stockage et le traitement, le *big data* a en effet incité à une collecte exponentielle de données, notamment personnelles, que l'Internet des objets devrait encore venir alimenter. Ces données peuvent ainsi être exploitées aussi bien par les géants du net que par les services de renseignement, comme l'affaire Snowden l'a amplement révélé. Le système par défaut est devenu la collecte généralisée de données.

Parallèlement, la dépendance croissante de nos sociétés à l'Internet est devenue facteur de vulnérabilité, si bien que le réseau est maintenant le théâtre de véritables attaques qui peuvent provenir d'Etats, d'organisations ou même d'individus : espionnage économique, déstabilisation, sabotage d'infrastructures critiques. Le *hacking* est devenu une véritable arme et les vulnérabilités informatiques, un marché.

2. Le séisme Snowden transforme la gouvernance de l'Internet en enjeu géopolitique mondial

• La gouvernance de l'Internet présente le même caractère distribué que le réseau, aucune autorité centrale ne gouvernant l'Internet aujourd'hui, ni aucune de ses couches réseau, transport ou application. Une pléthore d'enceintes (IETF, IAB, ISOC, W3C, ICANN...) participent à une forme d'autorégulation du réseau qui a fait la preuve de son efficacité et fonctionne sur un mode ascendant et consensuel, ainsi résumé par D.Clark : « *Nous refusons les rois, les présidents et les votes. Nous croyons au consensus approximatif et au code qui marche.* »

• Mais, pour des raisons historiques, cette gouvernance est américaine, de fait : les géants américains de l'Internet ont intérêt à être présents dans ces diverses enceintes souvent liées aux universités américaines ; 10 des 13 serveurs racine sont aux États-Unis ; l'ICANN est une société de droit californien, et gère le fichier racine du système des noms de domaine, forme d'annuaire central de l'Internet, auquel contribue aussi la société américaine VeriSign, tout ceci sous la supervision du Département du commerce américain. Or la gestion des noms de domaine, et notamment la création de nouvelles extensions génériques, a d'importantes conséquences économiques, voire politiques, comme en témoigne le cas du « .vin » et du « .wine ». Et l'ICANN, en proie aux conflits d'intérêt, fonctionne de manière trop opaque, n'offre pas de droit de recours satisfaisant et ne rend de comptes qu'au seul gouvernement américain, qui a ainsi joué depuis la création de l'ICANN en 1998 un rôle de pourvoyeur de confiance.

• **Cette domination américaine sur la gouvernance de l'Internet a été de plus en plus contestée** : l'Agenda de Tunis, qui a conclu le sommet mondial de la société de l'information en 2005, reconnaît le rôle de tous les acteurs (États, secteur privé, société civile) dans la gouvernance de l'Internet, sur un pied d'égalité, et appelle à leur coopération renforcée. Il fonde à cet effet l'*Internet Governance Forum* (IGF), forum multi-parties prenantes – *multistakeholder* –, onusien mais non interétatique. Doté d'un rôle seulement consultatif, ce forum, qui se réunit annuellement, affiche un bilan médiocre et se trouve concurrencé par une multitude d'événements traitant de la gouvernance de l'Internet. C'est finalement à l'occasion de la **conférence organisée par l'Union Internationale des Télécoms (UIT) à Dubaï en décembre 2012** que l'opposition s'est cristallisée entre les tenants d'une reprise en main étatique de la gouvernance de l'Internet, suspectée de conduire à plus de surveillance, de contrôle et de censure, et les tenants du *multistakeholderism* : une résolution annexée à l'accord final invitait l'UIT, instance onusienne, à prendre un rôle plus important dans la gouvernance mondiale de l'Internet. Dans ce contexte, **la parole européenne reste peu audible, souffrant d'être seulement portée par** la direction générale compétente de **la Commission européenne**, la DG Connect, **sans être**

assumée dans son ensemble par le Conseil qui réunit les États membres. Alors que tous ceux qui interrogent le *statu quo* sont présentés par les États-Unis comme des ennemis de la liberté, l'Union européenne n'est-elle pas bien placée, voire attendue, pour explorer une troisième voie fondée sur une approche véritablement inclusive de la gouvernance d'un Internet bâti sur des valeurs démocratiques?

• **À partir de juin 2013, les révélations d'Edward Snowden** sur la surveillance de masse exercée en ligne par les services de renseignement américains, avec la collaboration des grandes entreprises du net, **font l'effet d'un séisme** : attestant que les États-Unis avaient volontairement affaibli la sécurité en ligne, notamment au sein de l'IETF, elles ébranlent la confiance dans l'Internet, pesant sensiblement sur les résultats de l'industrie numérique américaine, qui se retourne contre son gouvernement. **À Montevideo, en octobre 2013**, les enceintes de gouvernance de l'Internet appellent à une mondialisation de la supervision du fichier racine de l'Internet, tandis que la présidente du Brésil convoque une conférence mondiale sur la gouvernance de l'Internet pour avril 2014. En novembre 2013, le Brésil et l'Allemagne font adopter à l'ONU une résolution réaffirmant le droit à la vie privée à l'ère numérique. **Les États-Unis, « garants » de la liberté en ligne, ont perdu leur magistère moral sur l'Internet**, ce qui rend impossible le *statu quo* dans le système actuel de gouvernance de l'Internet.

• L'électrochoc Snowden inaugure une **ère de soupçon à l'égard des États-Unis, qui vient accélérer une tendance à la fragmentation de l'Internet**, déjà à l'œuvre par stratégie souveraine ou commerciale. Un Internet fracturé contredirait l'esprit d'ouverture de l'Internet et tendrait à donner des moyens de censure supplémentaires à ceux contrôlant ces blocs fermés : comment donc rétablir la confiance des internautes et la sécurité en ligne tout en maintenant l'unicité du réseau ? Le président Obama, dans son discours de janvier 2014 sur l'état de l'Union, n'a pas su répondre : la chancelière allemande a appelé en février 2014 à un « Internet européen » et le Parlement européen a adopté en mars un rapport très offensif en réaction aux pratiques de surveillance en ligne. C'est finalement **le 14 mars**, avant la conférence NETmundial au Brésil, que **l'administration américaine a fait un pas significatif en annonçant son intention, contestée depuis au Congrès, de lâcher du lest sur la supervision du fichier racine du système des noms de domaine**. L'ICANN se voit confier la transition vers une privatisation de cette supervision.

• La **conférence NETmundial**, qui a rassemblé toutes les parties prenantes les 23 et 24 avril à São Paulo, représente une **avancée précieuse** : la déclaration finale de cette conférence, organisée sous la houlette d'une jeune démocratie, consacre certains **principes et valeurs fondamentaux pour l'Internet et sa gouvernance** et condamne la surveillance en ligne, sans renoncer pour autant à l'unicité et l'ouverture de l'Internet. Mais le rôle des

États doit encore être précisé : **la réforme de la gouvernance de l'Internet reste à faire**, à commencer par celle de l'ICANN, monopole privé toujours américain, qui gagne en pouvoir mais pas en responsabilité.

II. UNE OPPORTUNITE HISTORIQUE POUR GARANTIR UN AVENIR DE L'INTERNET CONFORME AUX VALEURS EUROPÉENNES

1. L'Union européenne, médiateur pour une gouvernance garantissant un Internet ouvert et respectueux des droits fondamentaux et des valeurs démocratiques

• L'Internet est un bien commun, ce qui fonde l'action des États pour assurer que cette ressource profite à tous ; sa gouvernance ne saurait être complètement privatisée et doit reposer sur un dialogue entre technique et politique, qui interfèrent tant l'architecture de l'Internet est politique et concerne tous ses acteurs. La mission invite donc les États membres de l'Union européenne à s'entendre pour **proposer la consécration des principes fondateurs du NETmundial de São Paulo par un traité international ouvert à tous les États, qui pourrait être soumis à une forme de ratification en ligne** par les internautes.

Elle recommande aussi de **globaliser la gouvernance de l'Internet sur le fondement des principes du NETmundial** et plaide pour :

– faire émerger **un réseau d'enceintes pour une gouvernance de l'Internet distribuée et transparente**, en formalisant les rôles et interactions entre l'ICANN, les registres Internet, le W3C, l'IETF, l'IAB, l'IUT, les gestionnaires de serveurs racine, les opérateurs de noms de domaine de premier niveau ;

– transformer le Forum pour la Gouvernance de l'Internet en **Conseil mondial de l'Internet**, doté d'un financement propre et chargé de contrôler la conformité des décisions des enceintes de gouvernance aux principes dégagés à São Paulo ; toutes les enceintes appartenant au réseau de gouvernance devraient rendre des comptes devant ce Conseil, pour éviter que se répètent les graves dysfonctionnements déjà constatés et mettant en péril la sécurité en ligne ;

– accueillir en Europe la célébration des dix ans du Sommet mondial pour la société de l'information en 2015 pour promouvoir cette nouvelle architecture mondialisée de la gouvernance de l'Internet.

• Il importe aussi de refonder l'**ICANN** pour restaurer la confiance dans le système des noms de domaine, donc :

– en faire une WICANN (*World ICANN*), de droit international ou, de préférence, de droit suisse sur le modèle du Comité international de la

Croix Rouge, et organiser une supervision internationale du fichier racine des noms de domaine en substitution de la supervision américaine ;

– rendre la WICANN responsable devant le Conseil mondial de l'Internet ou, à défaut, devant une assemblée générale interne et donner au Conseil ou à cette assemblée le pouvoir d'approuver les nominations au conseil d'administration de la WICANN ainsi que les comptes ;

– mettre en place un mécanisme de recours indépendant et accessible, permettant la révision d'une décision de la WICANN, voire sa réparation ;

– établir une séparation fonctionnelle entre la WICANN et les fonctions opérationnelles IANA pour distinguer ceux qui élaborent les politiques de ceux qui attribuent individuellement les noms de domaine ;

– définir des critères d'indépendance pour l'essentiel des membres du *board* de la WICANN afin de réduire les conflits d'intérêts.

Il convient d'exiger avant tout que **le groupe directeur prévu par l'ICANN pour organiser la transition soit composé de membres désignés par les parties prenantes de l'ICANN, selon des modalités transparentes et démocratiques**, et inclue également des représentants des autres parties prenantes non représentées aujourd'hui à l'ICANN.

Le schéma proposé pour cette nouvelle architecture de gouvernance de l'Internet figure en page 179 du présent rapport.

2. L'Union européenne doit prendre en main son destin numérique pour peser dans la gouvernance du net

• **La régulation des acteurs qui font partie de l'écosystème européen du numérique doit se faire offensive** pour améliorer la répartition de la valeur au bénéfice des acteurs européens, sans sacrifier le principe de neutralité du net : les fournisseurs de contenus et d'application doivent faire l'objet d'une **régulation concurrentielle** plus forte, afin que la neutralité s'applique non seulement aux réseaux mais aussi aux services. Parallèlement, la **fiscalité** européenne doit évoluer pour mieux faire contribuer les fournisseurs de services en ligne aux charges publiques des États européens. Enfin, de nouvelles modalités doivent être inventées pour faire vivre la culture européenne sur l'Internet, à commencer par l'alignement des taux de TVA des biens et services culturels numériques et physiques.

• L'Union européenne doit par ailleurs **se doter d'un régime exigeant et réaliste de protection des données à l'ère du *cloud* et du *big data***. L'approche européenne assise sur l'affirmation d'un droit fondamental à la protection des données personnelles est valide et peut donner un avantage comparatif à notre industrie, incitée à être plus innovante : elle doit

être confortée et modernisée, notamment par l'adoption rapide de la proposition de règlement européen en cours de négociation et par l'instauration d'un régime de responsabilité des responsables de traitement de données. Cette approche doit être promue à l'international, ce qui implique de renégocier le *Safe Harbor*, en se gardant la possibilité de le suspendre si les exigences des autorités européennes n'étaient pas entendues, et de tenir cette négociation distincte de celle du traité transatlantique. Devrait aussi être retenue la disposition introduite par le Parlement européen encadrant le transfert de données personnelles à la demande des autorités de pays tiers.

• L'Union européenne doit également **catalyser son industrie numérique autour d'une ambition affichée**, ce qui implique notamment de ne pas empêcher, au titre des règles de concurrence européennes, l'émergence de « champions européens », de faciliter l'accès au financement des entreprises européennes et de développer des *clusters* européens du numérique. En matière commerciale, il faut rendre plus équitables les règles du jeu (en matière d'aides d'État ou de marchés publics) au bénéfice des entreprises européennes du numérique, tout en défendant notre système d'indications géographiques et en veillant à assortir toute libéralisation transatlantique de la circulation des données, d'exceptions justifiées par des objectifs de protection de la vie privée et de sécurité publique.

• Cette ambition industrielle doit **permettre à l'Union européenne d'exploiter ses propres données** au service du « bien commun » : le *big data* doit être promu comme un véritable enjeu industriel, et des mécanismes raisonnables définis pour l'agrégation de données susceptibles de faire l'objet d'une valorisation économique. Le développement de l'*open data* doit être poursuivi, tout en respectant les principes d'anonymat et de non discrimination.

À l'initiative de la France et de l'Allemagne, **deux projets industriels concrets devraient être lancés : un système d'exploitation pour mobiles européen et un *cloud* européen sécurisé**, se différenciant par sa fiabilité et sa transparence attestées par un label, **mais ouvert**. Le potentiel européen en matière de sécurité doit être exploité : les compétences européennes en matière de **chiffrement**, doivent être développées ; les extensions en « .fr » et « .eu », qui ressortent des juridictions française et européenne, doivent être promues au titre de la sécurité juridique. Enfin, l'Europe doit préparer sa place dans l'**Internet de demain**, notamment en étant plus présente dans les grandes instances internationales de standardisation de l'Internet et en veillant à la mise en place en Europe d'un système de normalisation des objets connectés qui favorise leur reconnaissance mutuelle, leur interconnexion et leur sécurité à l'encontre d'attaques extérieures.

• Enfin, l'Union européenne doit **promouvoir une appropriation citoyenne de l'Internet**. Ceci passe par une plus grande sensibilisation des

citoyens au numérique, en garantissant sa place au cœur du socle commun des compétences et en formant progressivement l'ensemble des professeurs en fonction.

Ceci **implique aussi d'actualiser l'encadrement légal des activités de renseignement et d'en améliorer le contrôle politique** : la loi doit garantir la consultation préalable de la Commission nationale de contrôle des interceptions de sécurité (CNCIS) et étendre le contrôle de la CNCIS à la proportionnalité des moyens mis en œuvre par les services de renseignement. À partir de la CNCIS, une nouvelle autorité administrative indépendante – la Commission de contrôle des activités du renseignement – pourrait être créée pour délivrer les autorisations de mise en œuvre des moyens de collecte d'informations après examen de leur légalité et de leur proportionnalité. Les pouvoirs d'investigation de la Délégation parlementaire au renseignement (DPR) devraient en outre être renforcés. Enfin, un cadre européen de contrôle des échanges d'informations entre services de renseignement devrait être établi.

En outre, **la gouvernance des questions numériques doit être mieux structurée politiquement** : au sein du Conseil de l'Union européenne, grâce à une formation dédiée au numérique pour dépasser les cloisonnements administratifs ; au sein du Parlement européen, grâce à des commissions spéciales pour examiner les textes relatifs à l'Internet ; en France, grâce à la création d'un comité interministériel du numérique auprès du Premier ministre et d'une **commission du numérique au Sénat** dont les membres seraient également membres d'une commission permanente législative.

De surcroît, le modèle européen de l'Internet doit être promu par une **véritable diplomatie numérique** ; dotée d'une doctrine claire et de vrais moyens, cette diplomatie doit être associée à une politique industrielle européenne ambitieuse et cohérente et mettre à profit les instruments préexistants tels la politique européenne de voisinage, la francophonie, et la Convention 108 du Conseil de l'Europe sur la protection des données personnelles, pour promouvoir de par le monde le respect des valeurs européennes en ligne.

LISTE DES PROPOSITIONS

I - L'UNION EUROPÉENNE, MÉDIATEUR POUR UNE GOUVERNANCE GARANTISSANT UN INTERNET OUVERT ET RESPECTUEUX DES DROITS FONDAMENTAUX ET DES VALEURS DÉMOCRATIQUES

A. Refonder la gouvernance d'internet autour d'un traité assurant le respect des droits fondamentaux et des valeurs démocratiques en ligne

- inviter les États membres de l'Union Européenne à s'entendre pour proposer la consécration des principes du NETmundial de São Paulo, à la fois par un traité international ouvert à tous les États et par une forme de ratification en ligne par les internautes (n° 1)

B. Construire un réseau mondialise, légitime et responsable d'enceintes de gouvernance

1. Globaliser la gouvernance d'Internet sur le fondement des principes du NETmundial

- asseoir la gouvernance d'Internet sur un réseau de relations transparentes en formalisant les rôles et interactions entre l'ICANN, les registres Internet, le W3C, l'IETF, l'IAB, l'IUT, les gestionnaires de serveurs racine, les opérateurs de noms de domaine de premier niveau… (n° 2)

- transformer le Forum pour la Gouvernance de l'Internet en Conseil mondial de l'Internet, doté d'un financement propre et chargé de contrôler la conformité des décisions des enceintes de gouvernance aux principes dégagés au NETmundial de São Paulo (n° 3)

- accueillir en Europe la célébration des dix ans du Sommet mondial pour la société de l'information en 2015 pour promouvoir cette nouvelle architecture mondialisée de la gouvernance d'Internet (n° 4)

2. Refonder l'ICANN pour restaurer la confiance dans le système des noms de domaine

- refonder l'ICANN pour en faire une WICANN (World ICANN), de droit international ou, de préférence, de droit suisse sur le modèle du Comité international de la Croix Rouge, et organiser une supervision internationale du fichier racine des noms de domaine en substitution de la supervision américaine (n° 5)

- rendre la WICANN responsable devant le Conseil mondial de l'Internet ou, à défaut, devant une assemblée générale interne et donner au Conseil ou à cette assemblée le pouvoir d'approuver les nominations au conseil d'administration de la WICANN et les comptes de cet organisme (n° 6)

- mettre en place un mécanisme de recours indépendant et accessible, permettant la révision d'une décision de la WICANN, voire sa réparation (n° 7)

- établir une séparation fonctionnelle entre la WICANN et les fonctions opérationnelles IANA pour distinguer ceux qui élaborent les politiques d'attribution des noms de domaine de ceux qui attribuent individuellement les noms de domaine (n° 8)

- définir des critères d'indépendance pour l'essentiel des membres du *board* de la WICANN (n° 9)

- exiger avant tout que le groupe directeur prévu par l'ICANN pour organiser la transition soit composé de membres désignés par les parties prenantes de l'ICANN selon des modalités transparentes et démocratiques et inclue également des représentants des autres parties prenantes non représentées aujourd'hui à l'ICANN (n° 10)

II. L'UNION EUROPEENNE DOIT REPRENDRE EN MAIN SON DESTIN NUMERIQUE POUR PESER DANS LA GOUVERNANCE DU NET

A. Une régulation offensive de l'écosystème numérique européen pour une meilleure répartition de la valeur

1. Concrétiser l'ambition de neutralité du net…

- saisir la Commission européenne pour qu'elle soumette sans délai une proposition législative visant à réguler les fournisseurs de contenus et d'application, afin que la neutralité s'applique non seulement aux réseaux mais aussi aux services (n° 11)

2. … l'assortir d'une régulation forte en matière de concurrence et de fiscalité

- solliciter la Commission européenne pour améliorer les procédures de la politique de concurrence et les rendre plus réactives face aux abus de position dominante en ligne (n° 12)

- demander à la Commission de mettre en place un principe de séparation pour éviter l'intégration verticale des acteurs de l'Internet contrôlant de plus en plus de strates de la chaîne de valeur (n° 13)

- encourager les autres États membres victimes de l'optimisation fiscale des multinationales du numérique à exercer avec notre pays une pression continue sur les États membres complices de cette situation (n° 14)

- soutenir l'aboutissement des réformes fiscales en cours en matière de TVA et d'impôt sur les sociétés, pour mieux faire contribuer les fournisseurs de services en ligne aux charges publiques des États européens (n° 15)

3. …et la compléter par de nouvelles modalités pour faire vivre la culture européenne sur l'Internet

- inciter les fédérations professionnelles du secteur culturel à se rapprocher entre États membres pour faire valoir leurs droits en étant unies face aux « over the top » (n° 16)

- aligner les taux de TVA des biens et services culturels numériques et physiques (n° 17)

- intégrer une nouvelle dimension à la politique européenne de la culture, valorisant la créativité des internautes et le partage non marchand de contenus (n° 18)

B. Un régime exigeant et réaliste de protection des données à l'ère du *cloud* et du *big data*

1. Soutenir la validité de l'approche européenne fondée sur l'affirmation d'un droit fondamental à la protection des données personnelles

- promouvoir le *privacy by design* et le *privacy by default* par des labels européens et internationaux (n° 19)

2. Conforter en le modernisant le cadre juridique européen de protection des données

- adopter le plus rapidement possible la proposition de règlement européen sur la protection des personnes physiques à l'égard des traitements de données à caractère personnel (n° 20)

- renforcer les garanties procédurales entourant le traitement des données particulièrement sensibles par l'obligation de fournir des études d'impact sur la vie privée (n° 21)

- instaurer un régime de responsabilité des responsables de traitement de données à deux versants :

- en amont de la collecte, créer une obligation d'étude d'impact sur la vie privée afin de réduire les risques pour les usagers,
- en aval, créer une obligation de signalement des irrégularités dans le traitement des données (n° 22)

3. Promouvoir cette approche à l'international

- renégocier le *Safe Harbor* en se gardant la possibilité de le suspendre si les exigences des autorités européennes n'étaient pas entendues et tenir cette négociation distincte de celle du traité transatlantique (n° 23)

- adopter la disposition introduite par le Parlement européen dans la proposition de règlement encadrant le transfert ou la divulgation de données personnelles à la demande des autorités administratives ou juridictionnelles de pays tiers (n° 24)

- poursuivre les négociations en vue de l'adhésion de l'Union européenne à la Convention 108 afin d'asseoir la légitimité de l'Union à demander aux États-Unis d'y adhérer également (n° 25)

C. Construire une stratégie industrielle européenne pour maîtriser nos données et porter nos valeurs

1. Catalyser l'industrie européenne du numérique autour d'une ambition affichée

- réorienter le dispositif national de soutien à l'export sur le soutien à la R&D et à l'innovation pour les PME et ETI du secteur numérique (n° 26)

- faire émerger, à l'initiative de la France et de l'Allemagne, une véritable politique européenne de l'industrie numérique définissant les champs d'investissement à moyen et long terme, et mobilisant les instruments permettant de les atteindre (n° 27)

- inciter la Commission européenne à concilier les règles de concurrence européennes dans le secteur numérique avec une ambition de puissance industrielle favorisant l'émergence de « champions européens » (n° 28)

- mieux accompagner les TPE, PME et ETI françaises et européennes du secteur numérique en favorisant, à l'échelle nationale comme européenne, la coopération entre elles et en confortant leur accès à des solutions de financement adaptées (renforcement du capital-risque, facilitation de leur introduction en bourse…) (n° 29)

- utiliser davantage les instruments facilitant la mise en place de *clusters* européens dans les secteurs de l'Internet et du numérique (n° 30)

- obtenir la reconnaissance explicite par les États-Unis du système des indications géographiques avant la mise en place des noms de domaine se référant à de telles indications (n° 31)

- veiller à assortir toute libéralisation transatlantique de la circulation de ces données, d'exceptions justifiées par des objectifs de protection de la vie privée des personnes et de sécurité publique (n° 32)

- inciter la Commission européenne à assurer une convergence règlementaire garantissant des règles de jeu équitables *(level playing field)* pour les entreprises européennes du numérique, notamment eu égard à l'encadrement des aides d'État (n° 33)

- promouvoir une plus grande réciprocité dans l'accès aux marchés publics, pour ouvrir aux entreprises européennes des marchés dans les pays tiers (n° 34)

2. Exploiter les données européennes au service du « bien commun »

- promouvoir le *big data* comme un véritable enjeu industriel, source d'amélioration du bien commun, en définissant précisément des mécanismes raisonnables pour l'agrégation de données susceptibles de faire l'objet d'une valorisation économique (n° 35)

- poursuivre le développement de l'*open data* dans l'ensemble des collectivités publiques en standardisant les données délivrées et en tendant vers la gratuité de leur mise à disposition, tout en respectant les principes d'anonymat et de non-discrimination (n° 36)

3. *Lancer deux projets industriels concrets : cloud européen sécurisé mais ouvert pour les données les plus sensibles, et système d'exploitation pour mobile*

- favoriser le développement d'un système d'exploitation sur mobile européen constituant une alternative crédible aux principaux systèmes d'exploitation actuellement existants (n° 37)

- définir une classe de services labellisés « *Secure cloud* », faisant l'objet de cahiers des charges stricts et protecteurs, et promouvoir un acteur européen compétent pour émettre des certificats de sécurité correspondants (n° 38)

- mieux intégrer les solutions *cloud* dans la commande publique et mettre en place un espace de services *cloud* sécurisés à destination des administrations publiques (n° 39)

4. Exploiter les atouts européens en matière de sécurité sur l'Internet

- développer les compétences européennes en matière de chiffrement, notamment en facilitant l'utilisation de certificats (n° 40)

- promouvoir la diffusion du « .fr » et du « .eu » (n° 41)

5. Préparer la place de l'Europe dans l'Internet de demain

- veiller à la préservation du principe européen de non brevetabilité des logiciels (n° 42)

- encourager le développement des logiciels libres par leur intégration dans les marchés publics et par l'imposition de standards ouverts, à condition de développer les compétences pour l'utilisation de ces logiciels et standards (n° 43)

- conforter, au service d'objectifs industriels, la présence de l'Union européenne dans les grandes instances internationales de standardisation de l'Internet et développer les travaux menés par les organisations spécifiquement européennes en ce domaine (n° 44)

- veiller à la mise en place en Europe d'un système de normalisation des objets connectés afin de favoriser leur reconnaissance mutuelle, leur interconnexion et leur sécurité à l'encontre d'attaques extérieures (n° 45)

- renforcer la présence européenne dans les structures de standardisation des technologies industrielle recourant à l'Internet (réseaux intelligents, identité numérique…) et en faire un véritable enjeu économique (n° 46)

- préparer l'Internet du futur par une coordination plus poussée des initiatives et un soutien aux solutions mettant en avant la préservation de la confidentialité sur le réseau (n° 47)

D. Promouvoir une appropriation citoyenne de l'internet

1. Sensibiliser les citoyens aux libertés numériques et former à la programmation

- développer un enseignement ambitieux du numérique en garantissant sa place au cœur du socle commun des connaissances et des compétences et en formant progressivement l'ensemble des professeurs en fonction (n° 48)

2. Renforcer l'encadrement légal des activités de renseignement et en améliorer le contrôle politique

- inscrire dans la loi que l'avis de la Commission nationale de contrôle des interceptions de sécurité (CNCIS) est recueilli préalablement à la délivrance de toute autorisation d'interception de sécurité ou d'accès administratif aux données de connexion (n° 49)

– prévoir automatiquement la consultation de la CNCIS préalablement à la mise en œuvre de tout moyen technique de collecte d'informations dont les services seraient dotés (n° 50)

– étendre explicitement le contrôle de la CNCIS à la proportionnalité des moyens mis en œuvre par les services de renseignement afin d'empêcher une dérive des activités de renseignement vers une surveillance de masse (n° 51)

- créer, à partir de la CNCIS, une nouvelle autorité administrative indépendante – la Commission de contrôle des activités du renseignement -, chargée de délivrer les autorisations de mise en œuvre des moyens de

collecte d'informations après examen de leur légalité et de leur proportionnalité (n° 52)

- renforcer les pouvoirs d'investigation de la Délégation parlementaire au renseignement (DPR) en la dotant d'un pouvoir de contrôle sur pièces et sur place et en prévoyant l'assistance des services de la Commission de contrôle des activités de renseignement (n° 53)

- soumettre au contrôle de la Commission nationale de l'informatique et des libertés les fichiers du renseignement (n° 54)

- établir un cadre européen de contrôle des échanges d'informations entre services de renseignement (n° 55)

3. Structurer la gouvernance des questions numériques aux niveaux national et européen

- créer au sein du Conseil de l'Union européenne une formation dédiée au numérique pour dépasser les cloisonnements administratifs au service d'une ambition politique partagée (n° 56)

- recommander la création au sein du Parlement européen de commissions spéciales pour examiner les textes relatifs à Internet (n° 57)

- créer un comité interministériel du numérique auprès du Premier ministre pour conduire une stratégie d'ensemble cohérente (n° 58)

- créer au Sénat une commission du numérique dont les membres seraient également membres d'une commission permanente législative (n° 59)

- impulser la création d'un Conseil consultatif européen du numérique, véritable *task force* pour éclairer l'exécutif européen et fédérer l'écosystème européen dans un esprit d'équipe (n° 60)

4. Promouvoir le modèle européen de l'Internet par une véritable diplomatie numérique associée à une politique industrielle

- élaborer une véritable doctrine de diplomatie du numérique dotée de réels moyens, en s'appuyant sur un réseau d'expertise et sur une consultation de la société civile et des acteurs économiques (n° 61)

- appuyer la diplomatie numérique sur les instruments préexistants tels la politique européenne de voisinage ou la francophonie, afin de promouvoir à travers le monde le respect des valeurs européennes en ligne (n° 62)

AVANT-PROPOS

« Changer le monde », cette ambition autrefois réservée à la philosophie ou à l'action politiques, n'est-elle pas aujourd'hui clairement revendiquée, de Palo Alto à Mountain Views, par les « institutions » du web ? C'est en tout cas la motivation que se prêtent les patrons du net, leurs collaborateurs ou les créateurs de « start-up ».

Ce qui relevait autrefois de la pensée et de l'éthique, à savoir transformer ou améliorer notre condition, ressortirait désormais de l'invention et de la technologie !

Certes, il faut prendre pareille assertion avec le recul que ne permet pas encore la jeunesse du net et de ses principaux acteurs. Mais elle traduit plus qu'un changement de perspective. C'est d'une autre vision du monde que prétendent en effet s'inspirer les Apple, Amazon, Facebook et plus encore Google dont les laboratoires travaillent à une « humanité augmentée ». Mais c'est aussi à la remise en question de notions associées à nos démocraties libérales, comme le respect de la vie privée, que l'on est en train d'assister.

À l'augmentation exponentielle des capacités intrusives de l'État et de ses services de renseignement vient s'ajouter une volonté constante de « rester en contact », « d'évaluer la performance », bref de limiter la vie sociale à l'immédiat et au mesurable accentuant encore le risque d'obsolescence de l'homme pointé par le sociologue allemand Günther Anders voici plus d'un demi-siècle.

L'intime, le travail et plus encore le temps, qui constituent les bases de notre civilisation, seront de plus en plus mis en cause par ce que Lewis Mumford appelait « l'idéologie de la machine » si nous ne prenons pas la peine de redéfinir ce que nous considérons comme les conditions et les critères du « développement humain. » Le changement ne saurait être considéré comme sa propre fin : seule la personne, son épanouissement, sa liberté doivent être regardés pour telle, ce qui implique tout aussi bien la cohésion de la société dans laquelle elle vit que la préservation de l'environnement dont elle dépend.

Or, plus la technologie nous permet de savoir de choses sur le monde, plus l'idée que nous pouvons nous en faire se trouble. N'est-ce pas d'ailleurs ce paradoxe que les fondateurs de l'Internet voulaient, au nom « d'une cause commune », aider à dépasser avant que ne l'emporte dans les années 90 une logique de l'appropriation privée des données et de concentration des médias supports ?

Au-delà des enjeux économiques et de souveraineté, des questions posées sur les réformes de la gouvernance du système Internet, de l'analyse

des ambitions des États et des principaux acteurs, au-delà même d'un plaidoyer pour que l'Europe se dote d'une véritable stratégie afin de reconquérir une souveraineté numérique aujourd'hui écornée, ce rapport est d'abord une invitation faite aux responsables politiques comme aux citoyens à reprendre leur destin technologique en mains. Plus que jamais, ce sont des « valeurs » qui doivent guider nos choix et pas la seule logique des marchés, le lobbying des puissants ou la fascination pour l'innovation. Ainsi devons-nous, par exemple, affirmer et expliciter le droit au contrôle et au libre partage de ses données par le citoyen ! Ainsi devons-nous travailler à faire du web une économie de services plutôt qu'un outil de marketing !

Le numérique constitue sans doute une formidable opportunité. Mais outre le fait qu'il ne se développe pas sans nourrir de nouveaux rapports de force ou créer de nouvelles inégalités, son expansion doit rester soumise à la volonté démocratique et s'inspirer d'une idée de l'homme sur laquelle il ne saurait être question de transiger. Sans l'adhésion à cette éthique renouvelée, comment croire que les capitaines d'industrie disposant de milliards d'informations renonceront à les concentrer plus encore dans le seul but d'accroître leur influence, leur performance et leur richesse ? Sans de fortes convictions (et de sérieux contrôles) comment espérer que les patrons des services de renseignement s'interdiront d'accroître encore leur capacité de surveillance et leur puissance ? Le « nouveau scientisme », cette foi irrésistible dans la bonté et la beauté des processus numériques, constitue le meilleur allié des capteurs de pouvoir ou d'influence que secrète toute société. Et si l'abus qu'ils ont été susceptibles de faire d'une technologie de la communication, comme l'affaire Snowden l'a par exemple démontré, ne saurait justifier une défiance systématique à son encontre, elle devrait suffire à convaincre tout esprit avisé de se garder des naïvetés et des utopies qui pullulent autour du web. L'homme ne doit jamais faire l'économie de savoir ce qu'il veut et d'en décider collectivement. C'est à quoi ce rapport prétend modestement contribuer !

Gaëtan Gorce

Président de la mission

INTRODUCTION

« Internet, c'est nous. Ça nous appartient, en bien et en mal. »
Joël de Rosnay

L'Internet participe de la mondialisation générale des espaces par la technique, qui s'opère depuis plusieurs siècles. Mais peut-on citer une autre invention technique qui ait été adoptée par près de trois milliards de personnes en l'espace d'une génération et autant révolutionné le monde ? Amazon a été lancé en 1995, Google il y a quinze ans, Facebook il y a dix ans : cette industrie a connu la croissance la plus rapide de l'histoire, et compte aujourd'hui les deux premières capitalisations mondiales – Apple et Google.

Né dans les années 1960 aux États-Unis, l'Internet, qui permet la transmission d'informations entre réseaux grâce à l'usage de protocoles standardisés, a connu un large essor à partir de 1989, date à laquelle l'Organisation européenne pour la recherche nucléaire (CERN) met à disposition du public une application, le *World Wide Web*, qui permet de consulter, avec un navigateur, des pages accessibles sur des sites *via* l'Internet. C'est à partir de cette date que l'Internet a connu un essor fulgurant, si bien que s'y connecte aujourd'hui près de 40 % de la population mondiale. Cet essor prend donc racine sur les deux rives de l'Atlantique, et pourtant l'Internet que nous, Européens, « consommons » en 2014 est très largement américain, et même californien. Le monde politique des grands pays européens, ainsi que les entreprises du Vieux continent, n'ont pas pris la mesure des enjeux attachés à cette avancée technique, que M. Michel Serres, membre de l'Académie française, auteur de *Petite poucette* (2012)[1], met sur le même plan que l'imprimerie tant elle constitue une rupture dans l'histoire de l'humanité. Pourtant l'Internet ouvre un nouvel espace public de coexistence : c'est donc un espace essentiellement politique.

Désormais, l'Internet a pris une telle place dans nos vies que nous n'imaginerions plus nous en passer ; il a transformé notre façon de communiquer, d'échanger, de travailler, de nous distraire, d'accéder à la connaissance et à la culture. L'Internet est une technologie encore jeune et sa puissance transformatrice est loin d'avoir terminé de se déployer, d'autant que l'Internet va connaître une « désoccidentalisation accélérée » : sur les deux milliards d'internautes supplémentaires que devrait compter la planète en 2020, plus de 90 % proviendront des pays hors OCDE. L'Internet commence aussi à s'étendre aux objets : 1,4 milliard de terminaux étaient

[1] Petite Poucette, *Michel Serres, Ed. Le Pommier, 2012.*

connectés à l'Internet fin 2012 ; ils devraient être 14 milliards en 2022, ce qui produira une quantité incommensurable de données en ligne. Les perspectives de progrès qui s'ouvrent sont aussi grandes que les craintes que soulèvent les effets incertains de cette mise en réseau du monde, notamment sur l'emploi mais, plus globalement, sur les fondements de nos économies, de nos sociétés, de nos cultures et de nos systèmes politiques.

Car l'Internet, présenté comme un nouvel espace de libertés, elles-mêmes constitutives de capacités comme l'a fait valoir M. Amartya Sen, fait aujourd'hui figure de menace première pour nos droits et libertés fondamentaux.

La rançon du succès de l'Internet est brutalement apparue au grand jour l'été dernier quand M. Edward Snowden, ancien consultant pour la *National Security Agency* (NSA), a révélé l'ampleur de la surveillance exercée en ligne par les services de renseignement. Considéré comme un traître sur la côte Est des États-Unis, et comme un héros côte Ouest, M. Snowden a trouvé refuge en Russie, ravivant des antagonismes que l'on pouvait croire dépassés depuis la fin de la guerre froide. Même si la collecte de données par les entreprises du net était déjà suspectée de croître à l'insu des internautes, ces révélations ont réveillé les esprits, rompant le consensus positiviste béat sur la vraie nature du réseau et délégitimant la mainmise américaine sur la gouvernance de l'Internet. L'Internet est enfin devenu un sujet politique.

C'est dans ce contexte qu'à l'initiative de son groupe Union des Démocrates et Indépendants-UC, le Sénat a décidé le 6 novembre 2013 la création d'une mission commune d'information. Elle réunit 33 sénateurs, qui en ont confié la présidence à M. Gaëtan Gorce, sénateur de la Nièvre et membre de la Commission nationale de l'informatique et des libertés (CNIL) ; Mme Catherine Morin-Desailly, sénatrice de Seine-Maritime qui avait convaincu son groupe politique de demander la création de cette mission, en a été nommée rapporteure. Présidente du groupe Médias et nouvelles technologies du Sénat, elle a pu s'appuyer sur le rapport qu'elle avait déjà rendu en mars 2013, au nom de la commission des affaires européennes, pour dénoncer l'apathie par rapport à la révolution numérique en cours, exposant l'Union européenne à devenir « une colonie du monde numérique ».

Votre mission commune d'information s'est donc attelée à déterminer, dans ce contexte inédit « post-Snowden », quel nouveau rôle et quelle nouvelle stratégie l'Union européenne pourrait avoir dans la gouvernance mondiale de l'Internet.

Ce concept de gouvernance de l'Internet reste délicat à définir ; il se prête à des généalogies historiques et donne lieu à des affrontements théoriques. Il résulte de la traduction de l'anglais : *Internet governance*, notion ambivalente qui recouvre aussi bien la gouvernance de l'Internet – entendue comme la gestion technique de ce réseau de réseaux, de son architecture, de

ses ressources critiques – que la gouvernance sur l'Internet – à savoir les voies et moyens pour faire respecter certaines règles en ligne, malgré le caractère transnational du réseau qui défie les frontières et les souverainetés.

La notion-même de gouvernance est apparue au sein des Nations unies en 1995, dans un rapport intitulé *Notre voisinage global*, initié en 1992 par Willy Brandt, dans le cadre d'une commission sur la gouvernance globale : « *La gouvernance est la somme des multiples voies par lesquelles les individus et les institutions gèrent leurs affaires communes. Elle est un processus continu, à travers lequel les conflits et les intérêts peuvent être conciliés, et des actions de coopération décidées. Cela inclut autant des institutions formelles et des règles destinées à mettre en œuvre des engagements, que des arrangements informels, sur lesquels des personnes et des institutions peuvent être d'accord, ou qu'elles considèrent comme de leur intérêt* ». Le gouvernement, institution formelle et hiérarchique qui s'impose de manière unilatérale sur un territoire donné, se distingue donc – même s'il peut y participer – de la gouvernance, qui requiert la collaboration multilatérale, formelle ou informelle, d'acteurs variés aux intérêts croisés. La gouvernance se différencie également de la régulation, qui a une couleur plus économique et désigne un ensemble d'actions destinées à encadrer le fonctionnement d'un marché.

La notion de gouvernance trouve une application naturelle concernant l'Internet, du fait des difficultés que crée le partage de cet espace commun : conflits de culture et de juridiction par rapport à des pratiques illicites ou dommageables, absence de régime – au sens des relations internationales – et défaut d'instrument pour l'appréhender à l'échelon pertinent qui est mondial.

Lors du sommet mondial sur la société de l'information, qui s'est tenu sous l'égide des Nations unies en 2005, un groupe de travail a néanmoins élaboré la définition suivante : « *Il faut entendre par gouvernance de l'Internet l'élaboration et l'application par les États, le secteur privé et la société civile, dans le cadre de leur rôle respectif, de principes, normes, règles, procédures de prise de décisions et programmes communs, propres à modeler l'évolution et l'utilisation de l'Internet, évolution dans le sens technologique, utilisation au sens des pratiques* ». Cette définition reflète bien l'ambivalence intrinsèque de l'Internet dont le fonctionnement repose sur une imbrication de normes issues de la technique comme de la loi, sans organisme de tutelle centralisé. Quel ordonnancement peut-on y donner, dans quelles instances, avec quels instruments ? Comment concilier la liberté sur l'Internet avec les nombreux défis que sont la lutte contre la cybercriminalité, la protection de la vie privée des internautes, l'encadrement de la marchandisation des échanges et des données personnelles, la protection de la diversité culturelle et de la propriété intellectuelle, la protection de l'ordre public et de la sécurité des États ?

Répondre à ces questions demande de repolitiser la notion de gouvernance et il est apparu à votre mission que le moment était opportun

pour cela et particulièrement propice à une redistribution des rôles. L'Europe a une carte à jouer à l'heure où la mainmise américaine sur l'Internet est désavouée, ce qui donne lieu à des revendications multiples de reconquête de souveraineté, revendications légitimes qui ne manquent pas d'inquiéter quand elles émanent de régimes autoritaires. Comment prévenir le risque d'une fragmentation de l'Internet en blocs régionaux voire nationaux ? Car, si l'Internet bouleverse les souverainetés, c'est aussi cela – le fait qu'il soit un espace partagé – qui fait sa richesse.

Pour éclairer sa réflexion, votre mission a procédé à une soixantaine d'auditions, faisant appel aussi bien à des institutions, des acteurs privés, des chercheurs, des représentants des internautes… Elle a par ailleurs sollicité les contributions des internautes, qui ont été plusieurs dizaines à s'exprimer. Elle a également effectué plusieurs déplacements. Elle s'est d'abord rendue à Bruxelles, pour cerner le positionnement des institutions européennes sur le sujet. Convaincue du caractère moteur de l'axe franco-allemand en Europe, sur ce sujet comme sur d'autres, elle est allée à Berlin rencontrer notamment la Commission « Agenda numérique » tout juste créée au Bundestag. Elle a enfin effectué un déplacement aux États-Unis, où elle a pu s'entretenir aussi bien avec l'administration Obama, des membres du Congrès que des représentants des plus grandes entreprises de l'Internet ou des universitaires.

Au terme de plus de six mois de travaux, votre mission propose d'abord de retracer comment la gouvernance de l'Internet est devenue un nouveau terrain d'affrontement mondial : les révélations d'Edward Snowden ont fait tomber le mythe originel de l'Internet et révélé sa nature hybride, puisqu'il est aussi un instrument de puissance – qui échappe largement à l'Europe – et le support d'un monde d'hypersurveillance et de vulnérabilité. Le soupçon qui en résulte frappe aussi le système de gouvernance de l'Internet, encore sous domination américaine ; la conférence de São Paulo fin avril 2014 a ainsi tenté de définir des principes et une feuille de route pour la gouvernance à venir de l'Internet, tandis que les États-Unis annonçaient leur intention de céder la main sur la gestion des ressources critiques de l'Internet.

Convaincue que la révolution numérique ne s'arrêtera pas et que le monde ne reviendra pas en arrière, votre mission estime que s'offre à l'Europe une opportunité historique pour garantir un avenir de l'Internet conforme à ses valeurs et dans lequel elle pourra imprimer sa marque à l'échelle mondiale. Elle propose à cette fin que l'Union européenne se pose en médiateur pour dessiner une gouvernance assurant un Internet ouvert et respectueux des droits et libertés fondamentaux. Mais votre mission considère que l'Europe ne peut être crédible dans ce rôle que si elle reprend en main son avenir numérique, ce qui signifie : mieux répartir la valeur dans l'écosystème numérique européen ; finaliser un régime exigeant et réaliste de protection des données à l'ère du *cloud* et du *big data* ; construire une

stratégie industrielle dans l'ensemble des secteurs clés de l'Internet pour maîtriser ses données et porter ses valeurs dans le cyberespace ; et enfin promouvoir une appropriation citoyenne de l'Internet.

CHAPITRE PREMIER : LA GOUVERNANCE DE L'INTERNET, UN NOUVEAU TERRAIN D'AFFRONTEMENT MONDIAL

La vision béate d'un Internet, qui ne serait qu'un espace de liberté et d'émancipation, a été brisée par les révélations en juin 2013de M. Edward Snowden sur la surveillance en ligne.

Depuis déjà quelques années, l'essor fulgurant de l'Internet et le bénéfice qu'en tirent certains plus que d'autres avait fait naître des crispations au regard de la redistribution des pouvoirs en résultant. Mais c'est sans conteste « l'affaire Snowden » qui a achevé de transformer l'enjeu de la gouvernance de l'Internet en un nouveau terrain d'affrontement mondial.

I. INTERNET, LA FIN D'UN MYTHE

Initialement considéré comme un espace de liberté à réguler, l'Internet est progressivement apparu, à la faveur de son succès, comme un instrument de puissance, échappant d'ailleurs largement à l'Europe, et comme support d'un monde d'hypersurveillance et de vulnérabilité.

A. L'INTERNET, UN « MIRACLE » PLANÉTAIRE OUVRANT UN NOUVEL ESPACE DE LIBERTÉ ET DE REDISTRIBUTION DU POUVOIR

Apparu dans la nébuleuse des innovations libertaires et utopistes des années 60, l'Internet, porté à l'origine par le monde de la recherche avant d'être rapidement accaparé par les intérêts militaires et commerciaux, s'est caractérisé par ses dimensions d'horizontalité et d'ouverture, en faisant un instrument technologique accessible par et pour tous.

1. La naissance de l'Internet

a) Un projet à l'origine initié par le monde de la recherche

Si l'Internet, le « réseau des réseaux », est devenu aujourd'hui une « *infrastructure informatique généralisée* »[1] d'extension planétaire, ses **origines ont pourtant été confidentielles**, liées à une **poignée d'informaticiens passionnés** dans un **milieu purement universitaire**.

[1] *Expression tirée de l'article « Un bref historique de l'Internet », publié sur le site de l'*Internet Society : *http://www.internetsociety.org/fr/Internet/qu'est-ce-que-l'Internet/histoire-de-l'Internet/un-bref-historique-de-lInternet#Origins*

En août 1962, un chercheur du *Massachusetts Institute of Technology* (MIT), J. C. R. Licklider, imagina en effet l'**interconnexion d'un ensemble d'ordinateurs à l'échelle mondiale** afin de former un « réseau galactique ». Le terme d'origine américaine « Internet » dérive ainsi du concept d'*Internetting (*ou *internetworking)*, c'est-à-dire de mise en relation de réseaux. Son développement théorique, puis les premières expérimentations d'interconnexion, au cours des années 60, continuèrent d'être menées par des chercheurs et universitaires, notamment au sein du MIT, mais également de l'*University of California Los Angeles* (UCLA) ou de celle de Stanford[1].

« *Pendant des années,* ***l'Internet s'est développé sans le concours de l'industrie des télécommunications****, celle-ci le regardant avec méfiance, le considérant comme un réseau bizarre, sans centre* », fait ainsi observer à votre mission d'information M. Maurice Ronai, membre élu de la formation restreinte de la Commission nationale de l'informatique et des libertés (CNIL), co-auteur du rapport *République 2.0 : vers une société de la connaissance ouverte* (avril 2007). « *L'Internet a prospéré sans l'industrie des systèmes d'exploitation, et sans les constructeurs d'ordinateurs personnels, qui ont longtemps refusé d'intégrer des modems à leurs ordinateurs*. »

Comme l'a expliqué un expert en sécurité reconnu, Bruce Schneier, cité par Maurice Ronai, l'invention de l'Internet relève d'un ensemble d'éléments favorables réunis concomitamment. Il s'agit selon lui d'un **« *accident fortuit* » qui résulte « *d'un désintérêt commercial initial des entreprises, d'une négligence des gouvernements et de l'inclinaison des ingénieurs à construire des systèmes ouverts, simples et faciles* ».**

L'échelle de développement sans précédent que connaît aujourd'hui le réseau Internet, **et son immixtion chez des particuliers**, étaient alors **insoupçonnés**. Comme le rappelle l'Internet Society, « *le modèle original était composé de réseaux au niveau national […], desquels seuls un nombre relativement faible était censé exister* ». Ainsi, « *une adresse IP de 32 bits fut utilisée, dont les 8 premiers bits signifiaient le réseau et les 24 bits restants désignaient l'hôte sur ce réseau. L'hypothèse que 256 réseaux seraient suffisants dans un avenir prévisible, a manifestement eu besoin d'être reconsidérée lorsque les réseaux locaux ont commencé à apparaître à la fin des années 1970*. »

C'est bien, en effet, le **développement exponentiel de l'informatique personnelle** à partir du milieu des années 70 qui entraînera dans le même temps l'interconnexion des réseaux à grande échelle. Comme le rappelle Maurice Ronai, « *en 1975, on dénombrait aux États-Unis 200 000 ordinateurs, 25 millions en 1985, 90 millions en 1995, 225 millions en 2005. On en compte 1,4 milliard aujourd'hui, auxquels il faut ajouter 400 millions de tablettes et 1,6 milliard de smartphones, tous majoritairement connectés à l'Internet. Il s'agit d'un véritable changement d'échelle.* »

[1] *En parallèle, et sans que chaque groupe de chercheurs n'ait connaissance des autres, furent menés des travaux du même type au* National Physical Laboratory *(NPL) britannique et dans la fondation américaine RAND.*

b) Une technologie rapidement prise en mains par la structure militaire

L'origine universitaire de l'Internet s'accompagne, dès ses débuts, d'une **préemption par la sphère militaire** d'une technologie perçue comme prometteuse, notamment pour ses **applications potentielles dans le domaine de la défense**. Les années 60 constituent en effet le cœur de la Guerre froide, durant laquelle toute avance technologique était cruciale pour les deux blocs antagonistes que fédérèrent les États-Unis et l'Union soviétique.

C'est ainsi que Licklider, pionnier du concept de l'Internet, avait pour objectif de **faciliter les communications entre chercheurs de l'agence pour les projets de recherche avancée de défense** : la *Defense Advanced Research Projects Agency* (**DARPA**)[1], agence du département de la défense des États-Unis chargée de la recherche et développement des nouvelles technologies destinées à un usage militaire.

En octobre 1962, Licklider devint d'ailleurs le premier chef du programme de recherche en informatique de la DARPA. L'un de ses principaux successeurs au MIT, Lawrence G. Roberts, fut à son tour engagé par la DARPA fin 1966 pour développer le concept de réseau informatique, ce qui lui permettra de **mettre au point le réseau ARPANET**. Premier réseau à transfert de paquets, ce dernier constitue le véritable ancêtre de l'Internet.

Reposant sur l'interconnexion d'ordinateurs hôtes à travers des « nœuds », il se vit assigner comme objectif de **maintenir et sécuriser les communications militaires** « *quel que soit l'état de destruction du pays* ». Sa construction en rhizome permettait en effet, en cas de destruction de l'un de ses nœuds, d'emprunter d'autres chemins pour atteindre systématiquement les destinataires désignés, gage de son invulnérabilité supposée.

La **validation par la sphère militaire des aspects techniques de l'Internet naissant** fera beaucoup pour son développement. Ainsi, les protocoles TCP/IP (*Transmission Control Protocol/Internet Protocol*), élaborés dans les années 70[2] et que nous continuons d'utiliser aujourd'hui, ont été reconnus comme standards par la défense américaine.

Ainsi que le souligne l'Internet Society, « *cela permit à la défense de commencer le partage dans la base technologique de l'Internet de DARPA et mena directement à la segmentation des communautés militaire et non militaire* ». La **transition d'ARPANET du protocole NCP à TCP/IP** lui permit d'être scindé en deux réseaux, un réseau supportant des exigences opérationnelles de défense (MILNET) d'un côté, et ARPANET destiné à la recherche et au développement de l'autre.

---

[1] *L'*Advanced Research Projects Agency *(ARPA) a été rebaptisée* Defense Advanced Research Projects Agency *(DARPA) en 1971, puis à nouveau ARPA en 1993, avant de redevenir DARPA en 1996 pour en conserver l'acronyme.*

[2] *Voir* infra.

L'empreinte militaire sur la création du net ne doit pas masquer une **dimension antagonique, pourtant très présente** dès l'origine : celle de ses **sources libertaires**. Faisant état de « *l'irruption sur le net de la contre-culture américaine des années 1970* » et citant l'ouvrage de Fred Turner, *Aux sources de l'utopie numérique*, qui la retrace, M. Philippe Lemoine, président directeur-général de LaSer, président de la Fondation pour l'Internet nouvelle génération, chargé par le Gouvernement en janvier 2014 d'une « mission pour la transformation numérique de notre économie », a expliqué à votre mission comment le « *love summer* » de 1967 a précipité 700 000 jeunes américains urbains vers les campagnes, et de quelle façon ce milieu a généré les communautés virtuelles qui se sont formées sur le net.

« *Cette composante libertaire d'origine se retrouve dans le numérique, qui, en même temps qu'il représente à la fois les plus grosses entreprises et la plus grande forme de capitalisation boursière mondiale, est habité par des utopies libertaires fortes* », a observé Philippe Lemoine. Ce **contraste accentué entre considérations financières et créativité débridée** est toujours présent dans les entreprises dominant le monde du numérique, comme Apple, Google ou Facebook. Bien que constituant aujourd'hui des multinationales, elles laissent une liberté extrêmement importante à leurs ingénieurs et cherchent à stimuler leur inventivité et leur originalité en gommant l'organisation hiérarchisée des tâches que connaissent des entreprises plus traditionnelles.

c) Une ouverture plus tardive aux intérêts commerciaux

Mis au point par et pour les chercheurs, en partenariat étroit avec les intérêts de la Défense, l'**Internet échappait à l'origine à toute visée commerciale**. Ainsi que le fait observer le document de présentation de l'Internet Society, les premiers réseaux – y compris ARPANET – « *furent construits dans un but précis, c'est-à-dire qu'ils étaient destinés, et largement limités, à des communautés fermées d'universitaires* ».

En 1985, la *National Science Fondation* (NSF) créait le **NSFNET, un réseau reliant des centres de recherche et d'éducation**. Basé sur l'ARPANET, le NSFNET a constitué l'épine dorsale de l'Internet pour les États-Unis. Il proposait ses services **gratuitement** pour les institutions scolaires et les chercheurs américains, au-delà desquels il ne pouvait être étendu. La politique d'utilisation de la NSF interdisait en effet l'utilisation de l'épine dorsale à des fins « *non en faveur de la recherche et de l'éducation* ».

Ce n'est que plus tardivement, avec notamment la **privatisation de la NSF dans les années 90**, qu'interviendra la transition d'un réseau construit à partir des routeurs de la communauté de recherche vers un équipement proprement commercial. Comme le souligne l'Internet Society, « *l'Internet a évolué au-delà de ses racines essentiellement de recherche pour inclure à la fois une communauté d'utilisateurs au sens large et une activité commerciale accrue* ».

Aujourd'hui, la **dimension commerciale de l'Internet est devenue prépondérante**, selon des modèles économiques toutefois différents. Apparu dans les années 90, concomitamment au développement du Web, le **commerce électronique** (ou « e-commerce ») atteignait un chiffre d'affaires colossal de 1 221 milliards de dollars en 2013, d'après l'institut eMarketer.

Mais les nouveaux « géants du Web » se financent également, pour certains d'entre eux, par un autre modèle, basé sur la **publicité**. C'est le cas notamment de Google, dont le chiffre d'affaires en 2013 a dépassé les 60 milliards de dollars.

d) Une Europe « précurseure », mais progressivement distancée

Si les chercheurs américains et leurs universités de rattachement ont joué un rôle majeur dans la mise au point de l'Internet, l'Europe y prit également pleinement sa part, avant cependant de laisser les États-Unis développer le dispositif sur une plus grande échelle.

La mise au point de l'Internet proprement dit doit beaucoup aux travaux d'un **informaticien français, M. Louis Pouzin, un des pères de l'Internet**. Formé en partie aux États-Unis, au MIT, il dirigea, de 1970 à 1978, le **projet Cyclades** qui, porté par des partenaires industriels sous la supervision des pouvoirs publics, chercha à créer un « ARPANET à la française ». Inventeur du datagramme et concepteur du premier réseau à commutation de paquets, il vit ses travaux largement utilisés par M. Vinton Cerf, devenu entre-temps vice-président de Google, pour la mise au point de l'Internet et du protocole TCP/IP. C'est d'ailleurs au titre de ses travaux sur TCP/IP qu'il a été récompensé en mars 2013 par le premier prix *Queen Elizabeth for Engineering*.

Par ailleurs, l'**Organisation européenne pour la recherche nucléaire** (CERN) fut l'un des acteurs majeurs de la mise au point du *World Wide Web*. En 1989, l'un de ses ingénieurs informaticiens, M. Tim Berners-Lee, propose de créer un système hypertexte sur son réseau informatique pour permettre à ses collaborateurs de partager des informations. Avec son collègue belge M. Robert Cailliau, qui le rejoint ensuite dans ses travaux, il conçoit le *World Wide Web*.

Jusqu'en 1993, c'est principalement sous l'impulsion de ces deux hommes, en Europe, qu'est développé le Web. En avril de cette même année, le **CERN met dans le domaine public toutes les technologies** qu'il a développées autour de ce concept. Le relai est alors pris par les États-Unis, avec la mise au point d'un navigateur Web, NSCA Mosaic, développé au *National Center for Supercomputing Applications* (NCSA), dans l'Illinois.

Ce navigateur pose les linéaments de l'interface graphique des navigateurs modernes, par l'intégration des images au texte, popularisant ainsi à une grande échelle l'usage du Web. Certains de ses développeurs s'en inspireront pour mettre sur le marché, fin 1994, Netscape Navigator, avec le

succès que l'on sait. Fin 1995, Microsoft lancera, avec la sortie d'Internet Explorer, une **guerre des navigateurs** dans laquelle l'Europe sera définitivement marginalisée.

Cette mise à l'écart du Vieux continent dans la compétition internationale pour la maîtrise et le développement de l'Internet n'avait rien d'une fatalité. Elle résulte au contraire d'un **manque de vision politique et d'une absence de stratégie de long terme** dans un domaine pourtant fondamental pour l'avenir de nos économies. **Cette carence** – pour ne pas dire cet abandon, voire cette démission – **de l'Europe a largement facilité la mainmise des États-Unis sur l'organisation du réseau ; elle est, en tant que telle, en grande partie à l'origine de l'américano-centrisme de l'Internet**.

Comme le relevait M. Louis Pouzin lui-même devant votre mission, en matière d'innovation, « ***l'Europe est pratiquement restée muette*** *depuis que l'on a abandonné l'idée d'être* leader *en matière de réseaux, dans les années 1970 et 1980. Faute de concurrence, ce sont essentiellement les Américains qui innovent dans ce domaine* ». Même analyse de la part de M. David Fayon, administrateur des postes et télécommunications, auteur de *Géopolitique d'Internet : qui gouverne le monde ?* (2013)[1], pour qui « *en France, nous manquons singulièrement d'ambition et de continuité dans l'action (…). Le général de Gaulle a lancé le Plan calcul, et depuis, il n'y a quasiment rien eu* ».

Favorable au projet Cyclades porté par M. Louis Pouzin, M. Maurice Allègre, délégué à l'informatique du Plan calcul, justement, éprouvait les mêmes regrets. Il expliquait en 1999, s'être « *heurté à un mur* » lorsqu'il avait cherché à « *faire adopter le projet par la direction générale des télécommunications comme base pour leur futur réseau de transmissions de données* ». « ***Nous aurions pu être parmi les pionniers du monde Internet*** », regrettait-il, avant de reconnaître que « *nous n'en sommes que des utilisateurs, fort distants des lieux où s'élabore le futur* »[2].

Une fois passée la période des pionniers, et une fois réalisée la prise de conscience du potentiel extraordinaire de cette innovation, les acteurs se sont mobilisés pour se l'approprier et bénéficier de ses retombées. « ***L'initiative est venue du sommet, et le financement, de l'armée*** », a expliqué à votre mission M. Bernard Stiegler, directeur de l'institut de recherche et d'innovation du Centre Pompidou. La différence d'approche avec l'Europe est pour lui flagrante : aux États-Unis, « *il y a bien 52 États, avec des différences très fortes, y compris dans le droit, mais l'État fédéral américain est là pour les grandes orientations, pour la prospective – alors que l'Union européenne en est parfaitement incapable, parce qu'elle ne résiste pas aux* lobbies ».

Et c'est ainsi que le futur, aujourd'hui, s'élabore outre-Atlantique.

---

[1] Géopolitique d'Internet : qui gouverne le monde ?, *David Fayon, Ed. Economica, 2013.*

[2] *Cité par Stéphane Foucart dans son portrait sur « Louis Pouzin, L'homme qui n'a pas inventé Internet », publié dans* Le Monde *du 5 août 2006.*

2. Un système conçu comme ouvert et décentralisé, mais exposé à des pressions contraires

a) L'interopérabilité, un concept central dans la création de l'Internet

L'essence même de l'Internet est, dès sa conception, de constituer un « *interréseautage en architecture ouverte* » ou une « ***architecture interréseaux*** », pour reprendre l'expression de l'Internet Society. L'image de la **toile d'araignée** – l'expression de « toile » est d'ailleurs souvent retenue pour désigner le réseau – et de ses innombrables liens rend bien compte du **caractère polycentré** de l'Internet, par opposition à celle d'architecture « en étoile » caractérisant d'autres réseaux (Minitel, par exemple). Dans cette approche, chacun des réseaux constitutifs du « méta-réseau » peut être conçu et développé **séparément**, en fonction des besoins spécifiques de ses utilisateurs, et posséder sa propre interface.

La **structure « multi-couches »** de l'Internet rend bien compte de sa capacité à faire communiquer des réseaux entre eux. Le but d'un tel système est en effet de séparer chaque problème en différentes parties (les couches) selon leur niveau d'abstraction : les plus hautes, également les plus proches de l'utilisateur, gèrent les données les plus abstraites en recourant aux services des couches plus basses, qui mettent en forme les données afin qu'elles puissent être émises sur un *médium* physique.

Les « couches » de l'Internet

L'Internet repose sur le modèle TCP/IP, qui correspond à une architecture réseau en couches – trois ou quatre, selon que l'on distingue ou non les couches Internet et transport, dans lesquelles les protocoles de transport TCP et de réseau IP jouent un rôle prédominant. Il s'est progressivement imposé en lieu et place du modèle OSI[1], qui reposait lui sur sept couches ; certaines de ses couches « reprennent » donc plusieurs couches de ce modèle OSI.

Les couches de l'Internet sont :

– La **couche hôte-réseau ou accès-réseau**[2]. Elle doit permettre d'accéder à un réseau physique quel qu'il soit, et de transmettre des données *via* ce réseau. Son implémentation est laissée libre, mais beaucoup de réseaux locaux utilisent Ethernet[3].

– La **couche Internet**. Clé de voûte de l'architecture de l'Internet, elle réalise l'interconnexion des réseaux. Elle doit permettre l'acheminement des paquets de données (ou « datagrammes ») indépendamment les uns des autres jusqu'à destination ; s'ils y arrivent dans le désordre, ils seront réordonnés par les couches supérieures.

[1] *L'OSI (*Open Systems Interconnection*) est un standard de communication en réseau de l'ensemble des systèmes informatiques, qui sera supplanté par la norme TCP/IP.*

[2] *Elle rassemble les couches « physique » et « liaison de données » du modèle OSI.*

[3] *Bien qu'il implémente la couche physique, le protocole Ethernet est traditionnellement classé dans les couches de liaison de données.*

– La **couche transport**, parfois fusionnée avec la couche Internet. Si les deux couches précédentes ont pour objectif d'envoyer des informations d'une machine à l'autre, celle--ci doit permettre à des applications tournant sur des machines distantes de communiquer. Elle possède deux implémentations, dont la plus connue est le protocole TCP[1].

– La **couche application**[2]. Située au sommet, elle contient les applications réseaux permettant de communiquer grâce aux couches inférieures. Ces applications sont pour la plupart des services réseau, c'est-à-dire des applications fournies à l'utilisateur pour assurer l'interface avec le système d'exploitation : services de connexion au réseau ou à distance, services de transfert de fichier, divers utilitaires Internet (échange de courriers électroniques …).

Cette idée d'un tel interréseautage à architecture ouverte a été portée dès l'origine par MM. Robert E. Kahn et Vinton Cerf, co-inventeurs du **protocole TCP/IP**. Ce protocole prit la suite du *Network Control Protocol* (NCP), mis au point au début des années 70 pour le réseau ARPANET, mais qui avait le défaut de suspendre le système si des paquets de données étaient perdus.

Au contraire, le protocole TCP/IP présentait l'avantage de répondre aux besoins d'un environnement de réseau à architecture ouverte. Le premier principe que s'était fixé son concepteur posait l'autosuffisance de chaque sous-réseau et l'absence de changement interne pour le connecter à l'Internet. Comme le souligne l'Internet Society[3], « *un concept clé de l'Internet est qu'il n'a pas été conçu pour une seule application, mais comme une* ***infrastructure générale sur laquelle de nouvelles applications pouvaient être conçues****, comme illustré plus tard par l'émergence du* World Wide Web. *C'est la nature polyvalente du service fourni par le TCP et l'IP qui rend cela possible.* »

Comme le souligne M. Maurice Ronai, le succès de l'Internet tient à des « *propriétés peu communes* » ancrées « *dans la technologie et dans l'architecture du réseau, qui donne aux individus le pouvoir d'émettre des contenus, autant que de les recevoir, et s'assure que leurs messages seront transmis avec la même priorité que ceux des grands groupes internationaux* ». C'est donc la conception même de l'Internet qui a permis, dès l'origine, de garantir son ouverture et son interopérabilité.

Le **principe du « *end to end* »** – ou architecture de « bout en bout » – fait que « *l'intelligence est située à l'extrémité du réseau, et non en son centre, comme avec les réseaux traditionnels* », poursuit Maurice Ronai. Les fonctions de traitement sont assurées « *aux extrémités par les ordinateurs et par les usagers. C'est cette particularité qui a permis à des développeurs, des innovateurs, et des start-ups, de mettre ces technologies à la disposition du public, personne ne pouvant les en empêcher.* »

---

[1] *L'autre étant le protocole UDP.*

[2] *Elle rassemble les couches « session », « présentation » et « application » du modèle OSI.*

[3] *Voir note* supra.

Une telle configuration est par essence vertueuse. Selon M. Bernard Benhamou[1], ancien conseiller de la délégation française au sommet des Nations unies pour la société de l'information (2003-2006) et ancien délégué aux usages de l'Internet (2007-2013), cette particularité a donné la **possibilité « *à des utilisateurs « isolés » de développer des technologies qui par la suite ont été adoptées mondialement* »**, telles que le langage HTML, les systèmes de « pair à pair » (« *peer to peer* ») ou les *weblogs*[2]. Du fait de sa neutralité, le réseau constitue en effet « *une plateforme d'expression commune, un « bien commun » qui permet à l'ensemble des utilisateurs de développer de nouveaux contenus et de nouveaux services* ».

b) Un moteur transversal de progrès dans de nombreux secteurs

L'absence de restriction technique à l'accès à l'Internet a joué un rôle de catalyseur et largement contribué à son succès. Il a également permis des **développements illimités** enregistrés dans des **secteurs connexes à l'origine**, et diffusés aujourd'hui à l'**ensemble de la vie économique et sociale**. « *Ces propriétés – l'ouverture, l'interopérabilité, la neutralité, l'architecture du bout en bout – ont ouvert un champ inouï d'innovations, de circulation des connaissances et de développement des échanges* », conclut ainsi M. Maurice Ronai.

Même analyse de la part de Mme Françoise Massit-Folléa, chercheur et consultant senior sur les usages et la gouvernance de l'Internet, selon laquelle l'Internet constitue « *un **véritable écosystème*** » du fait de ses caractéristiques techniques. « *Le réseau des réseaux supporte, pour une part croissante de la population mondiale, un nombre exponentiel d'activités humaines, économiques, sociales, culturelles, politiques, qui sont favorisées par ce même principe du* « end to end », *une création permanente aux extrémités du réseau* », explique-t-elle : « *celui-ci devient ainsi l'*alpha *et l'*oméga *de la croissance, du développement, voire de toute la vie sociale* ».

Ainsi que l'a rappelé M. Philippe Lemoine devant votre mission, la naissance de l'Internet s'est faite aux États-Unis, dans un contexte utopique et libertaire considérant cette technologie comme un **moyen de pacification et d'émancipation des individus**. Il a ainsi cité les « conférences Macy », qui rassemblaient des chercheurs comme Gregory Bateson, Margaret Mead ou Norbert Wiener, élaborant le concept de cybernétique « *pour aller vers une connaissance pacifiste, en vue d'un monde meilleur – la métaphore du gouvernail indiquant bien qu'il s'agit de s'orienter dans ce monde nouveau en évitant les écueils* »[3].

---

[1] *« Organiser l'architecture de l'Internet », article de M. Bernard Benhamou publié sur Internet à l'adresse : http://www.diplomatie.gouv.fr/fr/IMG/pdf/OrganiserlarchitecturedelInternetBernardBenhamou-2.pdf*

[2] *Ou « blogs » : type de site web utilisé pour la publication régulière d'articles rendant compte d'une actualité ou d'une opinion autour d'un sujet donné.*

[3] *L'icône de Netscape est constituée d'un gouvernail de bateau.*

- **Les apports d'ordre interne**

L'apport sans précédent de l'Internet est d'abord survenu dans ce qui fait sa spécificité : l'échange de données et l'accès à l'information. C'est ainsi qu'est mise au point en 1972 sa **première application fondamentale, le courrier électronique** (ou « *e-mail* »). Cette invention a en effet bouleversé les modes de communication à distance basée sur la lecture, en accélérant la transition du papier vers le numérique. Il s'échange ainsi chaque jour plus de 300 milliards de courriels.

Si le courrier électronique représenta pendant longtemps l'application majeure de l'Internet, la **deuxième invention de rupture qui le supplanta fut l'invention du *World Wide Web***. Élaboré par Tim Berners-Lee et Robert Cailliau au sein du CERN, il représente aujourd'hui le principal support d'utilisation de l'Internet, pour des centaines de millions d'utilisateurs à travers la planète : on compterait aujourd'hui plus de 1 000 milliards de pages Web dans le monde pour plus de 600 millions de sites consultables.

Le *World Wide Web*, principale application de l'Internet

Le ***World Wide Web*** (WWW, communément appelé « Web », et parfois « la Toile »), est un système hypertexte public fonctionnant sur l'Internet et permettant de consulter, au moyen d'un navigateur, des pages comportant diverses ressources (textes, images, sons, vidéos …).

S'il est souvent confondu avec l'Internet, le Web n'en est en réalité qu'une des applications, certes la plus usitée. Il se distingue ainsi d'autres applications comme le courrier électronique, la messagerie instantanée ou le partage de fichiers en pair à pair (« *peer to peer* »).

L'**HTTP** (*HyperText Transfer Protocol*) est le nom du protocole de communication généralement utilisé pour échanger ou transférer les ressources du Web. Un navigateur Web (« *browser* ») est un logiciel HTTP permettant à un utilisateur d'accéder auxdites ressources.

L'**URL** (*Uniform Ressource Locator*) est une chaîne de caractères décrivant la localisation d'une ressource sur le Web. L'hyperlien – également inventé par Tim Berners-Lee – est un élément de type URL présent dans une ressource et renvoyant vers une autre ressource.

Le **HTML** (*HyperText Markup Language*) est le langage informatique le plus courant pour décrire le contenu d'un document (titre, paragraphe, intégration de photos …) et inclure des hyperliens.

Un **site Web** est un ensemble de pages Web contenant des ressources publiées par un propriétaire et hébergées sur un serveur Web. Le moteur de recherche est une application Web permettant de trier les sites Web en fonction de mots-clefs.

- **Les apports d'ordre externe**

Au-delà de ces applications intrinsèques à l'Internet, cette technologie – et l'ensemble de celles relevant du numérique, plus largement –, par son caractère neutre et transversal, s'est diffusée dans

chacun des aspects de la vie économique et sociale contemporaine, jusqu'à la bouleverser entièrement. Il n'y a plus aujourd'hui de champ d'activité qui soit soustrait à une « révolution numérique » qui « dévore le monde », pour paraphraser l'expression de Marc Andreessen, cofondateur de Netscape[1].

Cette invasion est, en majeure partie, source de progrès et d'émancipation pour des millions d'individus, dans des secteurs d'activité aussi nombreux que variés. Nous nous limiterons à trois exemples sectoriels particulièrement illustratifs du caractère global de cette « révolution digitale ».

Dans le **domaine de la santé**, tout d'abord, l'Internet est en passe de révolutionner la relation patient-médecin, mais également les pratiques médicales elles-mêmes. Au premier titre, se développe l'**auto-information** des particuliers sur leur état de santé et les diverses pathologies pouvant les affecter : 60 % des Français se tournent ainsi vers l'Internet pour obtenir des renseignements médicaux ou établir un premier diagnostic[2]. Du côté des praticiens, près d'un tiers d'entre eux se connecte en consultation pour prescrire, en interrogeant prioritairement les bases de données et interactions médicamenteuses.

Au second titre, on assiste à une généralisation des objets connectés équipés de capteurs permettant de mieux connaître l'évolution physiologique d'un individu. Cette transition vers la« **m-santé** » à travers le « ***quantified self*** » (l'auto-mesure) étend chaque jour ses supports : tensiomètre, balance, *pacemaker*, et même fourchette ou brosse à dents connectés ! Elle ne se limite pas à la livraison d'informations, mais peut aller jusqu'à la réalisation de soins ou à l'intervention médicale à distance. Une entreprise française a ainsi mis au point un timbre numérique permettant d'administrer jusqu'à sept médicaments simultanément ou de façon séquentielle. Programmable par des professionnels de la santé, cette innovation pourrait révolutionner la façon de soigner, notamment la maladie d'Alzheimer.

L'impact de l'Internet dans le **domaine de l'éducation** est tout aussi spectaculaire et prometteur. L'usage du réseau permet en effet une **démocratisation de l'accès à la connaissance**, par la consultation des articles, encyclopédies, bibliothèques numériques publiques (Gallica) ou privées (Google Books), forums de discussion spécialisés… Ainsi que le souligne le rapport du Commissariat général à la stratégie et à la prospective sur l'Internet à l'horizon 2030[3], « *le web est devenu une archive vivante : 23 millions d'articles sur Wikipedia dans près de 300 langues, réactualisés en*

[1] « Software is eating the world », *c'est-à-dire* « le logiciel dévore le monde », *est exactement l'expression qui lui est attribuée.*

[2] « *La santé s'impose sur Internet et les réseaux sociaux* », *article du* Figaro *du 28 novembre 2012.*

[3] La dynamique d'Internet, prospective 2030, *rapport du Commissariat général à la stratégie et à la prospective, étude 2013, n° 1.*

permanence, 20 millions d'ouvrages numérisés sur Google Books, des millions d'informations nouvelles publiées chaque jour en mode flux… ».

L'**approche de l'enseignement** se trouve par ailleurs elle-même remise en cause. L'enseignant ne s'adresse plus à ses seuls élèves physiquement présents, mais potentiellement à chaque individu s'intéressant à son champ d'intervention. Les « **MOOCs** » (*Massive Open Online Courses*, ou cours en lignes ouverts et massifs), qu'a promus le lancement en janvier dernier de la plateforme France université numérique (FUN), sont ainsi en passe de devenir un mode d'apprentissage à part entière.

Si les grandes universités ont depuis longtemps ouvert certains de leurs cours par leur diffusion en ligne (ou *podcast*), la Khan Academy, organisation à but non lucratif qui se donne pour mission « *d'offrir une éducation gratuite et de première classe pour tous, partout* », est allée plus loin en proposant des espaces numériques d'apprentissage par le jeu et la vidéo. C'est le domaine des « jeux sérieux » (ou ***serious games***), dont l'une des applications les plus intéressantes concerne le champ pédagogique, à travers les « jeux éducatifs » (ou *edugames*), auxquels il peut être recouru dans tout type de formation et à tout âge.

Enfin, dernier exemple de secteur dans lequel le numérique est source de progrès : la **recherche d'une croissance durable**. Si la moindre consommation de ressources physiques que permet la numérisation des contenus se trouve contrebalancée par l'accroissement des dépenses énergétiques qu'elle implique, la valeur ajoutée qu'apportent les systèmes d'intégration connectés – tels que les « réseaux électriques intelligents » (ou ***smart grids***) pour l'énergie – laisse augurer d'importants gisements d'économie de ressources rares, ainsi que le développement de ressources circulaires ou renouvelables.

Les technologie de ces « réseaux intelligents », particulièrement prometteuses en termes de durabilité, devraient à terme permettre d'optimiser la consommation d'énergie, de réduire les émissions de CO_2 et de stimuler le développement de nouveaux usages, comme le véhicule électrique. Au cours des dix dernières années, plus de 5 milliards d'euros ont été investis dans environ 300 projets concernant ces types de réseaux en Europe. Les compteurs intelligents, qui en constituent la première brique, devraient équiper 80 % de la population européenne d'ici 2020, et générer un marché de 40 à 50 milliards d'euros d'ici ce même horizon[1].

c) Le risque de dérives vers des systèmes fermés et centralisés

- **La fermeture des équipements, systèmes d'exploitation et applications**

Le caractère originairement ouvert et décentralisé de l'Internet s'est vu progressivement contrarié par des tentatives de fermeture et de

[1] Le marché des *smart grids* en France et en Europe, *étude réalisée par Eurostaf, décembre 2012*.

concentration, provenant des grands acteurs privés du secteur. L'usage de l'Internet *via* les équipements mobiles (*smartphones*, tablettes…) en donne un exemple particulièrement éclairant.

L'offre est en effet partagée aujourd'hui entre **deux grands systèmes d'exploitation, iOS (Apple) et Androïd (Google)**, qui se partagent plus de 95 % du marché[1]. Chaque terminal est pré-équipé de l'un de ces systèmes, selon les accords passés entre les constructeurs et ces entreprises éditrices de logiciels, sachant que certaines de ces dernières sont également constructeurs (c'est le cas notamment d'Apple avec ses iPhones). Or, cette **« surcouche » de logiciel d'exploitation** conditionne grandement les choix de l'utilisateur, qui devra rester dans « l'univers » de l'éditeur pour tirer toutes les possibilités de son équipement.

Cet « emprisonnement » de l'usage dans un système d'exploitation dit « propriétaire » se retrouve au niveau de **l'interface** et des **fonctionnalités de base** de l'appareil, mais surtout au niveau des « **applications** » (ou « applis ») qu'il permet d'enregistrer et d'utiliser. Ces « applis » sont en effet téléchargeables depuis des « **plateformes** » de téléchargement créées et exploitées par les éditeurs de logiciels : iTunes pour les produits équipés d'iOS et Androïd Market pour ceux équipés d'Androïd. Ainsi, le possesseur d'un *smartphone* ou d'une tablette qui « tourne » sur iOS ne peut télécharger ses « applis » que sur iTunes, et celui utilisant Androïd ne le peut de son côté que sur Androïd Market[2].

Il y a là une **logique de « silo »** (tel téléphone, équipé de tel système d'exploitation, et permettant d'accéder – uniquement – à telle plateforme de téléchargement) qui **nuit à la fluidité du marché et restreint la liberté de choix** des consommateurs. Ceux-ci n'ont en effet d'autre alternative que de choisir l'application apparentée à leur « univers logiciel » ; or, elle peut être moins performante ou plus chère que l'application liée au système d'exploitation concurrent, voire ne pas exister du tout. D'autre part, l'utilisateur perd l'usage de toutes les applications qu'il avait téléchargées le jour où il change de téléphone et en acquiert un muni du système concurrent.

Ce cloisonnement des équipements et des usages a été initié par les deux principaux éditeurs, Apple et Google, qui « verrouillent » ainsi le marché des applications mobiles et découragent leurs clients de se tourner vers des offres alternatives. Les **enjeux financiers sont colossaux** : le cabinet Gartner a estimé à près de 26 milliards de dollars le chiffre d'affaires généré en 2013 par les 102 milliards de téléchargements enregistrés. Un chiffre

---

[1] *Existent des systèmes d'exploitation concurrents – tels que Windows Phone (Windows), Bada (Samsung), BlackBerry OS (RIM), Symbian OS (Symbian)… – mais leurs parts de marché sont marginales par rapports aux deux principaux.*

[2] *Existent d'autres plateformes de téléchargement concurrentes, rattachées aux systèmes d'exploitation alternatifs précités, mais là encore, la diversité des choix qu'elles permettent et leur audience les confinent à un rôle anecdotique.*

d'affaires appelé à augmenter avec le développement massif des achats intégrés depuis l'application (ou *in-app purchases* – IAP), invite l'utilisateur d'une application gratuite à l'enrichir de nouveaux contenus ou services payants.

Ce modèle d'architecture fermée des appareils, des systèmes d'exploitation et des applications a, historiquement, été poussé par **Apple**, qui a toujours **cumulé les trois fonctions** de constructeur de terminaux, éditeur de systèmes logiciels et éditeur d'applications. Le projet de Steve Jobs, le dirigeant charismatique du groupe, jusqu'à sa mort en 2011, a toujours été « d'emprisonner » l'utilisateur dans un écosystème privé où, à terme, tout contenu deviendrait payant, ou dont la gratuité serait financée par le visionnage obligatoire de publicités de sa régie.

L'un des principaux acteurs et inventeurs de l'Internet, **Sir Tim Berners-Lee, s'est montré particulièrement inquiet de ces dérives**. Lors de la conférence mondiale du Web qui s'est tenue à Lyon en avril 2012, il s'est dit préoccupé par l'évolution des applications mobiles, un marché selon lui cloisonné par les fabricants de matériel et éditeurs de logiciels. « *Le Web, ce sont des standards, et chaque internaute doit pouvoir accéder au même contenu* », a rappelé Tim Berners-Lee lors de cette conférence, avant de vanter les **mérites du HTML5,** langage de programmation qui évite d'avoir à réécrire une application pour chaque système et permet donc de diminuer les coûts de développement de ces applications.

Mais cette évolution, qui concerne le web et les applications auxquelles il permet d'accéder, est en réalité beaucoup plus large et s'avère caractéristique d'une **reconfiguration de l'univers du net**. Ainsi que le soulignait le magazine en ligne spécialisé Wired en 2010[1], « *aujourd'hui, le contenu que vous voyez dans votre navigateur […] compte pour moins d'un quart du trafic sur Internet... et ça baisse. Les applications qui comptent davantage dans le trafic Internet incluent les transferts de fichiers P2P, la messagerie électronique, les réseaux privés virtuels (*Virtual Private Network - *VPN), les communications entre interfaces de programmation (*Application Programming Interface – *API), les appels Skype, World of Warcraft et les autres jeux en ligne, le Xbox Live, iTunes, la voix sur IP, iChat et la diffusion en* streaming *de films depuis Netflix…* ***La plupart des nouvelles applications du net sont des réseaux fermés, souvent propriétaires.*** »

- **La gestion intégralement centralisée de la racine du net**

Plus généralement encore, c'est l'**architecture même de l'Internet qui peut être considérée comme fermée**, ou du moins centralisée, sous influence américaine. Elle s'enracine dans la création, en 1982, par une équipe de San Francisco, de la première version du ***Domain Name System*** (DNS), ensemble de fichiers interconnectés qui remplit la fonction

[1] *Cité dans « Le créateur du web critique les applications mobiles fermées », article de* Numerama *du 19 avril 2012.*

d'annuaire. Or, c'est l'***Internet Corporation for Assigned Names and Numbers*** (ICANN), société de droit californien à but non lucratif, mais dont les liens avec le département d'État américain au commerce sont connus[1], qui en a depuis 1998 la gestion. Par ailleurs, la société américaine **VeriSign** est opérateur de la racine A[2], qui sert pour la mise à jour de toutes les racines de l'annuaire[3].

Il en résulte, s'inquiète M. Louis Pouzin[4], que « ***les États-Unis gèrent donc l'ensemble de l'annuaire****, même s'il est physiquement réparti dans tous les pays du monde* ». Reconnaissant que le DNS est devenu indispensable, l'ingénieur français fait toutefois observer que « *sa structure centralisée n'a rien d'indispensable* ».

Prenant l'exemple du téléphone mobile, et des 1 500 ou 2 000 opérateurs qui s'interrogent entre eux de par le monde « *grâce à un système de numérotation plus intelligent que l'Internet, basé sur un code pays et un code opérateur* » et sur la gestion par chaque opérateur de l'interconnexion de son propre annuaire, il estime ce modèle applicable à l'Internet. « *Mais les États-Unis ont* ***conçu le système de manière à ce que les États ne puissent pas intervenir dans sa gestion*** », note-t-il.

Cette hyper centralisation de la structure du net, au-delà des critiques politiques qu'elle peut alimenter, est **porteuse de réels dangers pour la sécurité du réseau**. « *Tout point de passage obligé induit une fragilité, c'est un fait. Avec son annuaire unique, Internet est un terrain plus propice aux attaques malveillantes* », souligne M. Louis Pouzin. « *Elles sont rarement de grande ampleur. Mais le risque est là. C'est la conséquence de l'absence de cloisonnements et donc de pare-feux.* » Surtout, cette centralisation induite par le système des noms de domaine déroge à la nature de l'Internet, conçu comme ouvert, décentralisé et distribué.

La solution, qui passerait par une **maîtrise du DNS au niveau national**, est toutefois **difficilement envisageable à court terme**. Elle susciterait en effet une forte hostilité des États-Unis, et ceci à plusieurs égards. La première réticence est d'ordre **sociologique** : « *les Américains estiment que l'Internet leur appartient. Toucher au DNS, c'est toucher à leur pré carré* », prévient M. Louis Pouzin. La deuxième raison de cette hostilité est **politique** : « *le DNS, ainsi conçu, est un excellent moyen d'observation. Il est évidemment impossible d'observer tout ce qui se passe. Mais par échantillonnage, il est possible d'examiner plus précisément le trafic de tel ou tel utilisateur. C'est un outil d'intelligence économique. Il n'y a pas de preuve formelle qu'il est aujourd'hui utilisé à cette fin. Mais un pays qui aurait une telle capacité et ne s'en servirait pas*

---

[1] *Voir* infra, *sur ce sujet, les développements consacrés à la question de l'indépendance de l'ICANN.*

[2] *La racine est la partie de l'annuaire qui se trouve au sommet de la hiérarchie. Elle contient uniquement les principales extensions : .com, .eu, .fr, .uk …*

[3] *Il existe de par le monde 280 copies de l'unique racine du DNS, mises à jour automatiquement par VeriSign.*

[4] *Interview de M. Louis Pouzin pour le Club Parlementaire du Numérique par* Armel Forest.

serait bien fou. » Enfin, restent « *les raisons* ***économiques*** *et l'usage commercial possible des flux dont VeriSign garde la trace* » ainsi qu'un « *volet corporatiste très lourd dans la mesure où la carrière de très nombreuses personnes, souvent compétentes, est liée à la continuité de ce système* ».

Mis à part la Chine, qui a créé son propre DNS, en 2003, les **initiatives nationales visant à briser ce « cadenassement » de l'Internet sont encore embryonnaires**. On peut néanmoins citer les États du Golfe, qui ont mis en place une sorte « d'Intranet arabe », ou encore la Russie, dont la volonté d'indépendance en la matière peine toutefois à se réaliser. Pour ce qui est de l'Europe, où l'usage de l'Internet et du DNS sous contrôle américain est ultra-majoritaire, seul un mouvement de grande ampleur soutenu par les institutions étatiques et communautaires permettrait de développer progressivement des DNS nationaux interconnectés.

3. Une innovation de rupture offrant à chacun le pouvoir d'agir

L'invention et la diffusion de l'Internet à travers la planète a profondément modifié les grands équilibres économiques, le modèle d'organisation de nos sociétés, nos modes de vie et jusqu'à notre rapport au monde. Plus qu'une simple révolution industrielle, le numérique emporte un véritable bouleversement philosophique qui interroge la dimension anthropologique de l'homme.

a) Une technologie de rupture à part entière

En ce sens, et pour le seul champ économique, l'Internet peut être qualifié de « technologie de rupture » (*disruptive technology*), selon le sens qu'en donne Clayton Christensen dans son ouvrage *The Innovator's Dilemma*, publié en 1997. Il s'agit bien d'une **innovation fondamentale** ayant pour particularité de **rompre avec le modèle existant** et de conduire à une **modification radicale du paysage économique**. L'Internet compte d'ailleurs les deux-tiers des douze technologies de rupture listées par Mac Kinsey dans son rapport de 2013 sur les technologies de rupture qui vont modifier le monde en 2025[1].

La dématérialisation des données, l'augmentation exponentielle des capacités de stockage et la possibilité de les transmettre de façon instantanée en s'affranchissant des contraintes physiques ont en effet **remis en question les modèles classiques**, ceux de la « vieille économie », et rebattu les cartes dans tous les secteurs d'activité économique.

Comme l'a fait observer à votre mission M. Pierre Bellanger, fondateur et président directeur-général de la radio Skyrock, auteur de

[1] Disruptive technologies: Advances that will transform life, business, and the global economy, *rapport McKinsey, mai 2013*.

***La Souveraineté numérique*[1], l'automobile** est sans doute **l'exemple le plus illustratif** de cette évolution dans le **secteur industriel**. Elle sera demain connectée et pourvue d'un système d'exploitation, devenant en elle-même un simple « terminal » dont la valeur résidera moins dans la qualité du châssis ou du moteur, que dans celle du « résogiciel » qui l'anime (les « résogiciels » désignant pour M. Bellanger les grands réseaux de services en ligne). La connexion de l'ensemble des GPS en temps réel permettra de connaître la circulation de façon prédictive et de gagner de la fluidité. L'étape suivante sera celle de la conduite automatisée, sur laquelle travaillent déjà de nombreuses entreprises, de l'industrie automobile comme de l'Internet. Le rapprochement entre ces deux mondes, autrefois étrangers, a déjà commencé, Nissan ayant par exemple signé un accord avec Google, tandis que certaines voitures sont équipées du logiciel Carplay d'Apple.

Outre l'industrie, **les services sont également touchés**, comme dans **la banque et l'assurance**. La possession de données personnelles permettra aux grandes plateformes Internet de personnaliser leur offre de crédit ou d'assurance à l'extrême, et donc d'emporter un avantage concurrentiel par rapport aux banques ou compagnies d'assurance classiques, qui ne connaîtront pas aussi bien le comportement de leurs clients. En réalité, ce sont l'ensemble des services « classiques » qui sont potentiellement affectés par ce changement de modèle : la santé, l'éducation, les loisirs…

Lors de son audition devant votre mission, M. Vinton Cerf a montré comment la conception même de l'Internet, en **permettant aux développeurs de générer de nouvelles applications sans demander la permission** des fournisseurs d'accès, a représenté « *une innovation au regard de la permission et a facilité le développement des connaissances et des pratiques commerciales* ».

Cette rupture technologique entraîne, dans la sphère économique, des changements de perspective importants. Elle **redistribue le pouvoir de concevoir et d'innover au profit de la base**. D'une économie de l'offre, on basculerait ainsi vers une économie où la demande créerait elle-même sa propre offre et d'une économie de la production à une économie où la valeur ajoutée est dans la distribution. Cela est rendu possible par la **personnalisation des produits à distance**, grâce à des spécifications fournies par le consommateur et permettant d'adapter un modèle de base à ses besoins ou à ses préférences.

Le stade ultérieur consiste pour le consommateur à concevoir, mais également à **fabriquer lui-même le produit** qu'il désire. Le développement des ***Fabrication laboratorys*** (ou *FabLabs*), concept défini en 2004 au sein du MIT, va dans ce sens. Plateformes ouvertes de création d'objets physiques équipées par des machines à commande numérique de niveau professionnel, telles qu'une imprimante 3D, une machine à sérigraphie ou une presse à circuits imprimés, elles permettent de créer rapidement des produits

[1] La souveraineté numérique, *Pierre Bellanger, Ed. Stock, 2014.*

personnalisés en série limitée, avant éventuellement de les commercialiser à une plus grande échelle[1].

b) L'instrument d'une révolution politique et philosophique

La « révolution Internet » va en réalité au-delà de cette redéfinition des hiérarchies économiques, qui redonne l'avantage aux structures légères et innovantes par rapport aux grands ensembles installés. Elle constitue en effet une **rupture politique et philosophique**, dans la mesure où elle réinvente entièrement le rapport à la connaissance, et redistribue de façon horizontale le « pouvoir d'agir ».

M. Michel Serres a longuement développé devant la mission les soubassements de cette révolution, qui trouve son origine dans la **modification contemporaine du « *couple support-message* »**, ainsi qu'il l'a décrit dans son ouvrage *Petite Poucette*. L'humanité en serait à la troisième phase d'évolution de ce couple, celle qui rendrait possible l'avènement d'une démocratie véritable « *du fait de l'indépendance de l'individu par rapport à l'information* ».

La première de ces trois ruptures se serait située lors du **passage de l'oralité à l'écrit**, qui a produit « *un véritable miracle d'externalisation, par l'objectivation du support* » : au corps humain (plus exactement, à la parole qu'il permet) se sont alors substitués des supports externes tels que la peau, le parchemin et le papier, matérialisant et mettant à distance la parole.

La deuxième rupture daterait de l'**invention de l'imprimerie**, à la Renaissance. La possibilité de lire « *renouvelle l'idée même de démocratie, de lien avec les autorités* », politiques comme religieuses. « *La cognition, la pédagogie, la science changent […]. Le spectre des changements se reproduit, aussi large que celui qu'avait produit l'apparition de l'écriture.* »

Enfin, l'**Internet** constitue donc « *un troisième état de cette affaire, une réplique* ». Il se matérialise dans le « *téléphone-ordinateur* », qui est le « *dernier avatar du couple support-message que l'humanité connaît depuis ses origines* ». La révolution numérique passe toute entière, selon le sociologue, par cette alliance de matériaux et de logiciels qui permet à sa Petite Poucette, par sa seule main, et plus précisément encore par son seul pouce, d'attraire à elle, instantanément et sans bouger, le monde tout entier.

Saisissant cet appareil hybride et connecté, sa Petite Poucette « ***tient trois choses** : les **lieux** du monde – grâce à son GPS, à Google Earth –, les **informations** du monde – qui sont en plus stockées dans une mémoire colossale, lui donnant un souvenir immédiat, maintenant –, et elle tient encore les **personnes** du*

[1] *Les pouvoirs publics ont aujourd'hui pris conscience de l'intérêt social, mais aussi économique, de ces* FabLabs. *Les nombreux espaces publics numériques (EPN) ouverts depuis la fin des années 90 se reconvertissent progressivement en* FabLabs. *Fin juin 2013, le Gouvernement a lancé un appel à projets d'aide au développement d'ateliers de fabrication numérique qui visait notamment ces EPN. Ainsi, il est prévu qu'un fonds finance une dizaine de projets à hauteur de 50 000 à 200 000 euros chacun.*

monde […]. Petite Poucette a donc cette devise : « main-tenant, tenant en main le monde. »

Il y a là un **renversement complet de la relation de l'être aux autres et au monde**. Alors que cette « *faculté de tenir le monde en main n'a jamais appartenu qu'à quelques personnes seulement dans l'histoire du monde* », ce sont aujourd'hui « *3,75 milliards de Petite Poucette qui tiennent en main le monde* ». À l'approche descendante classique (dite aussi *top-down*), voulant que les possesseurs de l'autorité et de la connaissance déversent les pouvoirs et les savoirs aux étages inférieurs de la pyramide sociale, se substitue une approche sinon ascendante (*bottom-up*), du moins **horizontale**, où chaque individu est source d'initiative ou d'information qu'il peut partager avec ses semblables, voire faire remonter vers les sommets de la hiérarchie sociale.

Si cette révolution est globalement source de progrès et d'émancipation, elle n'en implique pas moins une **reconfiguration des rapports interindividuels**, insiste M. Michel Serres. Les **élèves et étudiants**, à l'encontre desquels les maîtres et professeurs nourrissaient une « *présomption d'incompétence* », se voient reconnaître une « *présomption de compétence* », dès lors qu'ils peuvent consulter le thème du cours sur l'Internet. Les **relations intrafamiliales** sont également bouleversées, car « *si la science est ce que les parents enseignent à leurs enfants, la technologie est ce que les enfants enseignent à leurs parents* ». Les rapports entre **patients et médecins** sont aussi à réviser, Petite Poucette tenant en main « *tous les chiffres, alors qu'ils étaient hier encore l'apanage des seuls experts* ».

Ce renversement de point de vue, outre sa dimension philosophique et anthropologique, a un **impact politique**, en ce qu'il **redéfinit les relations de pouvoir et d'autorité**. L'Internet représente ainsi, pour M. Michel Serres, « *la révolution qui rend possible un changement de la gouvernance du monde : c'est Internet qui va redéfinir le système politique, et non l'inverse* ». Selon lui, le changement opéré est si radical qu'il « *exige de penser de nouvelles formes politiques, une nouvelle démocratie* » : c'est « *cet état des choses qui fait advenir une véritable utopie démocratique, unique dans l'histoire de l'humanité* ».

À un XIXème siècle prolifique en matière d'invention de systèmes politiques, a succédé un XXème siècle particulièrement pauvre en ce domaine. « *Voilà ce qui nous manque aujourd'hui alors que le monde a changé si vite* », estime M. Michel Serres. Il existerait ainsi un **décalage entre ce monde nouveau**, façonné par l'Internet et reposant sur des relations interindividuelles, égalitaires et ignorant les frontières, **et une organisation politique et institutionnelle** reposant sur une conception ancienne du monde, basée sur l'autorité et la hiérarchie. À terme, le changement de gouvernance de l'Internet doit donc évoluer vers une modification de la gouvernance du monde elle-même.

B. L'INTERNET, UN INSTRUMENT DE PUISSANCE QUI ÉCHAPPE À L'EUROPE

Or, dans ce changement en cours, le rôle et la place de l'Union européenne apparaissent singulièrement faibles. L'Internet redessine une cartographie du monde qui échappe à l'Europe, menacée de devenir une « *colonie du monde numérique* » comme l'avait déjà avancé votre rapporteure en mars 2013, dans un précédent rapport[1].

1. L'Internet comme prolongement de la puissance par le droit et l'économie : un enjeu bien identifié par les États-Unis et la Chine

L'omniprésence des États-Unis dans l'Internet n'est pas le fruit du hasard, mais d'une stratégie de long terme mise en place sciemment par ses grands acteurs publics, privés et militaires. Là où l'Europe ne saisissait pas sa chance pour occuper une place centrale dans le développement du réseau, les États-Unis allaient s'emparer d'une technologie dont ils entendaient faire le « cheval de Troie » de leurs valeurs et de leurs intérêts sur l'ensemble de la planète.

Très tôt, dès le début des années 90, avant même la généralisation de l'Internet et du *World Wide Web*, les États-Unis ont adopté des dispositions législatives et fiscales tendant à créer un réseau de transfert de données à travers tout le territoire américain pour améliorer la compétitivité et acquérir une position de *leadership* dans le domaine des technologies de l'information. Dans la décennie suivante, la seconde puissance du numérique à se constituer ne fut pas l'Europe mais la Chine qui s'est bâti un écosystème d'entreprises numériques parmi les plus importantes, à l'égal des GAFA.

a) Les autoroutes de l'information comme la continuation du leadership *économique et politique américain dans un espace ouvert et mondialisé*

Le Sénateur Al Gore est à l'origine du *Bill High-Performance Computing Act* de 1991 visant à créer un programme fédéral assurant la pérennité du *leadership* des États-Unis en matière d'informatique de haute performance[2]. Celui-ci ouvrait un financement de 1,75 milliard de dollars sur trois ans pour construire un réseau de communication de données capable de relier toutes les universités américaines et les centres de calculs.

---

[1] L'Union européenne, colonie du monde numérique ?, *rapport d'information de Mme Catherine Morin-Desailly, fait au nom de la commission des affaires européennes du Sénat (n° 443, 2012-2013) - 20 mars 2013 – http://intranet.senat.fr/notice-rapport/2012/r12-443-notice.html*

[2] Bill High-Performance Computing Act of 1991 to provide for a coordinated Federal program to ensure continued United States leadership in high-performance computing.

Ce programme permit de supplanter l'ancien réseau universitaire d'ordinateurs ARPANET et de diffuser l'Internet tel que nous le connaissons aujourd'hui, fonctionnant sur la base du protocole TCP/IP.

Le discours du Président Georges Bush prononcé lors de la signature du *Gore Bill* situe cette volonté de redéploiement de l'effort industriel vers les nouvelles technologies dans une stratégie globale du gouvernement, de l'industrie et du milieu universitaire pour développer l'emploi et la croissance économique par ces technologies, dont le potentiel transformateur est bien identifié[1].

Discours de George Bush du 9 décembre 1991

« *Le développement de l'informatique de haute performance et des technologies de l'information offre la possibilité de transformer radicalement la façon dont les Américains travailleront, apprendront et communiqueront à l'avenir. Il porte en lui la promesse de changer la société au même titre que les grandes inventions du vingtième siècle, telles que le téléphone, le voyage en avion, la radio et la télévision.*

"*Ce programme aidera les chercheurs à répondre aux grands défis de la science pour percer les secrets de l'ADN, prévoir les phénomènes météorologiques violents et découvrir de nouveaux matériaux supraconducteurs.*

"*Il n'est pas surprenant que l'Amérique soit* leader *dans le domaine des hautes technologies. Nos plus grands progrès ont été rendus possibles par l'exceptionnelle capacité de la société américaine à promouvoir la liberté, l'innovation et l'esprit d'entreprise dans une cohérence que l'on ne trouve nulle part ailleurs dans le monde. Ce programme soutiendra et étendra notre* leadership.

"*L'initiative que nous lançons pour le développement des hautes technologies de l'information fait partie d'une stratégie globale de l'administration pour améliorer notre compétitivité. Ma proposition d'affecter un milliard de dollars au budget de cette année induira des investissements accrus dans la recherche fondamentale et dans de nouveaux domaines clés de la recherche appliquée, qu'il s'agisse de la science des matériaux, des processus de fabrication avancés, de biotechnologie et de R&D dans le domaine de l'énergie.*

"*En plus de ces investissements essentiels dans la R&D, nous avons travaillé à l'amélioration de la compétitivité de notre pays dans le siècle à venir face à la concurrence, en obtenant l'ouverture des marchés étrangers aux exportations des États-Unis grâce à un nouveau cycle du GATT et un accord nord-américain de libre-échange. Ce succès provient également de nos propositions en matière de politique fiscale, telles que le crédit d'impôt permanent en R&D et la réduction des impôts sur les gains en capital pour promouvoir l'investissement à long terme. Nous renforçons également nos capacités productives en augmentant fortement le financement de l'enseignement des sciences et des mathématiques dans le cadre de la réforme « Amérique 2000 ».*

"*L'initiative met en œuvre huit agences fédérales, toutes susceptibles de contribuer au développement des nouvelles technologies et des bénéfices issus des progrès scientifiques. Le secteur privé travaillera en étroite collaboration avec les organismes fédéraux et les laboratoires dans la planification, le financement et la gestion de cette*

[1] *George Bush, « Remarks on Signing the High-Performance Computing Act of 1991 » (9 décembre 1991).*

initiative pour faire en sorte que ce programme de recherche porte rapidement ses fruits dans le commerce comme dans l'éducation.

"Notre initiative de développement des technologies de l'information les plus avancées est un excellent exemple de la philosophie qui guide notre administration pour investir dans l'avenir, créer de nouveaux emplois et offrir de nouvelles opportunités de croissance économique soutenue. Elle est également un excellent exemple de la façon dont le gouvernement, l'industrie et le milieu universitaire peuvent travailler ensemble pour développer des technologies nouvelles et déterminantes. »

M. Bernard Stiegler compare l'émergence de la puissance américaine en ce domaine à celle de la création de l'industrie cinématographique : « *L'histoire des deux décennies suivantes a des points communs avec celle du début du XXème siècle qui a vu les États-Unis asseoir sur le cinéma leur hégémonie mondiale, grâce à Hollywood. Le premier studio ouvre à Hollywood en 1912, alors qu'il n'y avait quasiment rien dans ce quartier de Los Angeles ; ce studio n'était peut-être qu'une baraque en bois, mais le Congrès américain n'en débattait pas moins du cinéma et de son importance pour l'économie américaine :* « Trade follows films », *a déclaré un sénateur dans ce débat, Jean-Luc Godard fait cette citation dans son histoire du cinéma. En fait, l'économie américaine s'est organisée pour solvabiliser l'industrie du cinéma, pour asseoir sa puissance – et en retour, par ce* soft power, *conforter la puissance américaine elle-même.* »

Alors qu'en 1993, les technologies du web sont versées dans le domaine public par le CERN, où elles ont été mises au point à grand renfort de subventions publiques, **Al Gore**, vice-président américain de l'époque, commande un **rapport sur les « autoroutes de l'information » et sur l'opportunité d'une politique de soutien** massif au numérique. « *Lisez ce rapport […] : vous y verrez clairement décrite la voie qu'ont suivie depuis les États-Unis pour faire du web une invention américaine au service du développement américain* », a insisté M. Bernard Stiegler.

Ainsi, a-t-il poursuivi, « *nombre d'innovations viennent d'Europe ou d'Asie, mais c'est aux États-Unis qu'elles trouvent leur développement, parce que le gouvernement américain met tout en œuvre pour qu'elles s'y épanouissent. Le CERN est européen, la France est l'un de ses principaux soutiens, mais le web est devenu américain ; le mode de transfert asynchrone (ATM), qui permet de transférer simultanément sur une même ligne des données et de la voix, a été inventé à Issy-les-Moulineaux, au Centre national d'études des télécommunications (CNET), mais il a trouvé outre-Atlantique son application industrielle.* »

Ainsi, l'économie américaine s'est organisée pour solvabiliser ces industries naissantes afin d'asseoir ses intérêts et, en retour, conforter la puissance américaine elle-même. M. Bernard Stiegler identifie la nouvelle inflexion que représente ce passage **du *soft power* au *smart power***, paradoxalement nourri par « *l'intelligence européenne et asiatique* »[1].

[1] *Cette puissance douce et dématérialisée, développée à l'origine par le professeur américain Joseph Nye dans la sphère des relations internationales, a été théorisée par les dirigeants américains – à commencer par le président des États-Unis – comme un instrument de « maîtrise complète du*

Mais contrairement à l'ère prénumérique, où ce *soft power* était en grande partie entre les mains des médias traditionnels et de l'industrie culturelle, ainsi que l'a fait remarquer Valérie Peugeot, vice-présidente du Conseil national du numérique, il **tend aujourd'hui à se disséminer** : « *tout un chacun peut aujourd'hui, sous condition d'équipement et d'accès au réseau, façonner les créations et les savoirs mondiaux, en écrivant, publiant, partageant, faisant circuler, produisant des contenus, des informations, des données* ».

La volonté politique américaine a été renforcée par une politique fiscale incitative au développement du commerce électronique mise en œuvre en 1998 avec l'adoption de l'*Internet Tax Freedom Act* qui prohibe la création de taxes discriminatoires sur le commerce électronique[1]. Concrètement, cette loi a instauré un moratoire à partir du 1er octobre 1998 sur toute création de taxes par les États ou les subdivisions territoriales sur l'accès à l'Internet et le commerce électronique[2].

Vingt ans après, le succès de cette stratégie ne paraît pas discutable : sur les 50 premières entreprises de médias numériques, 36 sont américaines, avec Google en tête, talonné par une entreprise chinoise.

Classement 2012 des 50 premières entreprises de médias numériques

PLACE	NOM DE L'ENTREPRISE	SECTEUR	CHIFFRE D'AFFAIRES EN DOLLARS	PAYS
1	Google	Recherche	36.4 Mrd	États-Unis
2	China Mobile	Télécom	7.58 Mrd	Chine
3	Bloomberg	Informations	7 Mrd	États-Unis
4	Reed Elsevier	Informations	5.93 Mrd	UE-Grande-Bretagne
5	Apple	Divers	5.4 Mrd	États-Unis
6	Yahoo	Divers	4.99 Mrd	États-Unis
7	WPP	Publicité	4.71 Mrd	UE-Grande-Bretagne
8	Thomson Reuters	Informations	4.71 Mrd	Canada
9	Tencent	Divers	4.46 Mrd	Chine
10	Microsoft	Divers	3.93 Mrd	États-Unis
11	Facebook	Réseaux sociaux	3.68 Mrd	États-Unis
12	Sony	Divers	3.38 Mrd	Japon
13	Pearson	Informations	3.14 Mrd	UE-Grande-Bretagne
14	Dentsu	Publicité	2.9 Mrd	Japon

monde ». Elle a pris le relai du hard power, *littéralement le « pouvoir dur », basé sur la contrainte (« le bâton ») et l'incitation (« la carotte »).*

[1] *Public law 105-227 (21 octobre 1998).*

[2] "No State or political subdivision thereof shall impose any of the following taxes during the period beginning on October 1, 1998, and ending 3 years after the date of the enactment of this Act—

(1) taxes on Internet access, unless such tax was generally imposed and actually enforced prior to October 1, 1998; and

(2) multiple or discriminatory taxes on electronic commerce."

PLACE	NOM DE L'ENTREPRISE	SECTEUR	CHIFFRE D'AFFAIRES EN DOLLARS	PAYS
15	Omnicom Group	Publicité	2.78 Mrd	États-Unis
16	China Telecom	Telecom	2.65 Mrd	Chine
17	Baidu	Recherche	2.3 Mrd	Chine
18	Publicis Groupe	Publicité	2.19 Mrd	UE-France
19	Netflix	Video	2.01 Mrd	États-Unis
20	News Corp	Divers	1.9 Mrd	États-Unis
21	Amazon	Livres	1.85 Mrd	États-Unis
22	Naspers	Divers	1.82 Mrd	Afrique du Sud
23	Dun&Bradstreet	Informations	1.76 Mrd	États-Unis
24	Groupon	Publicité	1.61 Mrd	États-Unis
25	Activision Blizzard	Jeux	1.56 Mrd	États-Unis
26	Comcast	Broadcast	1.5 Mrd	États-Unis
27	Time Warner	Divers	1.5 Mrd	États-Unis
28	Hearst	Divers	1.5 Mrd	États-Unis
29	Wolters Kluwer	Informations	1.47 Mrd	UE-Pays-Bas
30	AOL	Divers	1.4 Mrd	États-Unis
31	Universal Music Group	Musique	1.39 Mrd	États-Unis
32	IAC	Divers	1.34 Mrd	États-Unis
33	Axel Springer	Divers	1.22 Mrd	UE-Allemagne
34	Cox Enterprises	Divers	1.2 Mrd	États-Unis
35	CBS	Broadcast	1.2 Mrd	États-Unis
36	Netease	Divers	1.19 Mrd	Chine
37	Zynga	Jeux	1.14 Mrd	États-Unis
38	Gannett	Journal	1.1 Mrd	États-Unis
39	Electronic Arts	Jeux	1.07 Mrd	États-Unis
40	Monster Worldwide	Publicité	1.04 Mrd	États-Unis
41	Walt Disney	Divers	1 Mrd	États-Unis
42	Viacom	Broadcast	1 Mrd	États-Unis
43	DMGT	Journal	997.24M	UE-Grande-Bretagne
44	YP Holdings	Publicité	990M	États-Unis
45	EMI	Musique	903.16M	UE-Grande-Bretagne
46	Shanda Jeux	Jeux	838.3M	Chine
47	Informa	Informations	805.37M	UE-Grande-Bretagne
48	Warner Music	Musique	768M	États-Unis
49	Yell Group	Annuaire	722.84M	UE-Grande-Bretagne
50	Hakuhodo DY	Publicité	719.22M	Japon

Source : GIGAOM - paidContent 50 :
The world's most successful digital media companies (2012)

b) La Chine et la Russie, également dans des stratégies de puissance

Le premier opérateur de télécommunication au monde est chinois. Avec 7,59 milliards de dollars de chiffre d'affaires, China Mobile se classe en

deuxième position, derrière Google. Dans les dix premiers, Tencent, le service de messagerie le plus populaire en Chine se classe neuvième.

Ce poids particulier de la **Chine** dans l'économie Internet devrait aller croissant, car pour l'instant seulement 40 % des 1,3 milliard de Chinois sont connectés. En tous cas, elle fait déjà de la Chine un acteur majeur du web :

– le moteur de recherche Baidu a vu sa capitalisation boursière décupler depuis son introduction à Wall Street en 2005 ;

– la valorisation du site marchand Alibaba est estimée à près de 100 milliards d'euros[1], soit un montant équivalent à celui d'Amazon.

La Chine, deuxième puissance mondiale du net
(M. Stéphane Grumbach, directeur de recherche à l'Institut national de recherche en informatique et en automatique (INRIA))

« Les années 2000 sont celles de l'émergence du Web 2.0, des réseaux sociaux, et des autres systèmes coopératifs. Les États-Unis ont été véritablement des précurseurs dans le développement des grands systèmes reposant sur des investissements massifs. Ils sont à l'origine de toutes les grandes plateformes qui dominent aujourd'hui l'Internet. Mais ils ne sont pas tout à fait seuls. La Chine a su développer ses propres plateformes, avec un décalage de seulement un ou deux ans sur leurs consœurs américaines.

« Aujourd'hui parmi les 50 premiers systèmes mondiaux, Google, Facebook, Youtube, Yahoo, Baidu, Wikipédia, QQ, Taobao, ..., on compte 36 Américains, 11 Chinois et 3 Russes. Aucun Européen. Et parmi les huit premiers que j'ai cités, trois Chinois.

« Pendant les années 2000, la construction de l'Internet chinois est passée totalement inaperçue en Europe. Nous nous sommes focalisés sur les questions de contrôle policier et de censure, sans voir que la Chine rentrait dans la société de l'information avec le même engouement et la même maîtrise que les Américains.

« La Chine dispose de systèmes qui gèrent des centaines de millions d'utilisateurs. Le pays est grand, mais l'argument n'est pas essentiel, l'Inde ne dispose pas de tels systèmes. Le pays est partiellement fermé, mais partiellement seulement. La Chine ne bloquerait pas les grands systèmes américains comme Facebook, qu'elle aurait quand même développé de grands systèmes qui domineraient son marché. La Corée, complétement ouverte, a développé ses propres systèmes également.

« Ce qui est déterminant pour l'émergence des plateformes du net, c'est la volonté politique. Elle est aussi forte aux États-Unis qu'elle l'est en Chine. Elle fait clairement défaut en Europe. Les sociétés chinoises du net, cotées au Nasdaq, ressemblent d'ailleurs beaucoup à leurs homologues américaines. Les chercheurs qui travaillent dans les laboratoires de R&D des grands groupes chinois sont les mêmes que ceux qui travaillent chez Google ou Facebook. Ils ont le même esprit, le même engouement passionné pour la révolution numérique. Pour ce qui est de l'organisation, elle ne diverge pas beaucoup. Baidu est une société enregistrée aux Îles Caïman.

« L'exemple de la Chine est intéressant, car il montre que des systèmes politiques aussi différents que ceux de la Chine et des États-Unis réussissent à développer les piliers fondamentaux de cette industrie qui nous échappent à nous Européens. La Russie ainsi que d'autres pays d'Asie y parviennent également. Leurs gouvernements ont compris tout le profit qu'ils pouvaient tirer du numérique. Ils ont aussi compris que personne n'arrêterait la

[1] *Source : http://www.reuters.fr/article/technologyNews/idFRPAEA1B03W20140212*

révolution numérique et qu'il fallait donc l'orienter dans un sens favorable pour leur développement. »

Source : audition du 11 février 2014

Ainsi, selon M. Stéphane Grumbach, la Chine récolte 20 fois moins de données que les États-Unis mais 80 fois plus que la France.

La **Russie** a également émergé sur la scène numérique internationale, devenant à partir de 2011 le pays d'Europe comptant le plus d'utilisateurs de l'Internet, avec 50,9 millions de visiteurs uniques en ligne, devant l'Allemagne (50,1), la France (42,3) et le Royaume-Uni (37,2)[1], notamment en raison d'une forte appétence des internautes russes pour les réseaux sociaux. Cette caractéristique peut être liée à l'immensité du territoire et au contrôle des médias par l'État, faisant de l'Internet un moyen privilégié de communication et donnant naissance à de nouveaux géants de l'Internet :

– le réseau social VKontakte, créé en 2007, rassemble 23,4 millions d'utilisateurs actifs et surpasse très largement Facebook qui ne fédère en Russie qu'une dizaine de millions d'utilisateurs ;

– le moteur de recherche Yandex, coté au Nasdaq, a été créé en 1997 quelques mois avant Google et possède une position dominante sur le marché russe comme dans les pays de l'ex-URSS, avec une part de marché de 60 % contre 25 % pour Google[2]. En 2013, Yandex s'est classé en quatrième position des moteurs de recherche les plus consultés dans le monde avec 2,8 % de part de marché, derrière Google (65,2 %), Baidu (8,2 %) et Yahoo (4,9 %), mais devant Bing de Microsoft (2,5 %).

Il faut noter que cet écosystème s'est développé à partir de la prise de conscience du passage de l'an 2000 et du défi numérique qu'il a suscité. Un programme fédéral « e-Russia 2002-2010 » a été lancé en s'appuyant sur une communauté technique et scientifique russophone et le développement des réseaux et de la téléphonie mobile.

Ainsi, les grandes puissances du monde contemporain misent-elles sur l'Internet pour conforter leur stratégie de puissance. L'Union européenne a-t-elle une semblable ambition de puissance ?

c) Une domination commerciale consacrée par la prévalence du droit américain

Les souverainetés des États se trouvent imbriquées entre elles dans le cyberespace. Néanmoins, certains États y sont plus souverains que d'autres : ainsi, les États-Unis détiennent deux leviers importants pour étendre leur souveraineté juridique de par le monde.

---

[1] *Source : http://www.inaglobal.fr/numerique/article/la-russie-face-au-defi-des-nouvelles-technologies*

[2] *Source : http://www.latribune.fr/technos-medias/Internet/20130116trib000742919/le-russe-yandex-bat-google-sur-son-propre-terrain.html*

D'une part, de nombreuses extensions de noms de domaine ressortent des juridictions américaines ; il en est ainsi notamment du « .com ». En 2011, un département du *Homeland Security* américain chargé des infractions à la propriété intellectuelle a pu saisir les noms de domaine du site de rediffusion de matchs sportifs *Rojadirecta.com*, pourtant reconnu légal par la justice espagnole, du fait que ces noms de domaine avaient été acquis auprès d'un *registrar* établi aux États-Unis. Un site Internet espagnol peut ainsi être suspendu par les autorités américaines.

D'autre part, la plupart des grands acteurs du net sont américains et ressortent à ce titre des juridictions américaines.

Qu'il s'agisse de Google, Apple, Facebook, Amazon – les fameux GAFA – mais aussi de Yahoo, Youtube, Tweeter, iTunes..., l'utilisation de la plupart des services proposés par ces opérateurs requiert une inscription et l'acceptation de conditions générales d'utilisations (CGU), dénommées *terms of services* ou *terms of acceptance* sur les sites anglophones. À l'instar des clauses figurant dans les contrats d'adhésion (location de véhicule, ouverture d'un compte en banque, …), il est demandé au client internaute d'accepter les conditions proposées sans possibilité de négociation. Sur ces plateformes de services, l'absence d'agrément des clauses conduit au refus automatique du service.

La question des CGU n'est pas anodine dans l'économie numérique, par nature mondialisée et dématérialisée, car le cocontractant fournisseur de service n'est dans de nombreux cas pas établi dans le pays de résidence du consommateur. Cette situation pose la problématique de la juridiction territorialement compétente en cas de litige ; le fait que le siège de Google soit situé à Cupertino en Californie n'est donc pas sans conséquence pour un client résidant dans le Gers ou n'importe où ailleurs hors du territoire américain.

Qu'observe-t-on à la lecture des CGU ? Par défaut, les principales plateformes de services, notamment les GAFA ainsi que Twitter, prévoient que les actions judiciaires engagées contre les conditions contractuelles sont régies par les lois de l'État de Californie des États-Unis d'Amérique sans considération et sans faire application des dispositions légales de votre État ou de votre pays de résidence relatives aux conflits de lois. La question de savoir si ce type de clause d'attribution de compétence, défavorable au consommateur européen, pouvait, d'une part, être considéré comme une clause abusive, d'autre part, être contourné pour rendre possible la saisine d'une juridiction de laquelle ressort la résidence du client, revêt une importance considérable quant à l'effectivité des recours.

Interrogé sur ce point, M. Laurent Cytermann, rapporteur général adjoint de la section du rapport et des études du Conseil d'État, s'est attaché à battre en brèche les idées fausses en matière contractuelle, la prédominance de la volonté des parties n'étant pas sans limite : « *les règlements européens Bruxelles I et Rome I empêchent une entreprise de priver un consommateur de la*

protection de sa législation nationale. La cour d'appel de Pau, dans un arrêt Sébastien R. contre Facebook, estimant que les clauses de Facebook n'étaient pas claires et que, dès lors, le consentement de l'internaute n'était pas valable, s'est reconnue compétente et a écarté la compétence de la justice américaine. Le règlement Bruxelles I bis, qui remplacera en janvier 2015 Bruxelles I, élargit le régime, puisqu'il s'appliquera aux consommateurs, même si l'entreprise est située hors de l'Union européenne[1]. » Il faut donc en conclure que les clauses d'attribution exclusives de compétence à une juridiction située hors de l'Union européenne peuvent être écartées par le juge national, qui se reconnaît alors compétent dans certaines hypothèses.

De même, le juge national peut également décider de sanctions, comme l'illustre, en matière pénale, le cas des enchères d'objets nazis : ainsi que le rapporte M. Laurent Cytermann, « *Yahoo, qui avait été condamnée par la justice française, a été déboutée par la justice américaine qui a explicitement reconnu la compétence de la justice française pour prononcer des sanctions* ».

Ceci tempère la domination américaine par le droit qui reste néanmoins très large dans le cyberespace.

2. L'hypercentralisation de l'Internet autour de géants qui défient les États

a) Une concentration croissante de l'Internet autour de grands acteurs privés

Le rapport de la mission d'expertise sur la fiscalité de l'économie numérique, dit « Collin et Colin » du nom de ses auteurs[2], a mis en lumière le constat que « *l'économie numérique n'est pas un secteur de l'économie. Elle est un vecteur de transformation de tous les secteurs de l'économie, dans lesquels elle provoque de puissants déplacements de marges des entreprises traditionnelles vers les entreprises opérant des services logiciels de réseau*. »

---

[1] *Règlement (UE) n° 1215/2012 du Parlement européen et du Conseil du 12 décembre 2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale (refonte) :*
« … (14) De manière générale, le défendeur non domicilié dans un État membre devrait être soumis aux règles de compétence nationales applicables sur le territoire de l'État membre de la juridiction saisie.
Article 18. – L'action intentée par un consommateur contre l'autre partie au contrat peut être portée soit devant les juridictions de l'État membre sur le territoire duquel est domiciliée cette partie, soit, quel que soit le domicile de l'autre partie, devant la juridiction du lieu où le consommateur est domicilié. »

[2] *Le rapport de la mission d'expertise sur la fiscalité de l'économie numérique remis en janvier 2013 au ministre de l'économie et des finances, au ministre du redressement productif, au ministre délégué chargé du budget et à la ministre déléguée chargée des petites et moyennes entreprises, de l'innovation et de l'économie numérique et établi par MM. Pierre Collin, conseiller d'État, et Nicolas Colin, inspecteur des finances, est disponible en suivant le lien :*
http://www.economie.gouv.fr/files/rapport-fiscalite-du-numerique_2013.pdf.

Cette transformation de l'économie fait apparaître de puissants acteurs, ce qui déroge aux principes fondateurs de l'Internet. Selon les mots de M. Maurice Ronai devant votre mission, « *l'Internet a été originellement conçu comme un réseau décentralisé, dans lequel chaque ordinateur est son propre serveur, dans une architecte pair-à-pair. Assez rapidement, cet Internet historique a vu émerger des plateformes centralisées, autour desquelles les usagers se sont progressivement agrégés. Ces plateformes centralisées ont progressivement entrepris de développer leurs activités dans des secteurs jusqu'alors séparés de l'Internet, comme le mobile. Ceci constitue un changement majeur dans la dynamique du réseau, ces géants ayant reconstitué, au-dessus de l'Internet décentralisé, ou à côté, dans l'univers des mobiles, de véritables empires privés.* »

L'effet de réseau alimente en effet la croissance des acteurs en ligne : plus un réseau social ou un moteur de recherche est utilisé, plus il devient attirant. M. Pierre Bellanger a expliqué ce phénomène par la loi dite « de Metcalfe » : « *la « loi de Metcalfe » établit que la valeur d'un réseau est proportionnelle au carré du nombre de machines qu'il connecte ; supposez que vous ayez dix machines connectées et que vous en ajoutiez une onzième : la valeur de votre réseau passe de 10² à 11², de 100 à 121, soit +21 % de croissance de valeur pour une seule machine supplémentaire connectée. Sachant que dans le monde, plusieurs millions de nouvelles machines rejoignent chaque jour Internet, le réseau vit sous une loi de d'accélération continue, une exponentielle.* »

Ainsi, celui qui s'impose sur un marché le gagne complètement : comme l'a résumé M. Stéphane Grumbach devant votre mission, nous sommes « *dans une économie du* « winner takes all », *le gagnant récolte toute la mise* ». On comprend dès lors l'ambition universelle d'un Google (« *organiser les informations à l'échelle mondiale* ») ou d'un Facebook (« *connecter le monde* »).

Se distinguant en cela des États-Unis ou de la Chine**, l'Europe se caractérise par une concentration particulièrement forte autour de tels services en ligne, notamment sur le marché de la recherche en ligne, largement dominé par Google** (près de 93 % de parts de marché) devant Bing (2,5 %), Yandex et Yahoo (environ 1 %)[1].

Une fois acquise la position dominante sur un marché, les acteurs du net diversifient leurs activités ; ainsi, à partir d'une activité de moteur de recherche, Google poursuit une stratégie de diversification, devenant régie publicitaire, cartographe, fabricant de téléphone, de voiture, de lunettes connectées, commerçant et bientôt câblo-opérateur, … Dernièrement, Google a fait l'acquisition de sociétés produisant des lentilles de contact connectées pour mesurer le taux de glycémie pour les diabétiques ou du matériel de domotique afin de contrôler un nombre croissant de données de l'internaute-cible de publicité.

[1] *Sur le marché américain, Google occupe une part de marché de moins de 70 %, devant Bing (18 %) et Yahoo (11 %) ; en Chine, le leader des moteurs de recherche Baidu (80 %) devance trois autres concurrents : 360 (10 %), Sougou (5 %) et Google (4 %).*

D'autres entreprises se sont transformées en étendant très largement leur cœur de métier, Apple en contrôlant et monétisant tout l'univers applicatif nécessaire à l'utilisation de ses matériels (ordinateurs, *smartphones*, tablettes) et Amazon en créant une chaîne logistique globale qui dépasse très largement le cadre de la vente et livraison de livres puisque sa prochaine frontière concerne les produits frais et la livraison personnalisée par drones, tout en devenant un grand fournisseur des services de *cloud*.

L'intégration de volumes de données sans précédent dans les hautes technologies est au cœur des services toujours plus performants proposés par les géants du net. Incontestablement, selon l'expression des auteurs Collin et Colin, « *l'économie numérique obéit à des logiques radicalement différentes de celles des Trente glorieuses* » :

– par une accélération du rythme de l'innovation ;

– par la mobilisation d'investissements massifs ;

– par la mise en réseau d'écosystèmes entiers englobants sur différents marchés connexes ;

– par un modèle de réinvestissement des bénéfices plutôt que de redistribution de dividendes ;

– par le changement permanent et la rapidité des mutations, rendant difficilement opérant les dispositifs juridiques et fiscaux de régulation ;

– enfin, par le découplage systématique du lieu d'établissement du lieu de consommation, ne permettant pas de localiser précisément la valeur créée.

Le géographe et chercheur au sein du laboratoire Chôros de l'École polytechnique fédérale de Lausanne (Epfl), M. Boris Beaude, entendu par votre mission d'information, qualifie d'« hyper-centralité » ce phénomène où quelques acteurs peuvent concentrer du pouvoir quasiment à l'infini, sans être limités par des problèmes physiques tels que les limites territoriales et les règles locales. En effet, **la connexité ne se heurte pas aux mêmes contraintes physiques que la contiguïté**.

b) Des acteurs privés en passe de défier les États

L'Internet représente en lui-même un défi aux États, dans la mesure où il participe à leur perte de maîtrise de leur territoire. La loi nationale peine à s'appliquer sur cet espace transnational et les frontières y deviennent poreuses. Pour reprendre les exemples cités par Mme Pauline Türk, maître de conférences en droit public à l'université de Lille II, lors de son audition par votre mission, on peut évoquer le sort de la loi française sur la non diffusion des sondages le jour des élections, les tentatives de réglementation des jeux en ligne, l'impossibilité de lutter efficacement contre la divulgation sur l'Internet de données secret-défense, ou encore l'incapacité à circonscrire

l'influence de la communauté internationale dans les soulèvements populaires dans les pays du « printemps arabe ».

Au-delà de ce défi global que représente l'Internet pour les États, ce sont les géants du net qui concentrent une force nouvelle et provocante pour les États.

Ainsi, le fait qu'une grande partie de cette économie de l'Internet soit basée sur la gratuité de l'utilisation des services – ceux-ci étant financés par la publicité – a amené l'économiste **Paul Krugman à avancer l'idée que certaines plateformes devaient être considérées comme de quasi services publics**.

De fait, l'usage gratuit des moteurs de recherche, l'accès à une documentation, à la connaissance et à des capacités de stockage et de calcul en constante progression font de l'Internet un concurrent pour de nombreux services publics qu'il s'agisse de l'éducation, de la sécurité ou de la santé. Les moteurs de recherche proposent une alternative à de nombreux services d'intérêts généraux réglementés par exemple en matière de transport de personnes ou de presse d'information.

Mais c'est surtout en pratiquant à grande échelle l'optimisation fiscale que les géants du net défient les États. Si l'optimisation fiscale se distingue de la fraude ou de l'évasion fiscale dans le sens où elle n'enfreint pas les règles de droit mais fait un usage légitime de l'environnement juridique qui lui est le plus favorable, la structuration territoriale des grands groupes obéit à des schémas très complexes qui reflètent et alimentent, ainsi que le démontre le rapport « Collin et Colin », une concurrence fiscale intense entre États. Votre rapporteure a déjà détaillé, dans son précédent rapport déjà cité[1], les caractéristiques de l'économie numérique – modèles d'affaires évolutifs, modèle dominant de la gratuité, large part d'actifs incorporels, découplage entre lieu d'établissement et lieu de consommation – qui lui permettent de tirer aisément parti de cette concurrence fiscale, à laquelle se livrent même les États membres de l'Union européenne.

En outre, le modèle d'affaires dominant de l'économie numérique est celui de l'intermédiation. Qu'elle intervienne entre professionnels et particuliers ou entre particuliers, cette intermédiation capte la marge au détriment des acteurs traditionnels. L'intermédiaire acquiert en effet un pouvoir de marché qui force la baisse des prix au profit du consommateur, mais au détriment des bénéfices des entreprises : à mesure que la place de marché numérique devient incontournable, il devient indispensable pour tout fournisseur d'y être référencé, ce qui accroît l'intensité concurrentielle.

---

[1] *Cf. p.34-39* – L'Union européenne, colonie du monde numérique ?, *rapport d'information de Mme Catherine Morin-Desailly, fait au nom de la commission des affaires européennes du Sénat (n° 443, 2012-2013) - 20 mars 2013 – http://intranet.senat.fr/notice-rapport/2012/r12-443-notice.html*

Ceci bouleverse les modèles économiques et transforme radicalement des secteurs entiers de l'économie, qu'il s'agisse de la confrontation d'Amazon face aux libraires, des sites de voyage face aux agences de voyage, iTunes face aux disquaires, ou encore Tripadvisor face aux guides touristiques.

Le cas qui oppose aux taxis la plateforme Uber de mise en relation avec les véhicules de tourisme avec chauffeur (VTC) illustre cette redéfinition complète d'un secteur professionnel. Les manifestations de taxis, de San Francisco à Paris en passant par Londres, montrent qu'une innovation peut à elle seule bouleverser sur le plan mondial le modèle économique d'une profession réglementée.

Les fournisseurs traditionnels voient donc leur taux de marge diminué tandis que l'intermédiaire ayant acquis un pouvoir de marché peut facturer plus cher sa prestation d'apport d'affaires et capte ainsi une part croissante de la marge. Cette dynamique tend donc à diminuer la base fiscale imposable des États, qui repose sur les bénéfices des entreprises « traditionnelles » et peine à inclure l'économie en ligne.

Ce faisant, les géants de l'Internet privent les États de recettes fiscales, ce qui sape les moyens de l'action publique et, plus globalement, les fondements du modèle social européen.

C'est même le modèle culturel qui se trouve menacé, dès lors que la construction de l'information en ligne obéit à une logique quantitative, au détriment des contenus peu rentables qui n'attirent pas la publicité.

Enfin, l'une des attributions centrales de la souveraineté, l'émission monétaire, est également concurrencée par la création de monnaies virtuelles dont la plus connue est le *Bitcoin*. En France, ces monnaies ne font l'objet d'aucune définition légale spécifique et la Banque de France comme l'Autorité de contrôle prudentiel et de résolution (ACPR) les considèrent comme des services de paiement[1]. Les monnaies virtuelles ne sont pas soumises à l'impôt, que ce soit au titre des transactions, au titre de la détention ou au titre des plus-values. Au niveau international, certains États se sont préoccupés de ce phénomène à l'occasion de la faillite d'une série de plateformes. Entre neutralité bienveillante au Canada et arrestation en Chine du gérant de la plateforme Bitcoin GL opérée à Hong Kong provoquant une perte de 4,5 millions d'euros pour les utilisateurs du système, l'encadrement juridique demeure très variable selon les pays.

La monnaie virtuelle est avant tout une technologie créée en 2008 et mise en activité en janvier 2009, fonctionnant en réseau sur la base d'un protocole technique de transactions sur l'Internet complétement décentralisé, pair-à-pair (*peer-to-peer*) et *open source*. En France, le cœur du réseau est le

[1] *Soumis à la directive 2007/64/CE du Parlement européen et du Conseil du 13 novembre 2007 concernant les services de paiement dans le marché intérieur.*

Bitcoin central géré par la société Paymium. Celle-ci fonctionne comme une place de marché sur laquelle des acheteurs et des vendeurs peuvent acquérir ou vendre des *bitcoins* contre des euros, ou inversement. Cette unité de compte circule ensuite sur le réseau. Le défi majeur de ce moyen de paiement demeure la sécurité. Pour les autorités de régulation, le *Bitcoin* reste encore un système parallèle au monopole de fait de la monnaie légale, qui est émise par les autorités centrales. À terme, avec le développement de ce nouveau service qui demeure encore hautement spéculatif (+ 900 % par rapport à sa valeur en euro depuis sa création), se pose la question de son encadrement légal, dans ses aspects financiers et criminels[1].

À la croisée des libertés publiques et des enjeux économiques, la confrontation peut directement opposer un opérateur de l'Internet à un État : Twitter en Turquie. Ainsi le gouvernement turc, estimant que la souveraineté et l'intérêt national transcende les intérêts commerciaux, estime légitime de bloquer certains sites Internet et de leur demander d'installer une représentation dans le pays qu'ils opèrent. Devant cette situation, Twitter a fait le choix de ne pas s'installer afin de ne pas s'exposer à la législation turque. Il est intéressant de noter qu'une entreprise étrangère défie directement le gouvernement de l'État dans lequel elle propose ses services en adressant un *tweet* à ses utilisateurs turcs contenant une procédure de contournement des mesures de blocage[2].

Ces stratégies de défiance indirecte ou directe à l'égard des États peuvent s'avérer à double tranchant car le modèle économique des services numériques repose sur la confiance des clients et donc sur la bonne réputation des opérateurs. Or en matière fiscale comme de protection des données, les pratiques des GAFA appellent un encadrement à l'échelle européenne et mondiale.

3. L'Europe, largement distancée dans cette redistribution des pouvoirs

- **Une Europe objectivement « à la traîne » dans le secteur du numérique**

Le constat a été fait à de nombreuses reprises devant la mission : malgré un riche passé et de nombreux atouts dans le secteur des TIC,

[1] « Une enquête du *Federal Bureau of Investigation (FBI)* a été engagée contre des fournisseurs de plateforme de conversion soupçonnés de blanchiment d'argent et de fraude fiscale. Le 2 octobre 2013, les autorités américaines ont ainsi fermé le site Internet « Silk Road » – site d'acquisition de produits narcotiques en ligne – sur lequel s'échangeait une importante partie des *bitcoins* en circulation » *(Source : table ronde de la commission des finances du Sénat du 15 janvier 2014 sur les enjeux liés au développement des monnaies virtuelles de type* bitcoin*).*

[2] *Source : Wall Street Journal 2 mai 2014.*

l'Europe est aujourd'hui dépassée par ses concurrents, américains et asiatiques notamment.

Hervé Collignon, associé d'A. T. Kearney, co-auteur d'une étude de février 2014 sur le secteur de la haute technologie en Europe, en a fait une synthèse préoccupante devant votre mission. Hors télécoms et Internet, ce marché est évalué à 2 700 milliards de dollars, dont un quart en Europe. Or, a-t-il souligné, « *la place des acteurs européens sur ce marché est faible et en recul* ».

Ainsi, seuls **8 groupes européens** (après la cession de Nokia[1]) figurent désormais **dans le classement**, basé sur les revenus, **des 100 premiers groupes high-tech** dans le monde, contre 12 il y a deux ans. Plus précisément, l'Europe est absente dans des secteurs aussi essentiels que les composants électroniques, l'électronique grand public, les ordinateurs portables, *smartphones* et tablettes, segments largement dominés par les géants asiatiques et américains.

L'étude d'A. T. Kearney reconnaît que l'Europe occupe, en revanche, **quelques belles positions**, avec ses équipementiers télécom Ericsson, Nokia Siemens[2] et Alcatel Lucent, respectivement deuxième, quatrième et cinquième au classement mondial du secteur, ou ses sociétés de services informatiques Cap Gemini, Atos et T-Systems, respectivement huitième, dixième et douzième, ou bien encore avec un acteur du logiciel comme SAP, quatrième au classement, ou STMicroelectronics, septième du secteur des semi-conducteurs. Cependant, relève l'étude, si la gestion des infrastructures, ainsi que la fourniture et la maintenance des réseaux, sont en partie opérées par des compagnies européennes, elles ne disposent pas pour autant d'un *leadership* dans leur domaine.

Plus récemment encore, dans son nouveau **tableau de bord numérique**, publié le 5 juin dernier, la **Commission européenne** a clairement relevé que l'Union, dans son ensemble, demeurait en retard par rapport au Japon et aux États-Unis. Les dernières statistiques disponibles montrent en effet que, pour l'année 2012, seulement 6,6 % du total des **aides publiques à la Recherche et Développement (R&D)** (soit 6 milliards d'euros) des différents États membres vont, en moyenne, aux technologies de l'information et de la communication (TIC), contre 9,1 % au Japon et 7,9 % aux États-Unis. Ces chiffres illustrent la nécessité de redoubler d'efforts pour réaliser les objectifs fixés par la stratégie numérique pour l'Europe, à savoir atteindre, d'ici 2020, 11 milliards d'euros de dépenses publiques totales de R&D dans le domaine des TIC.

---

[1] *L'équipementier finlandais Nokia a cédé en avril dernier sa division téléphones portables et tablettes à l'Américain Microsoft, pour se concentrer sur les activités de services et de construction de matériels pour opérateurs de réseaux.*

[2] *En 2006, Nokia et Siemens ont fusionné leurs activités d'équipements pour réseaux télécoms dans une coentreprise, baptisée Nokia Siemens Networks.*

L'Union européenne consacre, de son côté, 16 % de son budget de recherche aux TIC : environ 13 milliards d'euros au titre du nouveau programme de recherche Horizon 2020 (2014-2020) iront ainsi à des projets dans le domaine des TIC sur une période de sept ans.

Giacomo Luchetta, chercheur au *Centre for European policy studies* (CEPS) de Bruxelles, a également pointé devant votre mission les carences européennes dans le domaine des TIC et de l'Internet. L'Europe, a-t-il observé, ne compte **que deux entreprises d'envergure spécialisées dans les applications Internet** : Spotify, site de musique en ligne, et Rovio, à l'origine du célèbre jeu *Angry birds. « Et voilà tout ! Nous n'avons pas ni réseaux sociaux, ni messageries instantanées, ni logiciels de bureaux… Certes, il y a Skype, qui a été initialement créé en Estonie par des ingénieurs danois et suédois avec des capitaux d'origine britannique et qui a été enregistré au Luxembourg ! Mais cette belle réussite européenne a dû passer sous giron nord-américain pour devenir un géant de l'Internet, suite à sa première vente à Ebay en 2007 puis à son acquisition par Microsoft en 2011. Il faut ainsi faire appel aux capitaux américains pour devenir un géant de l'Internet et c'est véritablement une lacune pour l'Europe de ne pas disposer d'un opérateur de taille critique* ! »

Un très récent rapport de l'institut américain ITIF[1], examinant la croissance de la productivité en Europe, montre bien comment cette dernière (excepté la seule Irlande, à certaines périodes) « décroche » par rapport à celle des États-Unis au milieu des années 90. En cause, selon le rapport, l'insuffisante intégration des TIC dans l'ensemble de notre modèle économique. Or, ces technologies ont représenté les deux-tiers des facteurs de productivité américains entre 1995 et 2004, et expliquent un tiers de la croissance américaine depuis cette date.

- **Des facteurs explicatifs de divers ordres, notamment culturel**

Le rapport McKinsey pointe divers facteurs explicatifs à ce retard : la **faiblesse de la croissance sur notre continent**, aggravée par l'**absence de préférence domestique des donneurs d'ordre européens** vis-à-vis de leurs fournisseurs, contrairement aux pratiques qui ont lieu outre-Atlantique ; la **complexité du marché européen**, divisé en sous-marchés nationaux délicats à investir, là où le marché américain est plus homogène ; la **faiblesse du financement des entreprises**, avec un marché du capital-risque s'élevant à 4 milliards d'euros en Europe en 2012, contre 20 aux États-Unis, ainsi que la moindre dépense des pouvoirs publics en matière de TIC ; l'**insuffisant développement de notre R&D**, à laquelle nous consacrons 1 point de PIB de moins qu'aux États-Unis et 1,5 de moins qu'au Japon ; la **faiblesse relative de nos diplômés en sciences dures**, qui représentent 17 % des étudiants européens, contre 30 % à Taiwan ou en Chine ; l'**importance de nos coûts de production**, quatre fois supérieurs à ceux de l'Europe de l'Est, et quinze fois

[1] Raising European productivity growth through ICT, *rapport de l'Information Technology & Innovation Foundation (ITIF), 2 juin 2014.*

supérieurs à ceux de la Chine ; l'**absence de collaborations stratégiques entre entreprises**, telles que celles liant Ericsson et Telia ou Alcatel et France Telecom dans les années 80 ; ou encore les ***« virages technologiques mal négociés par l'industrie européenne »***, tel Nokia ratant les révolutions du tactile et du logiciel embarqué, et laissant le champ libre à Apple et Samsung.

Selon le rapport de l'ITIF, le **manque d'investissement du « Vieux continent » dans les TIC s'expliquerait par plusieurs facteurs** : une règlementation de la production et du travail trop contraignante pour les entreprises ; une pression fiscale excessive, notamment sur la consommation ; une capacité limitée des marchés européens à atteindre des économies d'échelle, du fait de leur fragmentation interne ; et l'absence de techniques de management permettant d'exploiter pleinement le potentiel des TIC.

Au-delà de ces facteurs objectifs, il semblerait que des **explications d'ordre culturel**, telles qu'une réticence spontanée aux évolutions technologiques et aux bouleversements socio-économiques qu'ils entraînent, ainsi qu'une frilosité générale des pouvoirs publics et des particuliers vis-à-vis de l'entreprenariat, ne doivent pas être écartées. Stéphane Grumbach a pointé ces limites de façon détaillée. « *Focalisée sur la peur obsessionnelle du mauvais usage qu'une société peut faire des données personnelles et des atteintes à l'individu, l'Europe n'a pas anticipé ni même compris les changements en cours dans le monde, non seulement aux États-Unis, mais également dans les autres pays, acteurs de la révolution numérique* », a-t-il ainsi observé. « *Même si une certaine prise de conscience se fait jour, il me semble que le biais perdure. L'Europe est paralysée et cherche surtout le moyen de stopper l'inondation, l'invasion, par tout moyen, aussi dérisoire et inefficace soit-il.* »

Résultat : une **quasi absence de l'Europe parmi les grands systèmes de plateforme qui dominent l'Internet aujourd'hui**. Et à cette carence dans le secteur des *pure players*, s'ajoute un retard déjà conséquent dans l'ensemble des secteurs de l'économie réelle liés, de plus ou moins près, à l'Internet. L'exemple déjà évoqué des taxis, concurrencés par des sociétés de véhicules de tourisme avec chauffeur dont l'offre est disponible sur des plateformes en ligne, telles qu'Uber, est particulièrement éclairant à cet égard.

Dans une société contrainte à être plus économe, à cause tant des difficultés financières actuelles que des enjeux environnementaux de plus long terme, de tels **systèmes d'intermédiation entre l'offre et la demande offrent un immense potentiel**. Ils permettront par exemple de renforcer les politiques de la ville, les efforts de réduction de CO_2 et les mesures d'amélioration tant du cadre de vie que de son efficacité.

Cependant, notre pays, où « *numérique rime avec panique* », selon M. Stéphane Grumbach, a **déjà adopté une position défensive face à ces systèmes qu'il appréhende comme des menaces**. Selon un article du *Monde*

du 8 février cité par ce dernier, le ministère de l'économie aurait saisi la direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) pour enquêter sur le covoiturage « *réalisé dans un but lucratif* » par des particuliers. En outre, et suite à la pression des chauffeurs de taxi, le Gouvernement a publié, le 28 décembre 2013, un décret encadrant très strictement l'activité des véhicules avec chauffeur, en les soumettant notamment à un délai de 15 minutes entre la réservation et la prise en charge du client.

Si l'application de ce décret a finalement été suspendue début février par le Conseil d'État, saisi par les entreprises de voitures de tourisme avec chauffeur (VTC), ce dossier est révélateur de la **grande prudence des acteurs en place, économiques comme politiques, envers les innovations technologiques susceptibles de remettre en cause les modèles existants**. Pour M. Stéphane Grumbach, une telle mesure de confinement « *n'arrêtera pas le changement. Elle rappelle l'Hadopi. On imagine sans difficulté un résultat équivalent. Elle révèle l'incapacité de la France à accompagner ce changement dans le sens de l'intérêt commun et pas seulement de l'intérêt particulier.* »

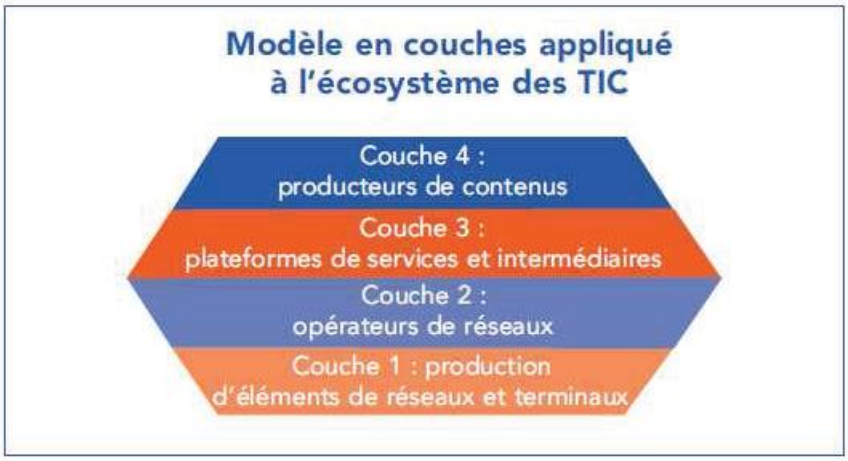
Notre pays, s'il reste prisonnier de telles réactions de repli, est parti pour passer à côté de la révolution numérique et de ses formidables potentiels de croissance. À cet égard, **la France est déjà en retard dans le domaine de la collecte de données**, fondamentale pour alimenter ces plateformes d'intermédiation qui seront au cœur de la société de demain et représenteront l'essentiel de la création de valeur[1].

- **Un déplacement de la chaîne de valeur numérique défavorable à l'Europe**

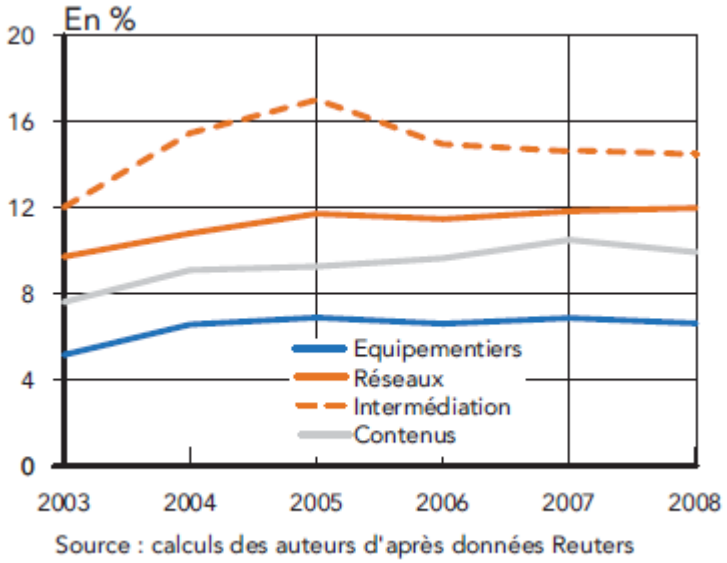
Ainsi que l'a souligné M. Jean-Ludovic Silicani, président de l'ARCEP, lors de son audition, la poursuite du développement de l'Internet repose sur le maintien d'un **équilibre durable entre ses trois différentes composantes** : « *les fournisseurs de services et de contenus, essentiels à son attractivité*[2] *; les opérateurs de réseaux qui permettent d'y accéder et doivent répondre à une demande croissante des utilisateurs ; et les fabricants d'équipements et de terminaux, dernier maillon de la chaîne qui va du service à l'utilisateur* ».

[1] *Voir* infra.

[2] *Laquelle peut être dédoublée, comme c'est le cas dans le schéma suivant, avec une couche « plateformes de services et intermédiaires ».*



Évolution du taux de marge par couches, toutes zones confondues



Source Coe-Rexecode, Les opérateurs de réseaux dans l'économie numérique, document de travail n° 16, janvier 2010.

Or, les **grands équilibres dans cette chaîne de valeur ont évolué ces dernières années**, et ce **dans un sens défavorable aux intérêts de l'Union européenne**. Ce point avait été développé par votre rapporteure dans son rapport *L'Union européenne, colonie du monde numérique ?* Citant une étude de l'institut Rexecode parue en 2011, qui analyse l'évolution des rapports de force mondiaux sur le marché du numérique, il décrivait le recul de notre continent sur deux segments de l'économie numérique : « *les équipements d'une part, secteur où l'Union européenne cède du terrain face à la concurrence asiatique ; les services intermédiaires ensuite, pour lesquels l'Union européenne se fait très largement distancer par les États-Unis et qui offrent en moyenne les taux de marge nette les plus élevés* », comme le montre le graphique suivant.

L'Europe, qui possède de solides opérateurs télécoms, compétitifs sur le marché international, est en revanche **dépourvue d'acteurs de premier**

plan aux deux autres bouts de la chaîne de valeur numérique : les **équipementiers** (Nokia excepté, les dix plus grands équipementiers mondiaux sont asiatiques ou nord-américains) et surtout, les **fournisseurs de contenus et d'applications**, également appelés *over the top* (OTT)[1]. C'est de ces derniers, dont les géants du web – les GAFA – sont la partie émergée, que vient le plus grand danger pour l'Europe : d'un côté leurs perspectives de développement semblent illimitées, et de l'autre, ils sont parvenus à se soustraire au financement des réseaux qu'ils utilisent largement, mais aussi à la contribution à la création culturelle, qu'ils diffusent pourtant amplement auprès de leur public.

- **Un accès au savoir filtré par des acteurs non européens**

Au-delà du financement de sa création culturelle, l'Europe est menacée de ne plus avoir accès au savoir et à la connaissance que par la médiation d'acteurs non européens. Cette perte d'indépendance est également très préoccupante.

Comme l'a souligné devant votre mission M. Laurent Sorbier, conseiller référendaire à la Cour des comptes et professeur associé à l'université Paris-Dauphine, « *quand la consultation d'un moteur de recherche devient le premier réflexe pour connaître quelque chose, le savoir se transforme et l'on doit se poser cette question : qui produit le contenu ? Quelles en sont les procédures de validation ? Ces questions vont prendre de plus en plus d'importance, à mesure que les objets connectés seront davantage utilisés. Dans un musée, par exemple, vous photographiez un tableau avec votre* smartphone *– demain avec vos lunettes – pour en savoir le peintre et la date grâce au système de reconnaissance d'images de Google : qui a écrit la notice, sinon un opérateur de Google – mais avec quelles compétences ? On verra, progressivement, que c'est notre construction même de la réalité qui en sera affectée ; or, étant donné qu'aucun des opérateurs de contenu n'est européen, ce nouveau filtre d'accès au réel sera composé par des opérateurs qui ne vivront pas dans notre société mais ailleurs, avec peut-être d'autres valeurs : c'est un changement anthropologique de première importance*. »

La domination en ligne d'acteurs non européens représente donc un défi culturel, voire anthropologique.

Pointant, derrière la domination de l'Internet par des acteurs non européens, le risque d'une « *Union européenne en voie de sous-développement dans le monde numérique* », le rapport rendu l'an dernier par votre rapporteure appelait à cet égard à resituer la stratégie numérique de l'Union européenne dans le contexte de cette nouvelle forme de mondialisation.

[1] *Position stratégique dans une chaîne de valeur consistant à utiliser les structures existantes installées par un autre acteur pour fournir un service de substitution sans rien lui reverser.*

C. L'INTERNET, SUPPORT D'UN MONDE D'HYPERSURVEILLANCE ET DE VULNÉRABILITÉ

Réseau de réseaux, l'Internet se caractérise avant tout par son architecture décentralisée. Cela semblait *a priori* garantir sa robustesse, du moins technique. Pourtant, l'expérience de ces dernières années a révélé certaines vulnérabilités et montré que tant l'évolution des technologies que celle des mentalités ont eu pour conséquence de transformer la promesse de liberté que constituait l'Internet en un fantastique outil de surveillance.

En facilitant le stockage et le traitement, le *big data* a en effet incité à une collecte exponentielle de données, notamment personnelles, que l'Internet des objets devrait encore venir alimenter. Ces données peuvent ainsi être exploitées aussi bien par les géants du net que par les services de renseignement, comme l'affaire Snowden l'a amplement démontré.

Parallèlement, la dépendance croissante de nos sociétés à l'Internet est devenue facteur de vulnérabilité, si bien que le réseau est maintenant le théâtre de véritables attaques.

1. Une collecte exponentielle de données, l'Internet des objets nourrissant le spectre de *1984*

a) L'amélioration des techniques a permis l'émergence du big data

Comme l'expliquait M. Pierre Bellanger lors de son audition par votre mission d'information, l'Internet est régi par diverses lois, dont deux intéressent particulièrement la question des données.

La première est la « loi de Moore », du nom du cofondateur de la société de processeurs Intel, qui constatait empiriquement dès 1965 que le nombre de transistors par circuit de même taille doublait tous les dix-huit mois, sans augmentation de leur coût. Ce constat, jamais démenti jusqu'à présent, a ainsi été érigé au rang de loi affirmant que **la capacité de calcul des puces électroniques double tous les dix-huit mois, à coût constant**. Cette loi a été étendue aux mémoires de stockage des données.

La seconde règle est le « calcul de Grötschel » qui établit que **la vitesse de calcul des algorithmes progresse quarante-trois fois plus vite que la puissance des microprocesseurs**, les algorithmes pouvant être définis comme les séquences d'opérations et d'instructions d'un programme informatique.

Ces deux lois expliquent la diminution du coût du stockage et celle du coût de la puissance de calcul des ordinateurs. La combinaison de ces deux éléments permet en conséquence de traiter des quantités toujours croissantes de données, donnant naissance au *big data*. **Le *big data* désigne donc l'ensemble des technologies, infrastructures et services permettant la collecte, le stockage et l'analyse de données recueillies et produites en**

nombre croissant, grâce à des traitements automatisés et au recours aux technologies de l'intelligence artificielle.

b) Le big data *a fait des données* « la ressource essentielle de l'économie numérique »

Si de nombreuses données ainsi collectées ou produites sont *a priori* anodines, le traitement qui en est fait, notamment par rapprochement et recoupement, tend à les rendre signifiantes. **Le *big data* a donc permis aux données, notamment personnelles, de devenir « *la ressource essentielle de l'économie numérique* »**, ainsi que l'ont mis en évidence MM. Pierre Collin et Nicolas Colin dans leur rapport sur la fiscalité du numérique précité. Comme l'indiquent les deux auteurs, « *les données permettent aux entreprises qui les collectent de mesurer et d'améliorer les performances d'une application, de personnaliser le service rendu, de recommander des achats à leurs clients, de soutenir des efforts d'innovation donnant naissance à d'autres applications, de prendre des décisions stratégiques. Les données peuvent également être valorisées auprès de tiers concessionnaires de leur utilisation*. »

« Carburant » de l'économie numérique, **les données font donc l'objet d'une collecte tous azimuts**. Celle-ci peut être « volontaire » : données publiées par les utilisateurs sur les différents réseaux sociaux (Facebook, Google +, Twitter…), données issues du développement du « *Quantified Self* » qui permet à chacun de « se mesurer » ou plus exactement de mesurer ses paramètres physiologiques pour mieux se connaître… Mais elle peut également être opérée à l'insu des individus par *online tracking* ou « traçage » des internautes lorsqu'ils naviguent sur le réseau, par exemple *via* des *cookies*. Ces données de navigation permettent de repérer les sites visités par les utilisateurs afin d'identifier leurs centres d'intérêts et d'élaborer des profils d'utilisateur. Ces profils sont souvent enrichis d'informations recueillies sur diverses bases de données publiques ou privées comme les réseaux sociaux, pour y inclure des données relatives à l'âge, au sexe, au nombre d'enfants, au niveau d'éducation...

Certaines entreprises se sont spécialisées dans le *online tracking* : les courtiers en données ou *data brokers*. Ces entreprises revendent les données collectées à des banques, des publicitaires, des agences de crédits, des assurances, des partis politiques... D'autres ont développé un modèle économique propre à l'Internet, qualifié de « bi- » ou « multiface » par MM. Collin et Colin, qui tend à devenir le modèle d'affaires dominant sur l'Internet. Sur la première face, un service rendu, gratuitement, au public permet de collecter des données qui seront exploitées sur un autre versant, par exemple en ciblant la publicité vers l'internaute ou en revendant ces données sur les marchés de traces. Les plateformes telles Google ou Facebook en sont les meilleurs exemples.

c) Des risques de manipulation et de discrimination inhérents au big data

Lors de son audition par votre mission d'information, Mme Valérie Peugeot a cependant dénoncé la « *dérive de notre économie vers [ce modèle économique qu'elle qualifie d']économie de l'attention, où le marketing prédictif occupe une place prédominante, car c'est structurellement encourager la captation plus ou moins licite de traces* ».

Outre ce risque de « vol » de données, cette « économie de l'attention » met en évidence le **risque de manipulation des individus** auquel nous expose le *big data*. À l'heure actuelle, le profilage des individus vise essentiellement à permettre de cibler la publicité, de façon à proposer aux internautes les produits dont leur profil laisse supposer qu'ils les intéresseront. Ce profilage pourrait cependant être utilisé à d'autres fins pour influencer les décisions des individus[1].

Ce risque de manipulation est d'autant plus grand que **les capacités techniques nouvelles du *big data* rencontrent opportunément les aspirations d'une société de plus en plus averse au risque et cherchant par tous les moyens à s'en prémunir**. Comme le remarquait M. Philippe Boucher, conseiller d'État honoraire : « *Nous entrons dans la société du contrôle permanent, qui refuse tout risque* ». Cela explique le succès de la co-production des données à laquelle se prêtent volontiers les internautes et qui aboutit au recueil de données en nombre toujours plus important dans l'idée que cette accumulation nous apportera une meilleure connaissance de tous les phénomènes, y compris humains. Lors de son audition, M. Viktor Mayer-Schönberger, professeur à l'*Oxford Internet Institute*, spécialisé en gouvernance et régulation de l'Internet, mettait toutefois en garde votre mission d'information : « *La dictature des informations mine l'avenir de nos démocraties : on leur accorde davantage d'importance qu'elles n'en ont, en pensant qu'elles peuvent tout expliquer. On veut réduire les risques et les incertitudes. La circulation libre de flux de données sur Internet, combinée à leur analyse, nous donne des prévisions probabilistes semblant très précises. On sera tenté de réagir, non aux comportements, mais à leur prédiction, réalisée par des algorithmes. Cela reviendrait à nier son libre arbitre. Le risque, en abolissant ainsi la responsabilité individuelle, c'est d'abandonner la culpabilité humaine et donc l'innocence.* »

En effet, la promesse de prédiction que recèle le *big data* ne doit pas faire oublier les méthodes mises en œuvre pour « faire parler » les données. En raison de leur volume croissant, de leur diversité et de leur qualité variable, les données recueillies ne peuvent plus être traitées avec des méthodes traditionnelles ; elles représentent un véritable défi en matière de vitesse de traitement. C'est pourquoi de **nouvelles méthodes d'analyse, fondées sur des calculs probabilistes**, se font jour qui permettent de tirer des conclusions sans avoir à consulter toutes les données. En outre, le *big*

[1] Cf. « *Des utilisateurs de Facebook « manipulés » pour une expérience psychologique* », LeMonde.fr, *30 juin 2014 : http://www.lemonde.fr/pixels/article/2014/06/30/des-utilisateurs-de-facebook-manipules-pour-une-experience-psychologique_4447625_4408996.html*

data ne fait qu'établir des corrélations ; on ne saurait donc faire l'économie de la recherche d'explications causales au risque de commettre des contre-sens et des extrapolations abusives.

La force du *big data* est donc également sa faiblesse : une confiance aveugle en ses capacités prédictives conduit à réduire chaque être humain à des comportements dont les probabilités auront décrété qu'ils constituent la norme. Cela emporte un fort **risque de discrimination** entre les internautes, notamment de ceux qui s'éloigneraient de certaines normes.

Ainsi que le montre le rapport de M. John Podesta[1] remis à M. Barack Obama, président des États-Unis, le risque de discrimination induit par le *big data* peut résulter de manière involontaire de la façon dont les algorithmes sont structurés. Le rapport donne ainsi l'exemple d'une application développée par la ville de Boston pour améliorer l'état des voiries en utilisant les données fournies par les GPS et accéléromètres placés dans les téléphones portables. Les développeurs se sont aperçus que les personnes âgées et celles de condition modeste possédant peu de *smartphones* et étant peu susceptibles de télécharger l'application, cela pourrait avoir pour conséquence de ne dresser l'état des voiries en vue de leur entretien que dans les quartiers occupés par des porteurs de *smartphones*. Cette discrimination peut toutefois également être volontaire pour écarter d'office certaines catégories de la population de l'accès à un emploi, à un crédit, à un logement...

d) Des risques renforcés par l'essor de l'Internet des objets

Prochaine étape du développement de l'Internet, qui n'en est encore qu'à ses prémices, ce que l'on appelle communément l'Internet des objets renvoie à la **faculté dont se voient dotés de plus en plus d'objets, y compris les plus banals de notre quotidien, de communiquer entre eux et avec des systèmes informatiques à travers divers réseaux et en particulier l'Internet, afin de s'identifier, de se géolocaliser et de proposer de nouveaux services**. Ce « web 3.0 » se propose, *via* des capteurs placés sur les objets connectés, de rendre plus « intelligents » un certain nombre d'équipements : la maison devient capable de réguler elle-même sa température, la *smart city* ou « ville intelligente », d'adapter l'offre de transport au trafic, les compteurs intelligents, de mieux anticiper les besoins énergétiques…

Cet essor de l'Internet des objets entraîne plusieurs conséquences.

Au niveau des flux échangés sur l'Internet d'abord, **les connexions humaines marquent le pas sur les connexions entre machines, déshumanisant les échanges sur l'Internet**. Selon une étude menée par la société américaine Cisco, citée par M. Per Stömbäck, responsable du Forum Netopia, au cours de son audition devant votre mission d'information, le

[1] *Cf.* big data : seizing opportunities, preserving values, *Executive Office of the President, mai 2014.*

trafic généré par les machines excèderait celui généré par les êtres humains dès 2020.

Ces données de plus en plus produites par des robots et analysées par des robots, conduisent à une prise de décision de plus en plus souvent assurée de manière autonome par des robots. Le *big data* s'accompagne en effet d'un essor des technologies de l'intelligence artificielle auquel on a recours pour analyser les données de masse, mais également désormais pour en tirer des conséquences et agir. L'exemple le plus flagrant en matière de prise de décision autonome par les automates est le *trading* haute fréquence : les algorithmes sont programmés de manière à exploiter le moindre mouvement de prix sur les marchés boursiers en se positionnant sur des laps de temps de l'ordre de quelques millisecondes. Le *trading* haute fréquence représenterait 50 % des échanges boursiers aux États-Unis et 37 % en Europe.

Or, on ne maîtrise qu'imparfaitement les effets de cette autonomisation croissante des machines. M. Murray Shanahan, professeur à l'*Imperial College* de Londres, observait ainsi qu'« *il est très difficile pour les concepteurs de tout prévoir surtout lorsqu'ils ne peuvent apprécier l'interaction de leurs systèmes avec d'autres. Outre cette interdépendance systémique et la globalisation, la rapidité d'exécution empêche que soit vue toute anomalie par un opérateur humain, cette anomalie pouvant, par un effet domino, perturber l'intégralité du système et des infrastructures dont nous sommes dépendants*. »

Surtout, **la masse des données recueillies et l'intrusion dans nos vies qu'elle implique va connaître avec l'Internet des objets un essor sans précédent**. M. Laurent Sorbier expliquait ainsi à votre mission d'information qu'en dépit de la faible mobilisation sociale contre les dangers de l'Internet, « *le législateur ne saurait se désintéresser d'un tel sujet – d'autant qu'avec les objets connectés, nous allons franchir un nouveau cap vers des existences complètement numérisées, où les données personnelles et comportementales que nous enverrons en continu aux* big data *dresseront nos sociotypes avec toujours plus de précision, offrant toujours plus de capacité de contrôle aux États et d'intrusion commerciale aux entreprises.* »

À sa suite, plusieurs personnes entendues par votre mission d'information ont exprimé cette même crainte de voir émerger une **société de surveillance**. Mme Valérie Peugeot décrivait ainsi la manière dont « *nous avons inconsciemment construit une société de surveillance absolue* » : « *plus notre économie inventera des services qui auront besoin de s'appuyer sur de la donnée pour fonctionner […], plus nous mettrons en place les infrastructures passives qui rendent les logiques de surveillance techniquement possibles, quel que soit le tiers qui décide de s'en servir. […] Le marketing prédictif est le meilleur ami de la surveillance car il recueille et traite les données toujours plus fines sur l'individu qui rendent cette dernière techniquement possible.* »

Dénonçant à son tour une « *aliénation généralisée* », M. Peter Warren, co-auteur du rapport *Can we make the digital world ethical ?* du Forum

Netopia[1], s'inquiétait d'un « *système où la surveillance est la règle, que ce soit dans la rue, désormais intelligente, avec votre portable, qui permet de connaître en temps réel votre géolocalisation, avec vos vêtements, qui seront en mesure d'émettre à tout moment un diagnostic sur votre état de santé et votre maison qui répondra à votre rythme de vie. Bref, la vie des individus va être cartographiée.* » Il invitait à mesurer l'« *avantage que peuvent retirer les agences de renseignements de cette profusion de données de masse* ».

De fait, les révélations de l'affaire Snowden accréditent le risque de surveillance généralisée que comporte le *big data* et les performances croissantes des algorithmes de traitement des informations.

2. De nouvelles possibilités pour les services de renseignement

Les services de renseignement ont, de tout temps, cherché à collecter des informations et, pour ce faire, intercepté les communications. Comme le rappelait le rapport de MM. Marcilhacy et Monory de 1973, invoquant la tradition du « Cabinet noir », dont l'existence est attestée depuis 1633, et le « ramollissement des cachets » selon l'expression de Beaumarchais, « *tous les régimes ont eu recours au viol des correspondances privées, jusqu'à ce que l'accroissement du volume du courrier postal et l'anonymat des envois, consécutif à l'emploi des timbres-poste, aient rendu matériellement impossible cette forme d'inquisition* »[2]. M. Olivier Guérin, délégué général de la Commission nationale de contrôle des interceptions de sécurité (CNCIS), rappelait quant à lui que les écoutes téléphoniques sont pratiquement aussi anciennes que le téléphone lui-même. Ces exemples montrent combien **les services de renseignement ont toujours su s'adapter à l'évolution des techniques. L'Internet n'a pas échappé à la règle**.

Bien que son architecture décentralisée paraisse à première vue rendre la tâche des services de renseignement plus compliquée, l'Internet semble au contraire, comme on l'a vu ci-dessus, aboutir à une hyper-surveillance que les services de renseignement ont appris à exploiter. Cet effet d'apprentissage a été particulièrement rapide, comme l'expliquait M. Bernard Benhamou à votre mission d'information : « *Les révélations d'Edward Snowden ont pris de court les experts, ainsi que les politiques, qui n'imaginaient pas qu'Internet permettait déjà de telles atteintes aux libertés publiques et à la vie privée. Nous pensions que les risques proviendraient de l'évolution vers l'Internet des objets […] Cet Internet du futur, tel qu'il avait été évoqué lors de la conférence interministérielle européenne de 2008, exigeait que soient mises en place de nouvelles mesures de protection de la vie privée. Mais peu d'experts imaginaient que les violations de nos droits étaient déjà quotidiennes,*

---

[1] *Peter Warren, Michael Streeter and Jane Whyatt,* Can We Make the Digital World Ethical ? Exploring the Dark Side of the Internet of Things and Big Data*, Netopia, février 2014.*

[2] *Cf. le rapport fait par MM. Pierre Marcilhacy et René Monory, au nom de la commission de contrôle des services administratifs procédant aux écoutes téléphoniques (n° 30, 1973-1974) disponible à l'adresse suivante : www.senat.fr/rap/r73-030/r73-0301.pdf*

orchestrées par les services de sécurité en prenant appui sur les réseaux sociaux et les moteurs de recherche, au point de poser un problème de confiance dans le réseau lui-même. »

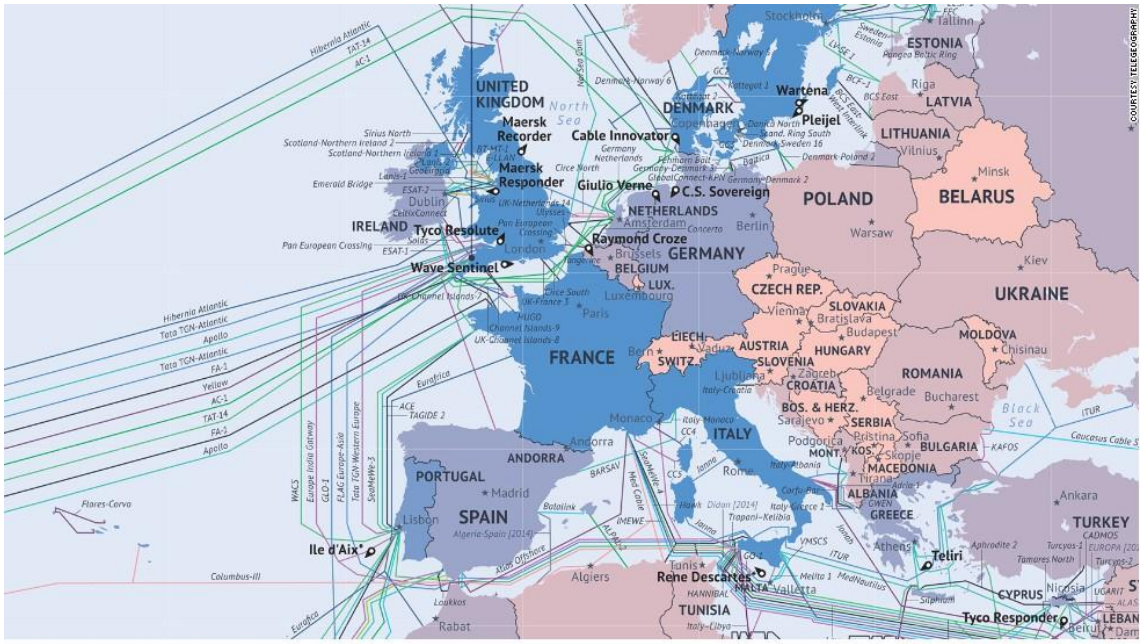
Cette hyper-surveillance a donc été rendue possible dès lors que les services de renseignement ont su s'approprier les outils du *big data*. Là où jadis les services de renseignement voyaient leurs capacités limitées par les moyens humains à leur disposition, un agent étant placé derrière chaque écoute, l'accroissement des capacités de stockage et d'analyse décrit précédemment a permis de démultiplier ces capacités *via* l'automatisation.

Les révélations d'Edward Snowden ont, à compter de juin 2013, mis en évidence que **la collecte en masse des données par les services de renseignement s'opère selon différents modes opératoires, l'interception intervenant à toutes les couches de la structuration de l'Internet**[1].

Au niveau de la couche des infrastructures techniques d'abord, l'*upstreaming* permettrait la collecte des données par branchement direct sur les réseaux publics ou privés. Ces branchements seraient effectués aux points d'atterrissement des câbles de fibre optique et dans les centres de commutation des données. Il est également probable que de tels branchements aient été opérés directement sur les très nombreux câbles sous-marins, qui font transiter 99 % du trafic intercontinental de données numériques[2]. Lors de son audition par votre mission d'information, M. Francesco Ragazzi, chercheur associé au centre d'études et de recherches internationales (CERI) de Sciences Po Paris et maître de conférences à l'université de Leiden (Pays-Bas), qui a contribué à l'enquête du Parlement européen sur les programmes de surveillance des différents services de renseignement, cet *upstreaming* serait « *le fait des États-Unis*, via *la NSA, mais aussi du Royaume Uni, qui [aurait] placé quelque deux cents de ces dispositifs sur les câbles qui relient les îles britanniques à l'Europe et aux États-Unis, de la DGSE française, autour de Djibouti et ailleurs, du* Bundesnachrichtendienst *(BND) allemand, qui s'intéresse entre autres aux données qui transitent à travers l'Internet Exchange de Frankfort, de l'agence suédoise FRA (*Försvarets radioanstalt*), pour les câbles qui relient les pays Baltes à la Russie* ».

[1] *Les développements qui suivent s'appuient notamment sur l'étude* « Les programmes de surveillance des États-Unis et leurs effets sur les droits fondamentaux des citoyens de l'UE » *de la direction générale des politiques internes, Départements thématique C, du Parlement européen, septembre 2013.*

[2] *Cf. David Fayon, ibid. p. 49.*



Source : CNN – 4 mars 2014

Au niveau logique ensuite, les informations recueillies par votre mission d'information feraient apparaître plusieurs procédés d'interception. Ils pourraient, en premier lieu, consister en le détournement de modalités de fonctionnement normal de l'Internet dont les protocoles, ouverts, sont construits sur la confiance. Ainsi de l'exploitation du protocole BGP (*Border Gateway Protocol*) permettant la communication entre les différents réseaux qui forment l'Internet pour détourner des données afin d'espionner le trafic à destination ou en provenance d'une partie du réseau sans avoir à installer de matériel ou modifier les systèmes qui sont attaqués. En deuxième lieu, ces procédés exploiteraient les failles de certains protocoles. Ce serait par exemple le cas pour la faille *Heartbleed* révélée dans le protocole *OpenSSL*, dont les services de renseignement américains sont soupçonnés avoir eu connaissance et avoir tiré profit.

M. Edward Snowden a, par ailleurs, révélé l'existence du programme *Bullrun* visant à affaiblir les technologies de chiffrement. Ce programme aurait permis l'intervention des services de renseignement sous plusieurs formes : « *collaboration avec les fournisseurs de produits et de logiciels de sécurité informatique, cryptanalyse mathématique et attaques par canal auxiliaire, falsification de certificats de clés publiques, infiltration et manipulation d'organismes techniques afin de leur faire adopter des normes non sûres, et utilisation coercitive probable d'injonctions judiciaires obligeant les créateurs de solutions de chiffrage à introduire des portes dérobées (*backdoors*)* »[1].

Enfin, le programme *Prism* a permis l'acquisition de données sur réquisition des opérateurs privés après délivrance de mandats par la *Foreign Intelligence Surveillance Court* (FISC), conformément aux dispositions du

[1] Cf. *l'étude du Parlement européen précitée, p. 19.*

Foreign Intelligence Surveillance Act (FISA). La publication par les « géants du net » – Facebook, Microsoft, Yahoo et Google – au mois de février dernier des détails sur le nombre de requêtes judiciaires reçues de la part des autorités américaines l'atteste.

Il convient au surplus de noter que la coopération des services de renseignement, dont les attentats du 11 septembre 2001 ont démontré l'impérieuse nécessité, accroît encore la masse de données à disposition de chacun des services de renseignement, compensant les inégalités de moyens[1].

En outre, ainsi que le faisait remarquer M. Maurice Ronai à votre mission d'information, « *la centralisation des usages et des trafics autour de quelques plateformes a considérablement facilité la tâche de la NSA. Ce n'est pas elle qui a créé les services Web centralisés, comme Facebook ou Google, mais elle les a utilisés.* »

Lors de son audition, M. Francesco Ragazzi indiquait que **le plus frappant est l'ampleur du phénomène de surveillance qui s'opère désormais à grande échelle**. Ainsi, le *Government Communications Headquarter* britannique intercepterait « *à lui seul 21 pétaoctets de données par jour, l'équivalent de l'utilisation quotidienne de 2,1 millions de gros consommateurs de bande passante, ce qui laisse penser que la surveillance porterait sur 3 à 4 millions de personnes par jour* ». Et M. Boris Beaude de conforter ce constat : « *les questions de surveillance, c'est un sujet très ancien où Internet, en fait, n'a fait qu'accélérer les choses, en changeant l'ampleur de la surveillance possible et en ouvrant des fenêtres sur la vie privée comme aucun dictateur aurait pu espérer en avoir* ».

Une fois les instruments de la collecte massive des données mis en place, les services de renseignement n'ont eu qu'à leur appliquer des algorithmes proches de ceux développés pour le profilage des consommateurs. Comme le disait M. Bernard Benhamou lors de son audition, « *les capacités de surveillance et de « profilage » des individus atteignent des niveaux qui n'ont proprement rien à voir avec ce qu'ils étaient il y a vingt ans. La cellule d'écoutes de l'Élysée utilisait des cassettes magnétiques, qu'il fallait transcrire, interpréter ; aujourd'hui, un opérateur peut analyser des milliards de données numériques, grâce à des machines mais aussi à des algorithmes dont la puissance est en évolution constante. […] L'analyse des « métadonnées » de communication (lieu, heure et type de connexion) permet à elle seule un « profilage » des utilisateurs dont la précision vous étonnerait…* »

Tel serait l'objet par exemple du système XKeyscore, décrit comme un « outil d'exploitation/cadre analytique » permettant d'effectuer des

[1] *M. Francesco Ragazzi a en effet indiqué à votre mission d'information que* « les chiffres […] révèlent l'extrême disproportion dans les moyens. La NSA emploie 37 000 personnes pour un budget annuel de 7 milliards, le GCHQ britannique (*Government Communications Headquarters*), 5 600 personnes pour un budget de 1,2 milliard, et la DGSE française 4 600 personnes pour un budget de quelque 650 millions ».

recherches sur un ensemble de bases de données regroupant les données stockées dans sept cents serveurs répartis sur cent cinquante sites. Ce système indexerait « *les adresses courriel, les noms de fichier, les adresses IP et les numéros de port, les mouchards (*« cookies »*), les noms d'utilisateurs et les listes d'amis utilisées par les systèmes de messagerie électronique ou de discussion en ligne, les numéros de téléphone et les métadonnées liées aux sessions de navigation (y compris les mots saisis dans les moteurs de recherche ainsi que les lieux observés par l'intermédiaire de Google Maps)* ». Ce système permettrait aux analystes de rechercher les événements considérés comme anormaux, par exemple une personne chiffrant ses communications ou recherchant des contenus suspects. À partir d'un « événement anormal » pourrait se déclencher une collecte automatique de données liées à cet événement.[1]

La tâche des services de renseignement serait ainsi en quelque sorte facilitée par l'évolution des comportements, les individus se dévoilant de plus en plus sur les réseaux sociaux. Telle est la thèse soutenue par M. Laurent Sorbier qui expliquait lors de son audition que « *l'action politique se heurte ici au fait que la conscience des citoyens et la mobilisation des décideurs face aux dangers d'Internet paraissent assez faibles, hormis la sphère assez spécialisée des activistes et des associations de défense des libertés ; la dissémination des données personnelles provoque une faible inquiétude, en particulier chez les jeunes* ».

Par ailleurs, **les études montrent une forme de résignation des populations face à cette surveillance exercée par les services de renseignement**. Ainsi, un sondage diffusé le 25 février dernier par Orange/Terrafemina indiquait que 57 % des Français estimaient la surveillance généralisée des échanges sur l'Internet justifiée à des fins de lutte contre les organisations criminelles et ce, bien qu'elle nuisît gravement aux libertés individuelles.

Ces divers éléments ont conduit à une **inversion dans la manière dont s'opèrent désormais les activités du renseignement**. Mme Isabelle Falque-Pierrotin, présidente de la Commission nationale de l'informatique et des libertés (CNIL), tirait des affaires récentes l'enseignement suivant : les affaires Snowden et Prism « *illustrent une rupture absolue dans le paradigme de surveillance. Jusqu'à présent, le pacte tacite était que les activités des services de renseignement ne visaient que les populations dites à risque et les dirigeants. Avec Snowden, nous changeons d'univers car tout le monde est maintenant concerné par la surveillance : cela signifie que le système par défaut est devenu la collecte généralisée de données. Il s'agit d'une inversion de la surveillance et donc de la présomption d'innocence*. »

Ce changement de paradigme est d'autant plus dangereux que comme M. Francesco Ragazzi l'expliquait à votre mission d'information, « *la NSA procède à un traitement algorithmique des données, qui produit directement*

[1] Cf. *l'étude du Parlement européen précitée, p. 18.*

des listes de cibles potentielles pour les drones de la CIA. De là à l'élimination totale du facteur humain dans la détermination des cibles, il n'y a qu'un pas. »

3. Des cyberguerres à venir

Les drones et autres robots ne sont cependant pas la seule menace qui pèse sur les États et les opérateurs économiques à l'heure du numérique. En matière de cyber-sécurité, outre la cybercriminalité, trois types de menaces sont aujourd'hui à l'œuvre sur l'Internet.

a) Une cyber-menace aux multiples visages

La première menace en termes d'importance est l'espionnage, et particulièrement l'espionnage économique. Cette menace concerne aussi bien les réseaux des administrations que des grandes entreprises : les informations visées peuvent être de nature politique, militaire, diplomatique ou économique lorsqu'un État est visé, technologique, commerciale ou financière lorsque l'attaque cible certains acteurs publics ou des entreprises. Selon M. Patrick Pailloux, ancien directeur général de l'Agence national de la sécurité des systèmes d'information (ANSSI), entendu par la commission des affaires étrangères du Sénat le 10 juillet 2013, « *le patrimoine de notre nation est littéralement pillé par voie informatique* », au point qu'il estimait qu'on n'avait jamais connu dans l'histoire « *une telle situation de pillage organisé à grande échelle* ». L'espionnage, souvent d'origine étatique, serait massif. Cette analyse semble partagée par d'autres, à l'instar de M. Philippe Lemoine qui déclarait lors de son audition par votre mission d'information que certains États tels les États-Unis n'hésitaient pas à mettre leurs services de renseignement au service des milieux d'affaires : « *Aux États-Unis, le contexte juridique, avec au premier chef le Patriot Act, s'est traduit, ainsi que le révèle le Washington Post, par une habilitation au secret-défense de 840 000 personnes, dont 135 000 seulement dans les agences de renseignement. Autrement dit, beaucoup sont dans les entreprises. Ces personnes ont deux employeurs, leur entreprise, et la NSA… Dans cet important appareillage, une part, très visible, se concentre sur la lutte contre le terrorisme, mais la plus grande part, beaucoup moins visible, se voue à l'espionnage économique.* »

La deuxième menace est la déstabilisation. Elle prend la forme de cyber-attaques visant à modifier le contenu des sites Internet attaqués, à en bloquer l'accès ou encore à voler les informations qu'ils contiennent afin de les rendre publiques. D'après M. Pailloux, de telles attaques seraient utilisées aussi bien dans des conflits internationaux – la France en aurait ainsi connu de faible ampleur alors qu'elle intervenait en Libye et au Mali – que dans des conflits franco-français. Il citait à cet égard l'attaque informatique contre le blog de M. Jean-Marc Ayrault, alors Premier ministre, dans le contexte de contestation du projet d'aéroport de Notre-Dame-des-Landes. L'exemple le plus marquant de cyberattaque demeure toutefois à ce jour celui de l'Estonie en 2007. Dans ce pays où la dématérialisation est très poussée – presque

toutes les démarches administratives se font par l'Internet –, des attaques dites « en déni de service » ont visé les sites gouvernementaux, les médias, les banques et les opérateurs téléphoniques : saturés par une multitude de demandes de connexion simultanées, les sites ne répondaient plus, paralysant des pans entiers de l'activité du pays durant plusieurs semaines.

La troisième menace est le sabotage des infrastructures critiques, à commencer par les réseaux d'importance vitale comme l'énergie, l'eau, les transports ou des opérateurs également d'importance vitale tels les hôpitaux. Lors de son audition, M. Pailloux citait divers exemples d'attaques avérées : le virus informatique Stuxnet qui a détruit des centrifugeuses de la centrale nucléaire de Natanz en Iran ou l'attaque contre les banques de Corée du Sud lors de tensions entre les deux Corées.

Si aucune de ces menaces n'est tout à fait nouvelle, l'Internet leur confère une acuité d'autant plus vive que **les attaques peuvent venir comme jadis de services de certains États, d'entreprises, d'organisations criminelles, mais aussi, et là réside la nouveauté, de simples individus**. En effet, le coût d'une attaque informatique est minime, la location d'un serveur coûtant moins d'un dollar. Le bénéfice attendu en revanche peut être énorme car chacun place de plus en plus de valeurs sur l'Internet : les individus, leurs données bancaires ; les bureaux d'études, leurs productions intellectuelles ; les industriels, leurs outils de production… En 2013, année où l'on aurait découvert 26 millions de logiciels malveillants, la cybercriminalité aurait pillé pour l'équivalent d'une valeur économique de 190 milliards d'euros en pertes directes, hors coûts d'arrêt des serveurs infectés ou coûts de communication sur l'incident.

En outre, **l'efficacité des attaques virales s'accroît au fur et à mesure de l'interconnexion des différents systèmes *via* le protocole Internet**. Pour reprendre l'image utilisée par M. Hervé Guillou, président du Comité des industries de la confiance et de la sécurité (CICS)[1], le cyberespace est un pavé à neuf cases composé de trois couches traversant trois mondes. Ainsi qu'on l'a déjà vu, ce qu'on appelle usuellement l'Internet est en fait une superposition de trois couches : la couche physique – les câbles, les liaisons radios, les liaisons satellites –, la couche technique comprenant les normes et protocoles standards assurant le transport de l'information, et la couche informationnelle comportant les applications et les contenus. Ces trois couches « horizontales » sont communes à trois mondes « verticaux » que les développements informatiques ont historiquement conduit à cloisonner : l'informatique générale, l'informatique industrielle avec ses automates, sa robotique, ses outils de gestion de la production assistée par ordinateur, et l'informatique embarquée, à bord des avions notamment, qui se caractérise par la gestion en temps réel.

[1] Cf. *l'entretien donné à ParisTech Review le 25 avril 2014.*

On assiste à l'heure actuelle à un double mouvement affectant cet ordonnancement traditionnel. En premier lieu, le protocole Internet est en train de déborder de sa deuxième couche originelle vers la première *via* la virtualisation des infrastructures et matériels : réseaux de télécom, routeurs, serveurs avec le *cloud computing* qui désigne le stockage des données et des applications non plus sur le terminal mais sur des serveurs distants, offrant la faculté d'accéder à ses données depuis n'importe quel terminal, tout en éloignant l'individu de ses propres données. En second lieu, le protocole Internet permet de connecter informatique générale et informatique industrielle d'une part, et informatique industrielle et informatique embarquée d'autre part. À titre d'illustration, on peut citer l'exemple de l'avion Airbus doté de sept adresses IP lui permettant de se connecter à des services électroniques d'approvisionnement, mais également de télécharger son plan de vol et de transmettre ses données de vol. Cette interpénétration des couches et des univers informatiques différents rend plus vulnérables les systèmes face à des attaques qui deviennent systémiques. Des pans entiers de la vie sociale ou économique peuvent désormais être détruits par une attaque ; **le *hacking* est devenu une véritable arme**.

Milton L. Mueller, professeur à la Syracuse University, a ainsi expliqué à votre mission d'information qu'à l'instar des marchés d'armes, il s'était développé un véritable marché des « *Zero Day vulnerabilities* ». La valeur d'une vulnérabilité informatique réside en ce qu'elle n'a pas encore fait l'objet d'une publication et est encore méconnue de la communauté de la cyber-sécurité. Son efficacité tient donc au fait qu'aucune réponse n'a encore été développée. Le virus Stuxnet qui a détruit des centrifugeuses iraniennes exploitait par exemple quatre de ces « vulnérabilités Jour Zéro ». Le magazine américain Forbes révélait en 2012 que les prix pouvaient varier entre 5 000 et 250 000 dollars selon les systèmes d'exploitation dans lesquels se trouvait la vulnérabilité[1].

b) Un constat d'impréparation des États et des entreprises

Face à cette cyber-menace de plus en plus prégnante, les différentes personnes entendues par votre mission d'information font montre de leur préoccupation quant au degré d'impréparation des différentes organisations et infrastructures européennes, en particulier des entreprises. La raison principale en est le coût de la mise en place de systèmes de cyber-sécurité efficaces qui constitue un investissement sans rentabilité immédiate. M. Jean-Claude Mallet, conseiller auprès du ministre de la défense, faisait ainsi le constat que **les capacités de défense sont inversement proportionnelles à l'imprégnation du numérique dans notre vie quotidienne**.

Pourtant, la cyber-sécurité fait l'objet d'une grande attention au niveau de l'Union européenne depuis le début des années 2000, attention

[1] Cf. *Andy Greenberg, "Shopping For Zero-Days : A Price List For Hackers' Secret Software Exploits"*, Forbes, *23 mars 2012*.

renouvelée après la cyber-attaque dont a été victime l'Estonie en 2007. Dès 2001, dans sa communication sur la « Sécurité des réseaux et de l'information : proposition pour une approche politique européenne », la Commission soulignait l'importance croissante de ces enjeux de cyber-sécurité. En 2004 a ainsi été créée l'ENISA, Agence européenne pour la sécurité des réseaux et de l'information, qui a pour mission d'assurer un niveau élevé de sécurité des réseaux et de l'information. À ce titre, l'ENISA intervient en tant qu'expert en matière de sécurité des réseaux et de l'information auprès des autorités nationales et des institutions européennes et favorise l'échange de bonnes pratiques. Depuis 2010, elle organise, en coordination avec l'ensemble des agences nationales en charge de la cyber-sécurité ainsi que les entreprises privées du secteur des télécommunications et de l'énergie, des exercices de simulation de cyberattaque. Le troisième exercice de ce type a eu lieu les 28 et 29 avril derniers.

Malgré cette attention particulière et devant l'inefficacité des mécanismes purement incitatifs jusqu'alors prescrits dans ses communications de 2009 et 2011, la Commission européenne a publié le 7 février 2013 une proposition de directive sur la sécurité des réseaux et des systèmes d'information, dite « directive SRI ». Cette directive a pour objet le renforcement des capacités des États membres face aux cyber-menaces. Pour ce faire, la Commission propose deux types d'actions. D'une part, elle impose aux États un certain nombre d'obligations : désigner une autorité nationale compétente en matière de SRI – ces autorités nationales étant appelées à coopérer au sein d'un réseau européen –, se doter d'un centre d'alerte et de réaction aux attaques informatiques, élaborer une stratégie nationale de cyber-sécurité ainsi qu'un plan national de réponse aux cyber-crises. D'autre part, s'agissant des entreprises, la proposition de directive souhaite étendre à certains opérateurs de marché incluant les secteurs d'importance critique, les obligations pesant actuellement sur les seuls opérateurs de télécommunication en matière de notification d'incidents informatiques significatifs et de soumission à des audits réguliers conduits par l'autorité nationale compétente, sous peine de sanction.

Cette proposition ambitieuse de la Commission européenne a cependant été partiellement vidée de sa substance lors de l'adoption du texte en séance plénière au Parlement européen, le 13 mars dernier. L'obligation de notification des failles de sécurité n'a ainsi été maintenue que pour les « acteurs du marché », à l'exclusion des fournisseurs de matériel et de logiciel[1]. Seuls les réseaux « critiques » y seraient donc soumis tandis que les administrations publiques, les éditeurs de logiciel, les réseaux sociaux, les fournisseurs de services en *cloud* et les fournisseurs de contenus notamment resteraient libres de notifier les incidents sur la base du volontariat. Pourtant,

[1] *Le considérant 24* bis *de la directive à l'issue de son examen par le Parlement européen énonce en effet que* « les fournisseurs de matériel et de logiciel ne sont pas des acteurs du marché comparables à ceux visés dans la présente directive ».

ainsi que le remarquait un observateur, dans 84 % des problèmes constatés, les failles se trouvaient du côté des logiciels[1]. Cette position du Parlement européen augure mal des progrès nécessaires des entreprises en matière de cyber-sécurité.

La France a, quant à elle, d'ores et déjà mis en œuvre une partie des obligations qui devraient résulter de la directive SRI. Après la création en 2009 de l'Agence nationale de sécurité des systèmes d'information (ANSSI) et la publication en 2011 de sa stratégie nationale de sécurité et de défense des systèmes d'information, elle a en effet érigé au rang de priorité nationale la cyber-défense dans son Livre blanc sur la sécurité et la défense nationale de 2013. À la suite de quoi, la France s'est dotée, avec la loi de programmation militaire du 18 décembre 2013[2], de nouveaux outils. Parmi ceux-ci, la faculté offerte au Premier ministre d'imposer aux opérateurs « *dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation* » les règles organisationnelles ou techniques de sécurité nécessaires à la protection de leurs systèmes d'information. Le Premier ministre sera désormais également en mesure de demander des audits ou des contrôles de sécurité à ces opérateurs qui ont, par ailleurs, une obligation de notifier les incidents affectant leurs systèmes d'information.[3] Ce dispositif devrait concerner environ deux cents opérateurs.

Le chemin vers la sécurisation de l'Internet est donc encore long.

II. LE SÉISME SNOWDEN TRANSFORME LA GOUVERNANCE DE L'INTERNET EN ENJEU GÉOPOLITIQUE

Si les dirigeants politiques des grands pays de l'Union européenne semblent encore peu sensibilisés à ses enjeux stratégiques, la gouvernance de l'Internet est bien identifiée par les États-Unis comme un sujet diplomatique d'importance. M. François Delattre, ambassadeur de France aux États-Unis, a même indiqué à la délégation de votre mission qu'il a reçue à Washington que Mme Madeleine Albright, ancienne secrétaire d'État des États-Unis[4], lui avait confié que ce sujet était « *en haut de l'agenda diplomatique des États-Unis* ».

---

[1] Cf. *Nathalie Steiwer, « Accord fin 2014 sur la cybersécurité en forme de coquille vide »*, Europolitics*, 27 mars 2014.*

[2] *Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale*.

[3] Cf. *les articles L. 1332-6-1 et suivants du code de la défense.*

[4] *1997-2001.*

A. LE SÉISME SNOWDEN REND IMPOSSIBLE LE STATU QUO D'UNE GOUVERNANCE AMÉRICAINE DE FAIT

Si les révélations d'Edward Snowden ne remettent pas directement en cause l'écosystème actuel de la gouvernance de l'Internet, leur effet politique a induit une perte de confiance globale dans l'Internet et dans les modalités de sa gouvernance. Le débat déjà ancien sur le rôle tenu par les États-Unis a pris un tour plus vif ces derniers mois.

1. Une gouvernance distribuée mais dominée de fait par les États-Unis

Aucune autorité centrale ne gouverne l'Internet aujourd'hui, ni aucune de ses couches réseau, transport ou application. En revanche, une pléthore d'enceintes participent à une forme d'autorégulation du réseau, qui répond bien au caractère décentralisé et distribué d'Internet. Comme le soulignent ses acteurs, cette **gouvernance distribuée** a fait la preuve de son efficacité puisque l'Internet n'a jamais été indisponible depuis quinze ans qu'existe l'ICANN : votre mission en convient, mais elle considère que la place qu'occupe l'Internet dans notre monde plaide pour aller au-delà d'une simple régulation technique, d'autant que les modalités techniques de ce fonctionnement ne sont pas, en fait, sans incidences politiques.

Diffuse, la gouvernance de l'Internet apparaît insaisissable. Sans doute la multiplicité des instances de gouvernance répond-elle à la complexité de la matière à gouverner, mais elle rend difficile toute vision d'ensemble. **Ceci nourrit chez les États et les organisations internationales une forme d'insécurité sur leur capacité à trouver un espace où s'exerce la gouvernance de l'Internet**.

a) Un foisonnement d'enceintes historiquement américaines qui, sous des dehors techniques, déterminent l'évolution de l'Internet

L'Internet se définit comme un réseau de réseaux qui utilisent un ensemble de protocoles communs TCP/IP (*Transmission Control Protocol/ Internet Protoco*l). Les organisations qui produisent ces protocoles techniques ont spontanément assumé la « gouvernance du réseau » dès ses débuts. Il s'agissait de maintenir l'Internet en état de fonctionnement. Issu de l'univers informatique, le protocole TCP/IP s'est progressivement imposé face à d'autres protocoles issus du monde des télécoms et ses promoteurs ont déployé leur action **en dehors de l'Union internationale des télécoms** (UIT), agence des Nations unies chargée de la réglementation et de la planification

des télécommunications, héritière de l'Union internationale du télégraphe créée en 1865[1].

Groupes de travail de l'Union internationale des télécommunications

Outre son secrétariat général et l'*International Frequency Registration Board* (IFRB), l'UIT est divisée en trois groupes de travail :

– l'UIT-T (CCITT, « Comité Consultatif International Téléphonique et Télégraphique », jusqu'en 1993) traite les questions techniques et de normalisation. À chaque catégorie de normes correspond une lettre de l'alphabet, la référence de la norme étant complétée d'un nombre. Les normes de la série V (Transmission de données par le réseau téléphonique), par exemple V.24 ou V.90, et de la série X (Réseaux informatiques et systèmes ouverts), par exemple X.25, X.400 ou X.500, sont plus particulièrement connues des utilisateurs ;

– l'UIT-R (CCIR, « Comité Consultatif International des Radiocommunications », jusqu'en 1993) traite les questions techniques et d'exploitation concernant les radiocommunications ;

– l'UIT-D (BDT, « Bureau de Développement des Télécommunications », jusqu'en 1993) s'attache à promouvoir l'accès aux télécommunications dans les pays en voie de développement.

Diverses applications ont été développées sur l'Internet : courrier électronique, messagerie instantanée, forums de discussion, transfert de fichiers, téléphonie… et surtout, depuis 1991, le web, qui permet d'explorer de manière graphique l'Internet *via* un système d'hyperliens. Le web a favorisé un développement rapide de l'Internet et a évolué dans les années 2000 vers le web 2.0, qui repose sur l'utilisation de techniques standards (langages, navigateurs…) offrant aux internautes de plus grandes possibilités d'interaction et de partage d'informations. On évoque aujourd'hui le web 3.0, conjonction de l'Internet des objets et du web sémantique, où l'information est qualifiée en amont pour faciliter son exploitation ultérieure et permettre de la retrouver plus aisément dans l'immensité du réseau.

On le voit, **l'histoire de l'Internet, c'est avant tout l'histoire d'une technique, celle de protocoles et de standards qui ont été mis dans le domaine public et ont fait l'objet d'une forme d'autorégulation très peu institutionnalisée, correspondant à la nature distribuée du réseau**.

Les développeurs de l'Internet, très liés aux universités américaines, forment une communauté soudée par des « valeurs » communes de partage des ressources, d'ouverture de l'accès et de méfiance à l'égard de toute implication des gouvernements. Comme l'a rappelé M. Jean-François Abramatic, ancien président du W3C (*World Wide Web consortium*) de 1996 à 2001, lors de son audition par votre mission, David D. Clark, le créateur du protocole IP, a bien résumé par ces mots l'état d'esprit des pionniers du

[1] *L'UIT conserve un rôle important en matière de normalisation dans le domaine numérique, notamment avec l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI).*

web : **« *Nous refusons les rois, les présidents et les votes. Nous croyons au consensus approximatif et au code qui marche.* »**

Cette « communauté de l'Internet » anime plusieurs instances qui participent à la gestion de l'Internet, chacune pour un aspect spécifique, et fonctionnent de manière informelle, selon un processus ascendant (*bottom up)* et privilégiant le consensus.

S'agissant des normes et standards, la communauté des concepteurs et des chercheurs se réunit depuis 1986 au sein de l'***Internet Engineering Task Force*** (IETF). Issue de l'***Internet Architecture Board*** (IAB)[1], cette *task force* sans personnalité morale produit par consensus des **standards techniques ou spécifications de protocoles**[2], qui orientent l'architecture du réseau à long terme. Son secrétariat est à Fremont, en Californie. L'IETF est ouverte à toute personne qui souhaite y participer. Mais la représentation en son sein reflète naturellement l'intérêt des entreprises présentes ; les plus grandes entreprises de l'Internet étant américaines, elles y sont donc particulièrement influentes.

Les documents sont tous publics, et discutés publiquement ; de plus, un projet de spécification ne peut passer la première étape de validation que si deux « implémentations » ont été faites de façon indépendante. Cette méthodologie garantit d'être à l'état de l'art et assure l'efficacité des protocoles et la lisibilité des documents de référence. **La prise de décision se fait par consensus, c'est-à-dire concrètement par *humming*** : comme l'a expliqué à votre mission M. David Martinon, représentant spécial pour les négociations internationales concernant la société de l'information et l'économie numérique, le consensus est atteint quand toute objection raisonnable a été discutée et quand une approbation (*hum*) assez sonore est audible. À titre indicatif, l'IETF produit ainsi environ 250 appels à commentaires ou *requests for comments* (RFC) par an, dont la moitié sont des propositions de standards. Au bout d'un processus qui peut durer plusieurs années, deux à trois de ces propositions deviennent chaque année des standards aboutis ayant un caractère obligatoire[3]. M. Pierre-Jean Benghozi, membre du collège de l'ARCEP, a fait observer à votre mission les limites de cette autorégulation : non seulement l'IETF est concurrencée par d'autres institutions – comme l'*Open Source initiative*, association de développeurs libres, lors de l'élaboration de la norme Wifi –, mais elle donne également lieu à une « coopétition » pour définir des standards communs, les entreprises tentant de traduire ces standards dans leurs systèmes propriétaires pour se faire concurrence par le biais de brevets.

---

[1] *Initiée dès 1979 par M. Vinton Cerf, alors directeur de programmes à la* Defense Advanced Research Projects Agency *(DARPA), et désormais sous contrôle de l'ISOC.*

[2] *Ainsi, selon le standard RFC-791 établi par l'IETF, chaque paquet IP se compose d'un en-tête, d'une adresse source, d'une adresse destination et de données à transmettre.*

[3] *La France est impliquée dans ce processus et représente 4 % de cette production à travers des auteurs issus du monde académique et industriel (France Telecom, Orange, INRIA, AFNIC, Alcatel Lucent, Renater, SFR, Bouygues Telecom, Institut Telecom…).*

L'IETF est chapeautée (et financée) par l'***Internet Society*** (ISOC), structure juridique fondée en 1992 par M. Vinton Cerf **pour promouvoir le développement universel de l'Internet**. L'ISOC est une association américaine de droit virginien – son siège est à Reston, aux États-Unis – qui a construit un réseau mondial, *via* des bureaux régionaux sur chaque continent et une centaine de chapitres nationaux. L'*Internet Society* regroupe dans ses chapitres de nombreux acteurs, personnes morales, associations et simples usagers : elle compte 65 000 membres. L'*Internet Society* gère l'extension « .org », dont elle tire une part de ses ressources, et participe aux activités de la communauté technique. C'est aussi le cas du W3C, dont elle assure une grande partie du financement, et de l'*Internet Engineering Task Force* (IETF), dont l'*Internet Society* assure la coordination et une partie du financement. Mais chaque chapitre doit trouver son propre financement, comme l'ont fait observer MM. Gérard Dantec, président du chapitre français de l'*Internet Society*, et Sébastien Bachollet, président d'honneur du même chapitre, lors de leur audition par votre mission. Selon M. David Fayon, son budget annuel, d'environ 6 millions de dollars en 2011, est couvert essentiellement par les cotisations et dons des organisations membres, les principaux donateurs étant de grandes entreprises américaines[1] (Cisco, VeriSign, Google, Microsoft, Comcast), mais aussi le Département de la Défense américain.

En 1994, avec le soutien du *Massachusetts Institute of Technology* (MIT), mais aussi de la Commission européenne, fut créé **le *World Wide Web consortium*** (W3C), consortium plus spécifiquement **dédié au web afin de conduire cette application à son plein potentiel** en développant des protocoles et des lignes directrices. Selon M. Jean-François Abramatic, qui en fut le président de 1996 à 2001, M. Tim Berners-Lee, concepteur du web, a d'emblée voulu donner une dimension mondiale au consortium en y associant le MIT et le CERN, qui fut ensuite remplacé par l'INRIA puis par l'ERCIM pour représenter l'Europe[2]. Et en 1996, l'Université de Keio au Japon a été choisie comme hôte asiatique du W3C. Depuis, en 2013, l'Université de Beihang en Chine a intégré le conglomérat. Le W3C a également ouvert des bureaux régionaux de par le monde, qui concourent à son internationalisation. Il existe un tel bureau en France, porté par l'INRIA.

S'appuyant sur des experts techniques surtout américains, mais aussi japonais, chinois et européens – votre mission a pu rencontrer à Boston l'un de ses membres français, M. Philippe Le Hégaret –, le W3C adopte des standards ouverts (non propriétaires), comme par exemple le langage HTML5, contribuant à faire évoluer les normes du web pour assurer sa cohésion et son interopérabilité. Il travaille également à améliorer l'accessibilité du web aux personnes handicapées. Les décisions s'y prennent dans un souci de transparence et par consensus ; aux dires de M. Le Hégaret,

[1] *Même si Nokia et Alcatel-Lucent figurent parmi les donateurs.*

[2] European Research Consortium for Informatics and Mathematics.

l'autorité morale de M. Tim Berners-Lee permet de résoudre les éventuelles difficultés.

Conformément à la philosophie de l'Internet, toute personne ou organisation, privée ou publique, peut devenir membre si elle en accepte les conditions et si elle s'acquitte d'une cotisation, qui varie pour les entreprises en fonction du chiffre d'affaires mais qui est plafonnée. Le W3C compte aujourd'hui 384 membres[1] qui lui apportent les deux tiers de ses revenus, le reste provenant de bourses de recherche ou de donations. Un comité consultatif réunit les représentants de ces membres (un par membre), et élit un conseil consultatif de dix membres, qui n'a aucun pouvoir décisionnaire mais dialogue avec l'équipe d'experts techniques. M. Le Hégaret a indiqué à votre délégation que la **NSA elle-même** avait été **membre en titre du W3C** il y a quelques années…

Comme l'a expliqué M. Le Hégaret – dont l'employeur direct est d'ailleurs le MIT – à votre délégation, **le W3C n'a pas de personnalité morale**. Ceci atteste bien du **lien organique qui relie les instances de gouvernance technique du web et les acteurs américains de la recherche et de l'innovation**, qui s'appuient sur les plus grandes universités de Boston.

b) L'ICANN, gestionnaire puissant des ressources critiques de l'Internet

À ces premiers cénacles « historiques », et face au développement de l'Internet et donc du nombre d'identifiants sur le réseau, le gouvernement américain a ajouté l'**ICANN**, en 1998[2]. Aux termes de ses statuts, cette société de droit californien, dont le siège est à Los Angeles, a pour mission de « *coordonner, à un niveau général, les systèmes mondiaux d'identificateurs uniques d'Internet et notamment d'en assurer la stabilité et la sécurité d'exploitation* ». Ceci recouvre **trois missions** essentielles : coordonner et assurer la sécurité du système global d'**identificateurs uniques** permettant de se connecter sur l'Internet (noms de domaine, adresses IP pour identifier le destinataire, numéros des ports de protocole et des paramètres…) ; coordonner l'exploitation et l'évolution des **serveurs racines du *Domain Name System*** (DNS), qui sont au nombre de 13 (désignés par des lettres de A à M) ; coordonner le **développement des politiques liées à ces fonctions techniques**. 265 millions de noms de domaine sont aujourd'hui enregistrés, selon les informations transmises par l'INRIA à votre mission.

Le DNS comprend deux types de domaines, l'un générique, l'autre géographique : le premier correspond aux *generic Top-Level Domain* (gTLD) comme « .net », « .com », « .org », « .info »… ; le second repose sur les codes des entités géographiques, désignés comme *country code Top-Level Domain*

[1] *Pour la France, on relève la présence de l'INRIA et d'Orange.*

[2] *Jusqu'à fin 2009, le Département du commerce américain était lié à l'ICANN par un* Joint Project Agreement *; ce lien étroit a été légèrement relâché à partir du 30 septembre 2009, date à laquelle l'ICANN est censée être devenue indépendante, quoique toujours engagée envers les États-Unis par une* Affirmation of commitments.

(ccTLD), même si les 247 ccTLD ne couvrent pas seulement des États souverains.

Originellement, seules quelques centaines d'ordinateurs étaient connectées à l'Internet et leurs adresses pouvaient être stockées dans un fichier unique établissant la correspondance entre chaque machine et un numéro. Du fait du développement exponentiel du réseau, le DNS fut créé en 1983 et sa gestion donna lieu à une controverse dans le courant des années 1990. L'US *National Science Foundation* décida de privatiser cette activité et de la confier à la société américaine *Network Solution Inc*. La communauté de l'Internet contesta cette solution et, après quatre ans de négociations, le vice-président américain Al Gore décida la création de l'ICANN, organisation dédiée à la gestion des noms de domaine. Comme l'a fait observer à votre mission Mme Massit-Folléat lors de son audition, la Commission européenne valida la création de l'ICANN[1], après avoir pesé pour une représentation des gouvernements en son sein.

L'ICANN assure la coordination globale du DNS ; elle attribue les gTLD et ccTLD et en assure la maintenance technique et administrative. Comme l'a fait observer l'INRIA à votre mission, la structure hiérarchique du nommage DNS crée une pseudo sémantique pouvant laisser penser que les sites dont l'extension est « .fr » sont établis en France, ou que ceux en « .com » relèvent de sociétés commerciales, ce qui peut être trompeur : en effet, une machine sous « .fr » peut être située n'importe où sur la planète, de même qu'il peut y avoir, sur le territoire français, des machines rattachées à pratiquement n'importe quel TLD.

L'ICANN attribue d'autorité des blocs d'adresses IP et numéros de systèmes autonomes aux **cinq registres Internet régionaux** (RIR) : un pour l'Amérique du Nord, un pour la zone Asie-Pacifique, un pour l'Amérique du Sud et les Caraïbes, un pour l'Europe et le Moyen-Orient et un pour l'Afrique. Chaque système autonome regroupe des réseaux IP possédant une politique de routage propre et indépendant, l'interconnexion de ces 45 000 systèmes autonomes constituant Internet. Ensuite, les RIR, qui sont parfaitement indépendants de l'ICANN, allouent les adresses IP aux **registres nationaux (NIR) et locaux (LIR)** ; les registres Internet locaux attribuent alors les adresses IP aux **fournisseurs d'accès à Internet (FAI)** qui assignent à leur tour les adresses IP aux utilisateurs finaux, les internautes.

[1] Cf. *communication de la Commission du 11 avril 2000, au Conseil et au Parlement européen concernant l'organisation et la gestion de l'Internet - Enjeux internationaux et européens 1998 – 2000, COM(2000)202.*

L'Association française pour le nommage Internet en coopération (AFNIC)

Conformément aux articles L. 45 à L. 45-7 du code des postes et des communications électroniques, le ministre en charge des communications électroniques désigne les opérateurs des domaines correspondant aux codes pays du territoire national ou d'une partie de celui-ci : « .fr », « .re » (Réunion), « .mq » (Martinique), « .pm » (Saint-Pierre-et-Miquelon)…, après consultations publiques et appels à candidature. Un décret pris en Conseil d'État précise les pouvoirs de cet office d'enregistrement et ses obligations. Une convention entre l'État et l'office d'enregistrement vient compléter ce dispositif.

L'Association française pour le nommage Internet en coopération (AFNIC), lauréat de l'appel à candidatures pour la gestion du « .fr », est une association « loi 1901 » qui opère dans un univers concurrentiel. Son organisation est multipartite depuis sa création, l'INRIA et l'État étant autour de la table du conseil d'administration, lequel comprend des représentants du secteur public, du secteur privé et des utilisateurs. On relève que les pouvoirs publics représentent la moitié du conseil d'administration, à parité avec l'ensemble des autres acteurs.

Les décisions opérationnelles sont prises dans ce cadre multipartite, dans le respect de la loi française. L'AFNIC bénéficie d'une certaine autonomie vis-à-vis de l'ICANN, avec laquelle elle a seulement procédé à un échange de lettres d'intention. Aucun texte juridique international n'attribue explicitement le domaine Internet « .fr » à la France.

Lors de son audition par votre mission, M. Mathieu Weill, directeur général de l'AFNIC, a indiqué que celle-ci, comme ses homologues dans d'autres États, était sous le régime de « *trustees* », c'est-à-dire de dépositaires de la confiance des parties prenantes de chacun de leurs pays pour gérer des ressources communes dans l'intérêt général. En France, a été reconnu comme une mission de service public le développement du « .fr », qui comprend environ 2,5 millions noms de domaine[1], face au « .com » qui demeure *leader*, y compris en France. Or le fait d'être enregistré en « .com » donne un point d'appui à la juridiction américaine.

Sur le plan technique, l'AFNIC gère un parc de serveurs dans le monde pour assurer la continuité de service du « .fr » et l'aiguillage des noms de domaine vers les serveurs sur lesquels ils sont hébergés.

Parallèlement, elle gère une base de données enregistrée en France que M. Weill a présentée comme l'une des plus protectrices au monde car, contrairement au « .com », les données des personnes privées enregistrées en « .fr » ne sont pas publiées. Elles ne sont communiquées qu'aux autorités françaises, uniquement sur la base d'un fondement légal, et aux ayant-droits, s'ils apportent la preuve que le nom de domaine constitue une atteinte à leur propre droit.

Le point fondamental de la mission de l'AFNIC est donc d'apporter un service sûr et stable, de soutenir l'innovation sur l'Internet et d'accompagner les acteurs français de l'écosystème national.

L'AFNIC et ses homologues européens se coordonnent au sein du *Council of European National Top Level Domain Registries* (CENTR).

[1] *À comparer aux 15 730 000 domaines en « .de » gérés par l'homologue allemand de l'AFNIC, la DENIC eG.*

Les serveurs racines ou serveurs de noms de domaine possèdent un répertoire officiel qui leur permet de répondre aux requêtes des internautes en traduisant les noms de domaine (ou URL) en adresses IP exploitables par un ordinateur. **Dix sur les treize serveurs racine se situent aux États-Unis**[1]. Cette répartition géographique s'explique par des raisons principalement historiques et doit être nuancée dans la mesure où chacun de ces serveurs est dupliqué plusieurs dizaines de fois à travers le monde afin d'assurer la stabilité et la résilience du réseau.

Serveur, serveur de nom et serveur racine : définitions

Serveur

Un serveur est un ordinateur de grandes capacités (puissance processeur, mémoire, disques durs) relié au réseau et ayant pour vocation de fournir un ou plusieurs services tels que, la messagerie, les noms de domaine, l'attribution d'adresses IP, l'accès à des répertoires de fichiers... Ces services sont « consommés » par d'autres ordinateurs ayant un accès direct par un réseau local ou indirect, par un extranet ou Internet, et qui agissent en tant que clients.

Serveur DNS ou serveur de nom

Serveur utilisé pour héberger les logiciels et les données nécessaires à la mise en correspondance des adresses IP et des noms de domaines pour les ordinateurs sous son autorité et les ressources Internet. Un serveur DNS remplit deux fonctions principales :

— traduire en adresse IP le nom des serveurs dans son périmètre d'autorité

— transmettre la demande à un serveur DNS ayant autorité dans le cas contraire

Il existe trois catégories de serveurs DNS, primaires, secondaires et récursifs.

Serveur racine ou serveur de noms de la racine

Le serveur racine est un serveur DNS qui répond aux requêtes qui concernent les noms de domaine de premier niveau (*top-level domain*, TLD) et qui les redirige vers le serveur DNS de premier niveau concerné. C'est le point de départ de l'arborescence hiérarchique des noms de domaines.

Serveur primaire

L'un des trois rôles particuliers affectés à un serveur DNS.

Un serveur est dit primaire d'une zone quand il obtient les informations de cette zone dans un fichier de configuration. Ce dernier fichier est écrit par un administrateur.

Le serveur primaire est « autoritaire » sur la zone.

Serveur secondaire

L'un des trois rôles particuliers affectés à un serveur DNS.

Un serveur est dit secondaire d'une zone quand il obtient toutes les informations de cette zone d'un autre serveur dit serveur primaire. Il télécharge le contenu de la zone régulièrement afin de pouvoir prendre le relai du serveur primaire en cas d'incident. Le serveur secondaire est « autoritaire » sur la zone.

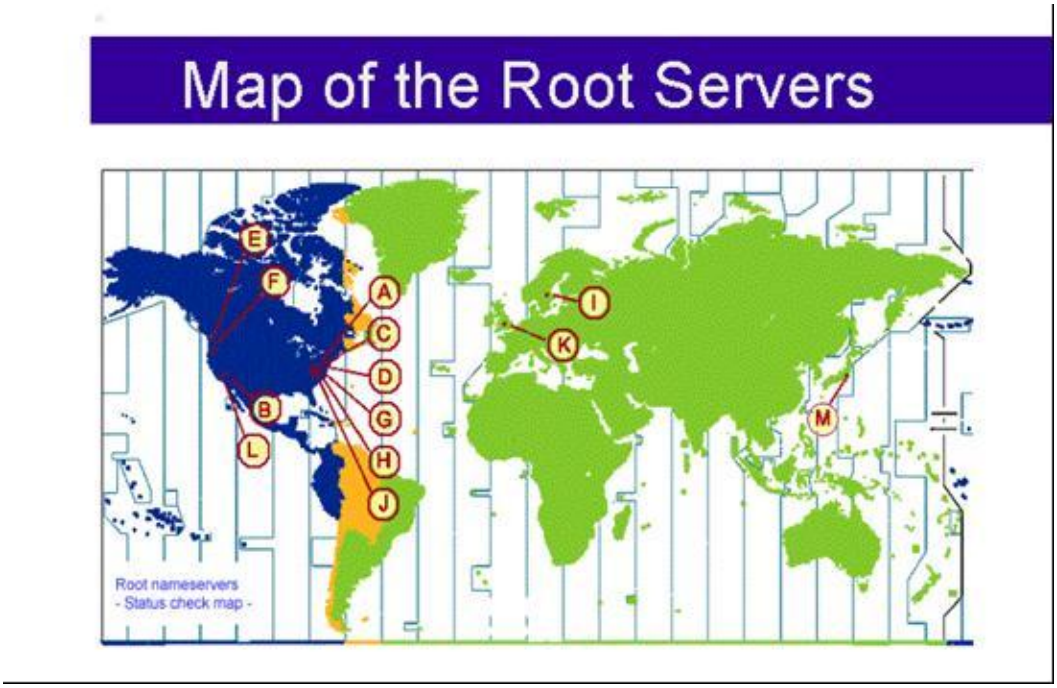
Serveur récursif

L'un des trois rôles particuliers affectés à un serveur DNS

[1] *L'Europe en compte deux, l'un en Suède, l'autre au Royaume-Uni, et le Japon un.*

Un serveur DNS récursif a pour mission d'explorer de façon récursive la hiérarchie des serveurs DNS lorsqu'il ne parvient pas à trouver le serveur DNS primaire faisant autorité pour le nom de domaine recherché.

Source : d'après l'AFNIC



Source : ICANN

SERVEUR	OPÉRATEURS	PAYS
A	VeriSign, Inc.	États-Unis
B	Information Sciences Institute (ISI) Université de Californie du Sud	États-Unis
C	Cogent Communications	États-Unis
D	Université du Maryland	États-Unis
E	NASA)	États-Unis
F	Internet Systems Consortium, Inc.	États-Unis
G	US Department of Defense	États-Unis
H	US Army Research Lab	États-Unis
I	Netnod *(anciennement Autonomica)*	Suède
J	VeriSign, Inc.	États-Unis
K	RIPE NCC	Pays-Bas
L	ICANN	États-Unis
M	WIDE Project	Japon

Source : http://www.root-servers.org et David Fayon
Géopolitique d'Internet – Qui gouverne le monde ?, Ed. Economica 2013.

L'attribution des noms de domaine se fait selon la règle du « premier demandeur, seul servi ». Comme le souligne M. David Fayon dans son livre, **« *cette règle n'est pas sans rappeler la conquête de l'Ouest* *(et le phénomène du* cybersquatting *d'adresses de sites qui pourraient présenter un intérêt dans le but de les revendre par la suite) où le pionnier délimitait le territoire conquis* »**. Il arrive que des conflits surviennent entre cybersquatteurs et sociétés détentrices de marque : ils peuvent être résolus par l'arbitrage ou une procédure judiciaire.

Une industrie du nom de domaine s'est donc créée progressivement. Certains réservent des noms de domaine dans le but d'en tirer profit ultérieurement.

L'ICANN elle-même en récolte directement le fruit : elle ne vend pas une fois pour toutes les noms de domaine, mais en cède l'exploitation à raison d'un certain montant auquel s'ajoute une forme d'abonnement annuel, ce qui lui assure un revenu régulier, et en croissance.

En effet, **le nombre de noms de domaine génériques**, qui était inférieur à 100 en 2012, **va prochainement s'étendre sensiblement** et atteindre le millier : l'ICANN a en effet décidé l'ouverture de nouveaux noms de domaine génériques, au côté des « .com », « .org », « .net » et, plus récemment du « .xxx », extension pornographique qui fait polémique dans certains pays. De nouvelles extensions vont ainsi apparaître, de type économique (« .eco », « .apple », « .music »…), géographique (« .quebec », « .london », « .paris »…) ou linguistique (« .bzh », « .scot »…). Ces nouvelles extensions pourront se faire en recourant aux accents et à des caractères non latins. Le coût d'entrée est de 185 000 dollars par extension, auquel s'ajoutent 25 000 dollars de frais annuels. La procédure d'attribution a abouti fin 2012[1] et a rapporté à l'ICANN 357 millions de dollars cette même année, venant en surplus des 80 millions de dollars de budget de l'ICANN[2]. Certaines extensions pourraient être mises aux enchères quand l'arbitrage n'est pas possible entre deux prétendants, ce qui devrait également être profitable à l'ICANN. Les sociétés obtenant des droits sur certaines extensions pourront toutefois percevoir ensuite des commissions annuelles des sociétés gérant des noms de domaine se terminant par ces extensions, ce qui devrait modifier l'économie des noms de domaine. Le référencement par les moteurs de recherche devra par ailleurs s'adapter à ces nouvelles extensions.

L'ICANN détient de fait un pouvoir important car le système des noms de domaine est la seule partie de l'Internet qui n'est pas décentralisée et car elle coordonne le système des serveurs racine, qui est au cœur du fonctionnement de l'Internet. Il faut aussi souligner **le rôle que joue également la société américaine VeriSign**, elle aussi sous contrat avec le

[1] *Un prochain tour d'attributions de noms de domaine génériques pourrait intervenir d'ici dix ans.*
[2] Cf. *le rapport annuel de l'ICANN 2013.*

Département du commerce américain : elle gère la racine de l'annuaire (serveur A qui a autorité sur les autres serveurs racine, en ce sens que les modifications apportées au serveur A sont répliquées sur les 12 autres), ainsi qu'un autre serveur racine (J), et publie les nouveaux noms de domaine ; elle gère également le registre officiel pour les domaines de premier niveau génériques « .com » et « .net » , le « .org » étant géré par l'ISOC, ce qui assure un financement important à VeriSign comme à l'ISOC.

La gestion des noms de domaine n'est pas une simple activité technique : elle emporte des conséquences importantes, à la fois politiques et économiques.

Ainsi, on ne peut pas dire que l'ICANN, en assignant un **nom de domaine géographique**, décide si une entité géographique est un pays. Mais il est certain que posséder un ccTLD peut représenter un premier pas vers l'indépendance : le Québec a obtenu le « .qc » et la Catalogne a créé en 2006 le « .cat ». Même si elle utilise sur une liste de codes ISO s'appuyant sur les Nations unies[1], la décision de l'ICANN a ici une dimension politique indéniable.

À l'inverse, l'ICANN est en position de priver un pays de l'usage de son extension. C'est ce qui s'est passé durant la guerre en Irak, le « .iq » ayant été coupé à la demande des États-Unis.

Concernant les **noms de domaine génériques**, il apparaît également que l'ouverture de certaines extensions a des implications en termes de contenus véhiculés sur le réseau : c'est ce qui explique la controverse à laquelle a donné lieu l'ouverture de sites pour adultes en « .xxx ».

Les nouvelles extensions de noms de domaine ont également de très fortes implications économiques, non seulement pour les entreprises connectées mais aussi, de manière collatérale, pour les activités qui ne s'exercent pas en ligne et qui peuvent subir une concurrence déloyale de la part de contrefacteurs en ligne. À cet égard, l'ouverture des « .vin » et « .wine » est de nature à gravement compromettre l'activité des viticulteurs européens et suscite de fortes tensions entre l'Union européenne et l'ICANN : des sociétés de l'industrie de l'Internet tentent en effet de capter à leur profit la notoriété et l'image d'une partie du patrimoine national et européen, au mépris notamment des règles de droit qui régissent la propriété intellectuelle, notamment les indications géographiques.

Les projets d'extensions « .vin » et « .wine »

Le débat portant sur les extensions « .vin » et « .wine » est lié à l'**ouverture des noms de domaine de premier niveau générique**. Face à la saturation de la vingtaine existants (« .com », « .org », « .net » …), l'*Internet Corporation for Assigned Names and Numbers* (ICANN), qui est chargée de les gérer, a lancé en juin 2011 un programme destiné à en accroître substantiellement le nombre – aux alentours d'un millier – et à en déléguer la

[1] *Liste tenue à jour par l'ISO 3166-1* Maintenance Agency.

gestion à des opérateurs privés. Les nouvelles règles en la matière permettront à ces derniers de demander auprès de l'ICANN de se voir attribuer n'importe quel suffixe, comme « .avocat », « .sport » ou les « .vin » et « .wine » litigieux.

L'attribution de ces extensions par l'ICANN sera précédée de l'**analyse d'un dossier** décrivant les capacités techniques du futur gestionnaire. Le coût de son dépôt avait été fixé à 185 000 dollars, et celui de la conservation du nom de domaine à 25 000 dollars par an. Un système d'enchères départagera les postulants demandant un suffixe identique.

Avec les nouvelles règles, l'achat d'un nom de domaine de premier niveau par un opérateur lui donnera également la **propriété de tous les noms de domaine de second niveau** liés à celui-ci[1]. Par exemple, l'acquisition de l'extension « .vin » permettrait de se voir attribuer les noms de domaine www.bourgogne.vin ou www.champagne.vin, et de les conserver ou de les revendre à des tiers.

Sur les 2 000 dossiers déposés à l'ICANN pour ouvrir de nouveaux noms de domaine de premier niveau, **quatre sont directement liés au secteur du vin**. Trois sociétés (respectivement américaine, irlandaise et de Gibraltar) ont demandé l'extension « .wine », et une quatrième (américaine) a demandé l'extension « .vin ». Or, leurs dossiers ne contiennent aucune protection des indications géographiques associées au secteur, et les sociétés ont annoncé qu'elles procèderaient à une vente aux enchères des noms de domaine de second degré associés.

Il résulte de l'ouverture non encadrée de ces extensions des **risques, tant pour les professionnels que pour les consommateurs**, qui ont été rapidement pointés par la Confédération nationale des producteurs de vins et eaux-de-vie de vin à appellations d'origine contrôlée (CNAOC) : détournement de notoriété des appellations, *cybersquatting*, spéculation, développement de la contrefaçon, tromperie du consommateur…

Concrètement, en effet, des sociétés commerciales pourraient être tentées de s'attribuer les noms de domaine www.bordeaux.vin et www.bordeaux.wine, par exemple, contraignant ensuite le Conseil interprofessionnel du vin de Bordeaux à les leur racheter au prix qu'elles auront fixé. Par ailleurs, l'internaute français surfant sur le site www.bordeaux.vin et croyant y trouver une information officielle sur les vins de la région pourrait être redirigé vers le site d'une société commerciale qui pourrait n'avoir même aucun rapport avec le secteur du vin.

D'influence américaine, le système d'enregistrement des noms de domaine mis en œuvre par l'ICANN prévoit certes des garde-fous pour les marques, mais **aucune protection pour les appellations géographiques**. Spécifiquement français à l'origine et limité au secteur du vin, ce dernier régime de protection a été ensuite élargi à l'ensemble de l'Union européenne et à tous les secteurs agricoles. Il marque donc une différence quasi philosophique d'approche avec les États-Unis, attachés non pas à l'origine des produits mais à leur licence d'exploitation, divergence que l'on retrouve d'ailleurs dans les négociations en cours sur un accord transatlantique.

Certes, l'**accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce** (ADPIC)[2], entré en vigueur le 1er janvier 1995 et constituant le traité le plus complet en matière de propriété intellectuelle, protège les indications géographiques, y compris les appellations d'origine. Aussi la France a sollicité de l'Organisation mondiale du commerce, dans le cadre duquel il a été négocié et conclu, son application. Cependant, ce traité ne couvre pas les noms de domaine, ce qui soulève d'ailleurs la question d'une inégalité de traitement entre commerce et e-commerce, ou entre *offline* et *online*.

La **CNAOC et la Fédération européenne** regroupant ses homologues des autres États membres (EFOW) sont intervenues auprès de leurs gouvernements respectifs en leur

[1] *L'attribution des noms de domaine de second niveau en .fr (comme www.cognac.fr) relève quant à elle de l'Association française pour le nommage Internet en coopération (AFNIC).*

[2] *Ou* Agreement on Trade-Related Aspects of Intellectual Property Rights *(TRIPS) en anglais.*

demandant de déclencher une « alerte », mécanisme prévu par l'ICANN pour signaler les difficultés posées par un dossier. Elles ont par ailleurs saisi les trois commissaires européens en charge de la société numérique, de l'agriculture et du marché intérieur (respectivement Mme Neelie Kroes, M. Dacian Ciolos et M. Michel Barnier) pour leur demander d'intervenir auprès de l'ICANN. Mme Kroes a alors écrit à deux reprises à la société américaine pour soulever les problèmes posés.

La **France** s'est rapidement investie dans le ce dossier, et a cherché à sensibiliser les instances européennes compétentes des risques qu'il faisait peser sur la filière vin, mais aussi, plus largement, sur toutes les appellations d'origine. S'adressant à la Commission européenne, le ministre de l'agriculture, M. Stéphane Le Foll, a fait de la reconnaissance et de la protection de celles-ci « *une priorité pour la France* », tout comme « *la mise en place d'une procédure visant la protection des indications géographiques* ». Il a depuis été rejoint par le ministre des affaires étrangères, M. Laurent Fabius, mais aussi par la secrétaire d'État chargée du numérique, Mme Axelle Lemaire.

Le **comité consultatif gouvernemental (GAC)** de l'ICANN, sur l'insistance notamment de la France, du Luxembourg, de l'Espagne – particulièrement mobilisée – et de la Commission européenne, a émis de façon consensuelle des réserves sur l'attribution des extensions « .vin » et « .wine » en avril 2013, et demandé à ce qu'un réel dialogue s'instaure. Dans un nouvel avis de juillet de la même année, il donnait 30 jours aux sociétés candidates et au secteur pour trouver une solution, qui ne s'est pas fait jour. Enfin, en novembre, il proposait au bureau de l'ICANN de porter une extrême attention à la complexité juridique et politique constituant l'arrière-plan du dossier.

Le 22 mars dernier, et de façon assez inattendue, le comité responsable de l'ouverture de nouveaux noms de domaine gTLD (le NGPC) se prononçait en faveur d'une délégation sans condition des « .vin » et « .wine ». Le 4 avril, l'**ICANN** décidait une nouvelle fois de **reporter de 60 jours** (donc **d'ici le 3 juin**) sa décision quant à cette attribution aux sociétés candidates, afin de trouver une solution satisfaisante avec le secteur du vin. Son nouveau président, M. Fadi Chehadé, s'est engagé à ce qu'il n'y ait pas de délégation sans accord à ce terme. Auditionné fin février par la mission commune d'information, ce dernier avait estimé que « *ce n'[était] pas au conseil d'administration de l'ICANN de trancher* », indiquant qu'il avait « *invité toutes les parties dans [son] bureau* » et s'efforçait de « *faciliter les discussions entre elles en créant un espace de dialogue* ».

Dans la foulée, des **recours contre l'ICANN** étaient déposés par la Commission européenne, les gouvernements français, espagnol et anglais, la CNAOC, l'EFOW, le CIVC, le CIVB et le bureau national interprofessionnel de Cognac (BNIC). Ils demandent un système de vérification des appellations d'origine obligatoire pour toute commercialisation d'extensions de sites Internet, et assurent qu'ils soutiendront et promouvront les « .vin » et « .wine » dès lors qu'un tel régime sera établi. À défaut, ils menacent d'organiser une grande campagne de boycott de ces noms de domaine et de demander leur blocage sur le territoire de l'Union européenne.

Si l'Union européenne a été rejointe dans son combat par les pays producteurs de vin d'Amérique latine et par les États francophones, formant un groupe de 34 pays, elle doit composer avec la **forte pression exercée par les États-Unis** sur le dossier. Réunis avec deux autres pays (Australie et Nouvelle-Zélande) dans un groupe plaidant pour une ouverture générale des noms de domaine de premier niveau, ils exercent une très forte influence sur les sociétés candidates et ont écrit à l'ICANN pour lui demander de procéder immédiatement à la délégation des extensions litigieuses.

Le 3 juin, date-limite fixée par l'ICANN pour obtenir un accord, les trois candidats au « .wine » et le secteur n'ont **pas réussi à s'entendre**. Selon les représentants de la CNAOC, ceci est à mettre au compte de l'influence américaine sur ces trois opérateurs. Ceux-ci entendraient réaliser d'ici peu une enchère entre eux, vraisemblablement remportée par une société américaine refusant de protéger les indications géographiques et souhaitant vendre

aux enchères tous les noms, y compris d'AOC.

Les gouvernements n'ayant pas réussi non plus à trouver un consensus lors de la dernière réunion de l'organisation du 22 au 26 juin à Londres, il n'y a **plus d'obstacle désormais à une délégation** des noms de domaine en « .vin » et « .wine ». Cela malgré la mobilisation très forte de la France, par la voix de la secrétaire d'État en charge de l'économie numérique, Mme Axelle Lemaire - soutenue par l'Espagne, l'Italie, le Portugal et la Commission européenne -, qui demandait la suspension de leur attribution.

La CNAOC a annoncé qu'elle **engagerait une vaste campagne visant à dissuader** les vignerons d'acheter des noms de domaine en « .vin » et « .wine », et les consommateurs de se rendre sur ces sites. Souhaitant élargir le débat à d'autres secteurs également concernés, la confédération entend par ailleurs demander aux gouvernements de mettre en place des plateformes pour identifier les sites qui seront en infraction avec la réglementation communautaire et de prévoir des mesures pour les neutraliser.

L'Italie, qui assurera la présidence du Conseil de l'Union le 1er juillet, s'est engagée à considérer la **question comme de la plus haute importance** au cours du prochain semestre, et s'est déclarée déterminée à prendre une initiative forte en la matière.

Ce dossier illustre combien **des décisions de caractère apparemment technique prises par les organes de gouvernance de l'Internet peuvent avoir des implications non seulement économiques mais culturelles et sociétales, en un mot politiques**. Sans doute aussi la maîtrise du répertoire des adresses et noms offre-t-elle des facilités en matière de renseignement : M. Milton Mueller, professeur à l'université de Syracuse que la délégation de votre mission a pu rencontrer aux États-Unis, a indiqué que les noms de domaine étaient utilisés par le gouvernement américain pour des motifs de vérification de l'identité des personnes enregistrées, d'application de la loi, notamment en matière de droits d'auteur, voire de surveillance[1].

c) L'ICANN, objet juridique non identifié qui prospère sous le seul contrôle des États-Unis

Dotée donc de pouvoirs aux implications considérables, **l'ICANN reste pourtant un objet juridique non identifié**.

L'ICANN se définit comme une société à but non lucratif d'intérêt public (« *not-for-profit public-benefit corporation* ») de droit californien ; au titre de ce statut hybride, elle n'a ni actionnaires ni associés.

Son lien avec le gouvernement américain est double :

– une déclaration d'engagements, dite *Affirmation of committments* (AoC), signée avec le Département du commerce américain en 2009[2] ;

– un contrat par lequel le Département du commerce confie à l'ICANN les fonctions assumées avant 1998 par l'IANA (*Internet Assigned Number Authority*) sous la responsabilité de son fondateur Jon Postel : attribuer les noms de domaine de premier niveau (donc gérer la racine),

[1] *L'ICANN tient à jour une base de données WHOIS de la zone racine qui contient les informations de contact réelles et vérifiées de tous les opérateurs de registre TLD.*

[2] *Et qui se substitue au précédent* Memorandum of Understanding *initialement signé en 1998 et prolongé deux fois.*

attribuer les adresses IP et les numéros de systèmes autonomes (ASN) aux registres Internet régionaux, et définir les paramètres des protocoles Internet (liste des numéros de ports…) en collaboration avec l'IETF.

L'infographie ci-dessous, élaborée par l'ICANN, permet de mieux visualiser ces fonctions de l'IANA.

ICANN

FONCTIONS DE L'IANA : LES BASES

Lorsque vous voulez vous rendre sur un site Web, soit vous tapez ou vous copiez le **nom de domaine** de ce site dans la barre d'adresse de votre navigateur, soit vous cliquez sur un lien html.

Ce nom de domaine est envoyé à un serveur, qui le traduit en une série de chiffres (l'adresse de protocole Internet, ou **adresse IP** pour pouvoir acheminer votre requête jusqu'à l'emplacement physique du site Web. ***Tout cela se passe en un clin d'œil.***

Ces noms de domaine et chiffres sont appelés des « **identificateurs uniques** » et suivent un ensemble standard de **paramètres de protocole** qui assurent que les ordinateurs peuvent communiquer et se comprendre entre eux.

Ils font partie des **fonctions de l'IANA**, fonctions qui sont gérés par l'**ICANN**, la **Société pour l'attribution des noms de domaine et des numéros sur Internet**.

Elles ne se limitent pas à la navigation sur Internet : elles vous permettent aussi, entre autres, d'envoyer du courrier électronique ou de sauvegarder vos photos dans le cloud.

1

HISTORIQUE

Internet
Assigned
Numbers
Authority

Cet acronyme a été créé à l'époque où Jon Postel était responsable de la gestion de l'ARPANET, un réseau du ministère de la défense américain financé par le gouvernement des États-Unis. On disait à l'origine The IANA en anglais, car ses fonctions étaient assurées par une seule personne.

Depuis, l'Internet n'a cessé de se développer. Les fonctions de l'IANA ne sont plus gérées par une seule personne : aujourd'hui, elles sont gérées par l'ICANN.

2

LES FONCTIONS DE L'IANA EN LIGNE

Coordonner les identificateurs uniques qui permettent le bon fonctionnement d'Internet est une fonction importante de l'IANA.

Lorsqu'un ordinateur ou un appareil se connecte à un réseau, il doit savoir comment communiquer avec les autres appareils qui sont en ligne. Cette communication entre appareils est rendue possible par les normes mises en place et par le fait que chaque appareil possède un identificateur unique.

3

NOMS ET NUMÉROS

L'Internet est conçu pour être intuitif et facile à utiliser. Puisqu'elle assure les fonctions de l'IANA, l'ICANN coordonne les noms de domaine, comme par exemple www.icann.org. Chaque nom de domaine renvoie à une adresse IP spécifique.

icann.org } NOM DE DOMAINE

192.0.32.7 } ADRESSE IP

4

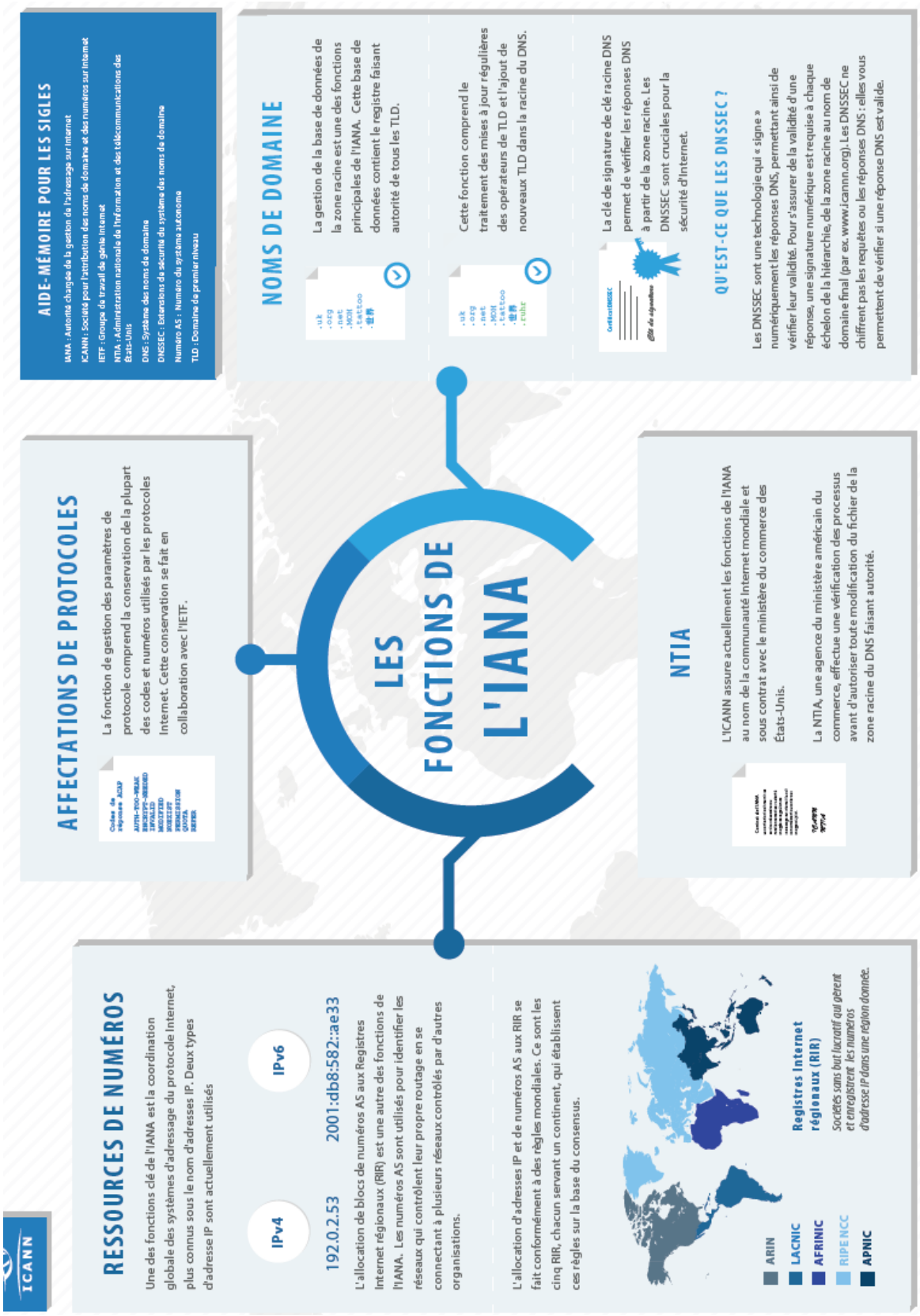
L'ÉCOSYSTÈME INTERNET

Bien qu'elles soient importantes pour l'écosystème Internet, les fonctions de l'IANA ne sont qu'une partie de cet écosystème. D'autres acteurs jouent un rôle essentiel dans le fonctionnement d'Internet.

L'**ICANN**, en assurant les fonctions de l'IANA, coordonne les identificateurs uniques.

L'**ICANN** remplit ces fonctions en vertu d'un contrat conclu avec la **NTIA**.

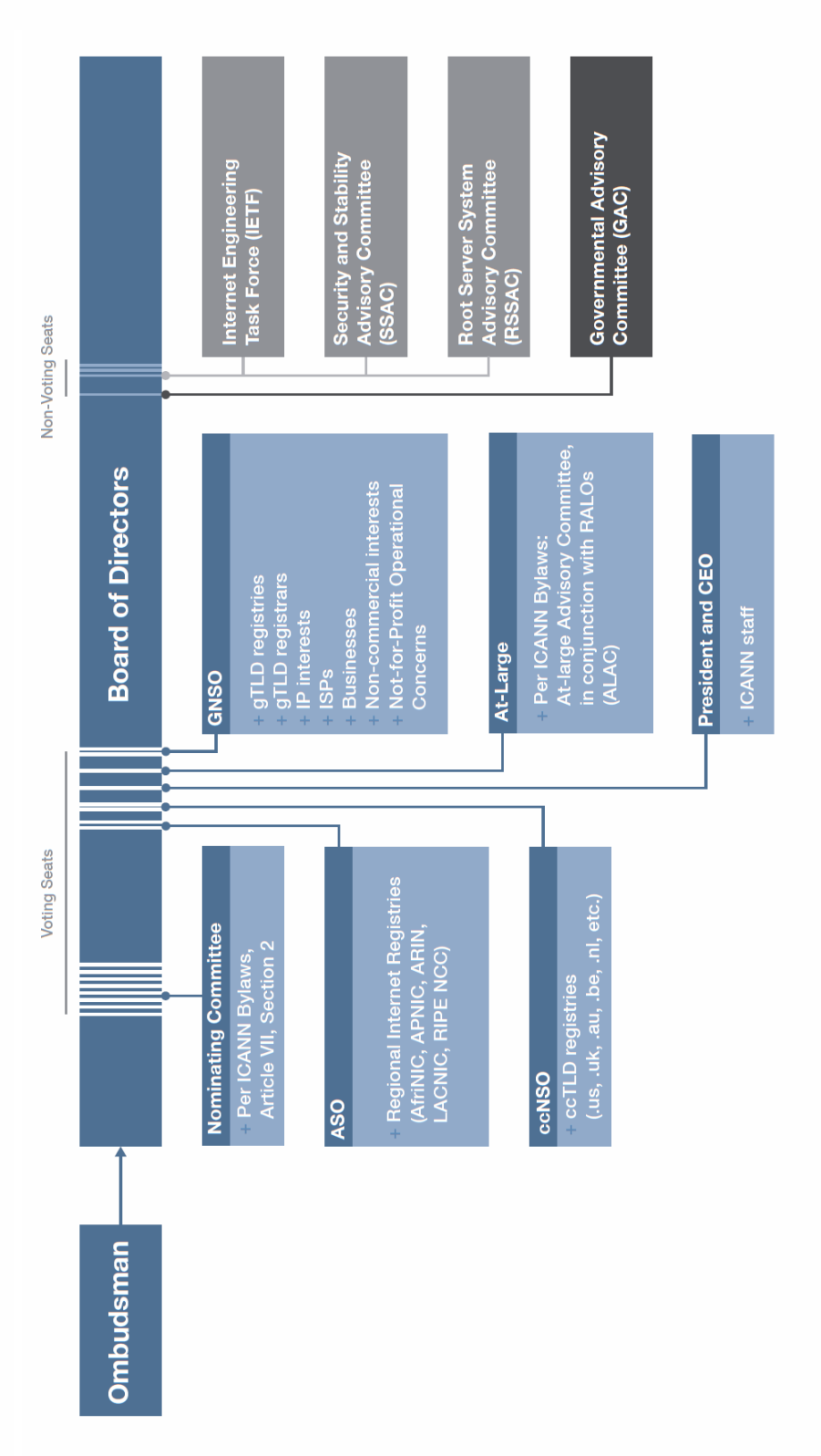
Verisign édite et publie le fichier de la zone racine faisant autorité.


AIDE-MÉMOIRE POUR LES SIGLES
IANA : Autorité chargée de la gestion de l'adressage sur Internet
ICANN : Société pour l'attribution des noms de domaine et des numéros sur Internet
IETF : Groupe du travail du génie Internet
NTIA : Administration nationale de l'information et des télécommunications des États-Unis
DNS : Système des noms de domaine
DNSSEC : Extensions de sécurité du système des noms de domaine
Numéro AS : Numéro du système autonome
TLD : Domaine de premier niveau
NOMS DE DOMAINE
La gestion de la base de données de la zone racine est une des fonctions principales de l'IANA. Cette base de données contient le registre faisant autorité de tous les TLD.
Cette fonction comprend le traitement des mises à jour régulières des opérateurs de TLD et l'ajout de nouveaux TLD dans la racine du DNS.
La clé de signature de clé racine DNS permet de vérifier les réponses DNS à partir de la zone racine. Les DNSSEC sont cruciales pour la sécurité d'Internet.
QU'EST-CE QUE LES DNSSEC ?
Les DNSSEC sont une technologie qui « signe » numériquement les réponses DNS, permettant ainsi de vérifier leur validité. Pour s'assurer de la validité d'une réponse, une signature numérique est requise à chaque échelon de la hiérarchie, de la zone racine au nom de domaine final (par ex. www.icann.org). Les DNSSEC ne chiffrent pas les requêtes ou les réponses DNS : elles vous permettent de vérifier si une réponse DNS est valide.
LES FONCTIONS DE L'IANA
AFFECTATIONS DE PROTOCOLES
La fonction de gestion des paramètres de protocole comprend la conservation de la plupart des codes et numéros utilisés par les protocoles Internet. Cette conservation se fait en collaboration avec l'IETF.
NTIA
L'ICANN assure actuellement les fonctions de l'IANA au nom de la communauté Internet mondiale et sous contrat avec le ministère du commerce des États-Unis.
La NTIA, une agence du ministère américain du commerce, effectue une vérification des processus avant d'autoriser toute modification du fichier de la zone racine du DNS faisant autorité.
RESSOURCES DE NUMÉROS
Une des fonctions clé de l'IANA est la coordination globale des systèmes d'adressage du protocole Internet, plus connus sous le nom d'adresses IP. Deux types d'adresse IP sont actuellement utilisés
IPv4
192.0.2.53
IPv6
2001:db8:582::ae33
L'allocation de blocs de numéros AS aux Registres Internet régionaux (RIR) est une autre des fonctions de l'IANA. Les numéros AS sont utilisés pour identifier les réseaux qui contrôlent leur propre routage en se connectant à plusieurs réseaux contrôlés par d'autres organisations.
L'allocation d'adresses IP et de numéros AS aux RIR se fait conformément à des règles mondiales. Ce sont les cinq RIR, chacun servant un continent, qui établissent ces règles sur la base du consensus.
ARIN
LACNIC
AFRINIC
RIPE NCC
APNIC
Registres Internet régionaux (RIR)
Sociétés sans but lucratif qui gèrent et enregistrent les numéros d'adresse IP dans une région donnée.

L'ICANN est dirigée par un conseil d'administration (*board*) qui prend les décisions et **qui comprend 20 membres**, dont le président – M. Fadi Chehadé en ce moment – sélectionné par le *board*. Ces membres sont, pour les uns, **des représentants des organisations de soutien de l'ICANN** : deux membres pour celle en charge des noms de domaine génériques *(Generic Names Supporting Organization* – GNSO[1]), deux pour celle en charge des noms de domaine géographiques (*Country Code Names Supporting Organization* – ccNSO), et deux pour celle représentant les cinq registres Internet régionaux qui gèrent les adresses IP (*Address Supporting Organization* – ASO). Depuis 2001, siège aussi au *board* un représentant de l'ensemble des parties prenantes (comité *« At-Large »*, représentant plus de 160 structures de diverses origines géographiques[2]).

[1] *Le GNSO est composé de deux chambres : dans la première, les registres (gestionnaires d'extensions) et les* registrars *(bureaux d'enregistrement permettant d'acquérir des noms de domaine dans ces extensions) ; dans l'autre, des représentants de l'industrie, des fournisseurs d'accès, du secteur de la propriété intellectuelle et des entités non commerciales (comme la Croix Rouge). C'est le GNSO qui a initié en 2007 le processus conduisant à la libéralisation de la racine de l'Internet, qui rend désormais possible la création de nouvelles extensions.*

[2] *En France, il y a trois structures* At-Large *: le Chapitre français de l'*Internet Society*, l'association e-senior et* Together against cybercrime*. En Europe, au titre du regroupement régional, a été créé l'*European At-Large Organization *(EURALO) en 2007.*


Ombudsman
Board of Directors
Non-Voting Seats
Voting Seats
Internet Engineering Task Force (IETF)
Security and Stability Advisory Committee (SSAC)
Root Server System Advisory Committee (RSSAC)
Governmental Advisory Committee (GAC)
GNSO
+ gTLD registries
+ gTLD registrars
+ IP interests
+ ISPs
+ Businesses
+ Non-commercial interests
+ Not-for-Profit Operational Concerns
At-Large
+ Per ICANN Bylaws: At-large Advisory Committee, in conjunction with RALOs (ALAC)
President and CEO
+ ICANN staff
Nominating Committee
+ Per ICANN Bylaws, Article VII, Section 2
ASO
+ Regional Internet Registries (AfriNIC, APNIC, ARIN, LACNIC, RIPE NCC)
ccNSO
+ ccTLD registries (.us, .uk, .au, .be, .nl, etc.)

Les **critères de nomination** de ces directeurs membres du *board* sont précisés dans les statuts de l'ICANN (*Bylaws*), dont un extrait est reproduit ci-dessous : ils privilégient **la compétence technique, l'intégrité, l'objectivité, l'intelligence, le jugement, l'ouverture d'esprit et la capacité à décider en groupe**. L'exercice de la fonction de directeur se faisait à titre bénévole, elle donne désormais lieu à défraiement ; seul le président de l'ICANN est officiellement rémunéré.

Critères pour la sélection des directeurs de l'ICANN

Les directeurs de l'ICANN doivent être :

1. des personnes réputées pour leur intégrité, objectivité et intelligence, ainsi que pour leur bon jugement, ouverture d'esprit et leur capacité confirmée dans la prise de décision au sein d'un groupe ;

2. des personnes ayant intégré la mission de l'ICANN, l'impact potentiel de ses décisions sur l'ensemble de la communauté Internet, et prêtes à s'engager en faveur de la réussite de l'ICANN ;

3. des personnes qui formeront la plus large diversité culturelle et géographique au Conseil d'administration, conformément aux autres critères soulignés dans cette section ;

4. des personnes, qui, dans l'ensemble, sont familières avec le fonctionnement des registres et bureaux d'enregistrement de gTLD ; avec les registres de ccTLD ; avec les registres d'adresses IP ; avec les normes et protocoles techniques de l'Internet ; avec les procédures d'élaboration de politiques, les coutumes juridiques et l'intérêt public ; avec la grande variété d'utilisateurs commerciaux, individuels, académiques et non-commerciaux de l'Internet ;

5. des personnes désireuses d'agir de manière bénévole, sans autre compensation que le remboursement de certains frais ; et

6. des personnes capables de travailler et de communiquer en anglais à l'écrit et à l'oral.

Source : Statuts de l'ICANN (article VI – section 3)

En outre, **huit membres dotés du droit de vote sont directement sélectionnés par le Comité de nomination de l'ICANN**, lequel se compose de membres non votants, désignés par le *board* ou les comités consultatifs de l'ICANN, et de membres votants, désignés par des parties prenantes participant à l'ICANN. Il est paradoxal que le **comité de sélection de membres du *board* soit lui-même composé de membres nommés par ce même *board* !** Le détail de la composition de ce comité de sélection est précisé ci-dessous, dans un extrait des statuts de l'ICANN. On remarquera que le chapitre des entreprises (*Business constituency*) se distingue par son privilège consistant à pouvoir nommer deux membres à ce comité ; selon les informations fournies par M. Philippe Lemoine, lors de son audition par votre mission, ce chapitre représentant les entreprises compte 53 multinationales, dont 40 américaines qui ne lésinent pas sur les moyens de lobbying.

Composition du Comité de nomination de l'ICANN

Le comité de nomination se compose des personnes suivantes :

1. un président sans droit de vote, nommé par le conseil d'administration de l'ICANN ;

2. un président élu sans droit de vote, nommé par le conseil d'administration de l'ICANN en tant que conseiller sans droit de vote ;

3. un agent de liaison sans droit de vote nommé par le comité consultatif du système de serveurs racine établi par l'Article XI de ces statuts ;

4. un agent de liaison sans droit de vote nommé par le comité consultatif pour la sécurité et la stabilité établi par l'article XI de ces statuts ;

5. un agent de liaison sans droit de vote nommé par le comité consultatif gouvernemental ;

6. sous réserve des dispositions de l'article de transition de ces statuts, cinq délégués dotés d'un droit de vote, sélectionnés par le comité consultatif *At-Large* établi par l'article XI de ces statuts ;

7. les délégués dotés d'un droit de vote du Comité de nomination seront sélectionnés par l'Organisation de soutien aux politiques des noms génériques suivant ce qui est établi dans l'article X de ces statuts ;

a. un délégué du groupe multipartite des registres ;

b. un délégué du groupe multipartite des bureaux d'enregistrement ;

c. deux délégués du regroupement des utilisateurs commerciaux d'Internet, l'un représentant les utilisateurs commerciaux et l'autre représentant les grandes entreprises ;

d. un délégué du collège regroupant les fournisseurs de services Internet ;

e. un délégué du regroupement de la propriété intellectuelle ; et

f. un délégué des groups des consommateurs et de la société civile, sélectionnés par le regroupement des utilisateurs non commerciaux.

8. un délégué doté d'un droit de vote sélectionné par les entités suivantes :

a. le Conseil de l'Organisation de soutien aux politiques des noms de pays (CCNSO), établie par l'article IX de ces statuts ;

b. le conseil des organisations de soutien aux politiques d'adressage établi par l'article VIII de ces statuts ;

c. le groupe de travail de l'ingénierie Internet ; et

d. le groupe de liaison technique de l'ICANN, établi par l'article XI-A de ces statuts ; et

9. un président adjoint sans droit de vote, qui peut être nommé par le président, à sa seule discrétion, pour exercer sa fonction pendant une partie ou tout le mandat du président. Le président adjoint ne peut pas être une personne autrement membre du même comité de nomination. Le président adjoint assiste le président dans l'exercice de sa fonction, mais n'agit en aucun cas, temporairement ou autre, à sa place.

Source : statuts de l'ICANN (article VII – section 2).

Outre ces 16 membres – incluant le président – qui ont le droit de vote, **quatre siègent au *board* sans droit de vote** : un représentant de l'IETF et trois membres qui assurent la liaison avec les trois comités consultatifs que sont le *Root Server System Advisory Committee* (RSSAC), le *Security and Stability Advisory Committee* (SSAC) et le *Governmental Advisory Committee* (GAC).

L'ICANN défend une approche inclusive qui traite le secteur public, le secteur privé et les experts techniques comme des pairs. Son **organisation** lui paraît illustrer ce modèle **multi-parties prenantes** (*multistakeholders*) :

Les États participent à l'ICANN puisqu'ils sont représentés par le biais du *Govermental Advisory Committee*, le GAC, au sein duquel siègent aujourd'hui près de 140 pays, et notamment l'Union européenne. Mais ce **comité** est **purement consultatif**, quand d'autres parties prenantes sont dotées, elles, d'un droit de vote au sein du *board* de l'ICANN. Car, **même si l'esprit de l'Internet refuse les procédures de vote, le *board* de l'ICANN fonctionne malgré tout de manière assez formelle**, avec 16 membres dotés d'un droit de vote et 4 autres qui en sont privés.

La composition du *board* fonctionne largement par cooptation, comme l'a dénoncé devant votre mission M. Louis Pouzin : « *ce sont pratiquement ceux qui en sortent qui décident de ceux qui y entrent ! Ce sont les mêmes têtes qui tournent entre l'ICANN, l'Internet Society (ISOC), et les différents comités qui gravitent plus ou moins autour - ceux qui gèrent les noms de domaine, les protocoles, ... Il s'agit de la génération qui a suivi les pionniers.* ». Me Iteanu, avocat à la Cour d'appel de Paris et président d'honneur de l'Internet Society France, passé de l'ISOC à l'ICANN, l'a confirmé à demi-mot.

Il a aussi pointé du doigt les intérêts privés qui sont présents au sein de l'ICANN : « *quand j'étais au comité de l'ICANN, je pouvais connaître à la seconde le cours de bourse de Cisco…. Les entreprises américaines ont pénétré l'ICANN.* »

En effet, **le *board* n'est pas à l'abri des conflits d'intérêt**, les procédures mises en place par l'ICANN pour l'éviter n'étant pas assez strictes : ce *board* est censé valider un certain nombre de décisions prises par les organisations de support qui traitent de la préparation des décisions politiques de l'ICANN. Or, le *board* de l'ICANN est constitué de personnes qui viennent de ces communautés. M. David Martinon a donné à votre mission l'exemple suivant : « *Le GNSO, par exemple, est une instance qui a vocation à représenter toutes les personnes impliquées dans le* business model *des noms de domaine. On retrouve donc forcément au* board *un certain nombre de personnes qui dirigent des sociétés, ou qui bénéficient d'investissements de sociétés qui présentent des projets jugés par le* board. »

Même s'il est possible de contester les décisions du *board*, **le système de recours reste très insatisfaisant**. Un médiateur réputé neutre - *ombudsman* -, mais nommé par le *board*, règle les différends, en cas de

plainte d'un membre de la communauté ICANN au sujet d'une mesure ou d'une absence de mesure émanant d'un membre du personnel, des organes ou du *board*. Les statuts[1] prévoient une procédure plus largement ouverte à toute personne ou entité touchée par une action ou inaction de l'ICANN : il est possible de demander un réexamen de cette action ou inaction ; mais ce réexamen est confié à un comité du *board* composé d'au moins trois de ses membres ! Selon M. David Martinon, sur les 70 ou 80 demandes déposées, une seule a été acceptée, ce qu'il interprète ainsi : « *on peut en tirer deux conclusions : soit le* board *de l'ICANN travaille merveilleusement bien et sans défaut, soit il n'a pas envie d'être redevable, ni de reconnaître ses erreurs !* » La possibilité d'une révision indépendante des actions du conseil d'administration est toutefois prévue : en ce cas, la révision est confiée à un panel de révision indépendant ne comprenant aucun membre de l'ICANN. Mais cette solution d'arbitrage international est très coûteuse (500 000 dollars d'après les informations transmises par M. David Martinon à votre mission) et les frais sont aux dépens du perdant, ce qui peut faire hésiter un pays déjà endetté ou, plus encore s'il est en développement, à déposer une plainte. C'est sans doute pourquoi cette solution du panel n'est pour l'heure pas très rodée : M. Martinon a indiqué à votre mission qu'il y en avait eu trois récemment, et que l'ICANN n'avait pas correctement travaillé, ayant été prise de cours et mise en contradiction face à ses propres règles.

Par ailleurs, **le fonctionnement de l'ICANN apparaît globalement opaque**. Conformément à la déclaration d'engagements signée avec le Département du commerce américain, l'ICANN affiche pourtant des pratiques transparentes : chacun est invité à participer, des forums en ligne sont organisés, des réunions publiques se tiennent régulièrement, les décisions du *board* sont accessibles et le suivi de leur mise en œuvre est ouvertement assuré. Mais, comme l'a souligné devant votre mission **Me Iteanu**, le foisonnement des documents, la multiplicité d'acronymes et la technicité des sujets rendent en fait son action largement opaque pour l'internaute non expert.

On peut aussi s'interroger sur la redevabilité (*accountability*) de l'ICANN, qui figure aussi parmi les engagements pris en 2009 avec le Département du commerce américain.

[1] *Article IV, sections 2 et 3.*

Éclairages sur la notion de « redevabilité »

Traduction encore maladroite du terme anglophone *accountability*, le mot « redevabilité » demeure pour beaucoup un terme flou du débat international. (…) Il est donc nécessaire de mieux comprendre les difficultés de traduction qui entourent le terme anglo-saxon *accountability* (…). En français (et dans bien d'autres langues), l'emploi du terme de « redevabilité » pour traduire l'*accountability* est le résultat d'un espace laissé en partie vide entre deux expressions avec lesquelles il est souvent confondu, mais qui ne suffisent pas à elles seules à assurer une traduction pertinente :

– le premier terme (…) est : « responsabilité ». C'est bien souvent ce terme qui traduit aujourd'hui, à la fois en français, en suédois, et dans plusieurs autres langues européennes, l'*accountability* anglo-saxonne. La « responsabilité » renvoie à l'idée de l'engagement d'un acteur vis-à-vis d'une partie prenante extérieure. Pourtant, le terme de « redevabilité » se distingue de la seule « responsabilité » en y ajoutant une exigence supplémentaire : celle de donner à voir que la responsabilité a été assumée et que les engagements ont été tenus (Wenar, 2006). La redevabilité peut ainsi se définir comme étant l'obligation de rendre compte de l'exercice d'une responsabilité ;

– le deuxième terme qui encadre la notion de redevabilité est celui de « reddition de comptes », qui sert lui aussi parfois de traduction au terme *accountability*. (…) Cependant, cette notion renvoie généralement à l'idée d'une redevabilité limitée à une dimension très restreinte de l'action engagée – avant tout financière – ne donnant généralement pas à voir l'ensemble des engagements qui définissent la responsabilité d'un acteur.

Le terme de redevabilité, aujourd'hui largement appliqué au domaine du développement, navigue donc entre un concept très large de « responsabilité », outil de réflexion avant tout utile à la science politique et peinant à trouver une traduction opérationnelle, et une expression plus opérationnelle de reddition de compte, trop restreinte à un type spécifique d'information.

En dehors du simple enjeu de traduction, il est également utile de poser quelques principes qui permettent de définir la redevabilité par ce qu'elle n'est pas.

La « redevabilité » ne se décrète pas seule : elle naît d'une relation avec un acteur extérieur.

La redevabilité se distingue en effet du simple exercice de « transparence » : la transparence est avant tout conçue comme un « état », consistant à rendre publiques les informations relatives à l'organisation, la stratégie, l'action et les résultats d'un organisme public ou privé. La redevabilité, quant à elle, implique nécessairement une relation dynamique avec une partie prenante extérieure et n'a de sens qu'en réponse à une demande. Elle ne peut donc se concevoir qu'à travers l'identification du type d'acteurs auprès duquel nous sommes redevables. Le détour par la langue suédoise est à ce titre intéressant. Elle distingue aujourd'hui deux traductions du terme de redevabilité, l'une définissant l'agent devant être redevable (*ansvarsskyldighet*), l'autre définissant l'agent exigeant cette redevabilité (*ansvarsutkrävande*), montrant bien ainsi l'existence nécessaire d'une relation entre une « offre » et une « demande » de redevabilité. Par ailleurs, contrairement à la notion de transparence, la redevabilité implique que le partenaire ait les moyens de

sanctionner, de manière formelle ou informelle, directe ou indirecte, la mauvaise orientation des stratégies ou l'absence de résultats des actions. (…)

La redevabilité n'est pas ponctuelle ou sélective : elle suppose des outils systématisés d'information et de dialogue.

La redevabilité se distingue d'un simple exercice de « communication » qui sélectionnerait, parmi les informations existantes au sein de l'agence, les actions et les résultats permettant de justifier son action et de renforcer l'adhésion de ses partenaires. La redevabilité implique une systématisation dans la production de l'information et des canaux qui permettent de la diffuser. Elle entraîne donc la mise en place d'un système normé permettant des flux réguliers d'information, sans sélectivité dans le type de résultats présentés, et donnant à voir une certaine exhaustivité des informations produites. (…) Si le renforcement de la redevabilité se distingue d'une pure démarche de communication par la systématisation et la perte de pouvoir sur l'information qu'elle suppose, ces deux démarches visent chacune à renforcer la légitimité des politiques (…).

Source : d'après « Le défi de la « redevabilité » des agences de développement », note méthodologique n°4, Agence française de développement, septembre 2010.

Les engagements de l'ICANN en termes de redevabilité sont formulés dans l'extrait de l'*Affirmation of commitments*, reproduit ci-dessous.

Extrait de l'*Affirmation of commitments* signé en 2009 entre l'ICANN et le Département du commerce américain, relatif à la redevabilité et à la transparence de l'ICANN

Assurer la responsabilité, la transparence et les intérêts des utilisateurs mondiaux d'Internet :

L'ICANN s'engage à maintenir et à améliorer des dispositifs solides en faveur de la contribution du public, de la responsabilité et de la transparence de sorte à assurer que les résultats de ses prises de décisions reflètent l'intérêt public et soient responsables devant toutes les parties prenantes en :

(a) évaluant et améliorant continuellement la gouvernance du conseil d'administration de l'ICANN (Conseil d'administration). Ceci comprend l'évaluation continue de la performance du Conseil d'administration, du processus de sélection du Conseil d'administration, de la mesure dans laquelle la composition du Conseil d'administration satisfait les besoins présents et futurs de l'ICANN, et la considération d'une procédure d'appel concernant les décisions du Conseil d'administration ;

(b) évaluant le rôle et l'efficacité du GAC et son interaction avec le Conseil d'administration et en faisant des recommandations d'amélioration afin de garantir une prise en considération réelle par l'ICANN de la contribution du GAC sur les aspects de politique publique de la coordination technique du DNS ;

(c) évaluant et améliorant continuellement les processus par lesquels l'ICANN recueille les contributions du public (y compris l'explication adéquate des décisions prises et de leur logique) ;

(d) évaluant continuellement la mesure dans laquelle les décisions de l'ICANN sont adoptées, soutenues et acceptées par le public et la communauté d'Internet ; et en

(e) évaluant le processus d'élaboration de politiques pour faciliter les délibérations renforcées au sein de la communauté et l'élaboration de politiques opportunes et efficaces. L'ICANN organisera une révision de son exécution des engagements ci-dessus au moins tous les trois ans, la première révision de la sorte devant être terminée au plus tard le 31 décembre 2010. La révision sera réalisée par des membres bénévoles de la communauté et l'équipe de révision sera constituée et sa composition publiée pour solliciter les commentaires du public. Elle comprendra les membres suivants (ou leurs candidats désignés) : le président du GAC, le président du Conseil d'administration de l'ICANN, le secrétaire adjoint pour les communications et l'informatique du Département du commerce, des représentants des comités consultatifs et organisations de soutien de l'ICANN pertinents et des experts indépendants. Le président du GAC (en consultation avec les membres du GAC) et le président du Conseil d'administration de l'ICANN conviendront conjointement de la composition de l'équipe de révision. Les recommandations qui résulteront des révisions seront fournies au Conseil d'administration et publiées en ligne pour la sollicitation de commentaires du public. Le Conseil d'administration prendra des mesures dans les six mois à compter de la réception des recommandations. Chacune des révisions susdites doit examiner la mesure dans laquelle les évaluations et les actions entreprises par l'ICANN ont réussi à assurer que l'ICANN agit de manière transparente, est responsable de sa prise de décisions et agit dans l'intérêt public. Les appréciations de la mesure dans laquelle le Conseil d'administration et le personnel ont mis en œuvre les recommandations émanant des autres révisions d'engagement énumérées ci-dessous feront partie intégrale des révisions susdites.

La mise en œuvre de ces engagements en matière de transparence et de redevabilité est prévue tous les trois ans et supervisée par une équipe formée de volontaires dont la composition est validée par le président du *board* de l'ICANN et le représentant du GAC à ce *board*. **Ce système de redevabilité en circuit fermé**, le *board* gardant la main sur sa propre évaluation, assure peut-être une redevabilité de l'ICANN devant la communauté de l'Internet qui la compose, mais assurément pas à l'égard des États et des 3 milliards d'internautes.

Ce n'est finalement que devant les États-Unis que l'ICANN doit rendre des comptes. Mme Anne-Thilda Norodom, professeur à l'université de Rouen, a notamment fait valoir que l'ICANN devait se soumettre à des auditions devant le Congrès américain. Globalement, l'ICANN reste donc sous la férule américaine. Même si certaines personnes non américaines, y compris des Français, ont pu y prendre des responsabilités importantes, ces personnes sont toutes acculturées sur le mode anglo-saxon, soit par les liens culturels anciens qu'entretient leur pays d'origine avec les États-Unis, soit par leurs propres expériences académiques ou professionnelles.

2. Une domination américaine de plus en plus contestée : de la création de l'*Internet Governance Forum* à la fracture de Dubaï

Cette domination américaine sur la gouvernance de l'Internet a fait l'objet d'une contestation croissante.

Par la voix de son président, **l'ICANN a fait valoir à votre mission que les États-Unis, en assurant le rôle de superviseur ultime de l'Internet, avaient en fait joué un rôle de pourvoyeur de confiance ou de « garant »**, pour reprendre les mots de M. Fadi Chehadé : « *En quinze ans, le Département du commerce américain n'a pas refusé une seule fois son accord, pas plus qu'il n'a exigé de prendre une mesure quelconque qui n'aurait pas été décidée par la communauté, comme par exemple de retirer la Syrie de la racine… Les Américains n'ont pas exercé un contrôle, ils se sont contentés d'être les garants de l'ICANN.* »

*a) La création de l'*Internet Governance Forum*, lieu de débat inédit, onusien mais non interétatique, sur la gouvernance Internet*

Depuis le début des années 2000, à la faveur du succès croissant rencontré par le web, les États ont porté une attention plus grande à l'Internet et à sa gouvernance aussi bien à l'UIT, à l'Organisation mondiale de la propriété intellectuelle (OMPI), à l'UNESCO, à l'Organisation pour la coopération économique et le développement (OCDE) qu'au Conseil de l'Europe ; parallèlement, les acteurs privés plaidaient pour un Internet plus régulé, ce qui a donné lieu à l'adoption de législations nationales sur le commerce en ligne ou sur les droits d'auteur et à des procès.

C'est à **Genève en 2003** que fut prise par le secrétaire général de l'ONU la décision d'établir un groupe de travail sur la gouvernance de l'Internet (GTGI). Ce groupe, composé de représentants des gouvernements, du secteur privé et de la société civile, a préparé le **Sommet mondial sur la société de l'information** (SMSI). Ce SMSI s'est tenu à **Tunis** et a réuni non seulement les États mais aussi le secteur privé, la société civile et d'autres organisations internationales. Sans parvenir à un consensus, ce forum mondial, institué par l'UIT, agence des Nations unies, s'est conclu **en 2005**, au terme d'une négociation difficile, par une déclaration de compromis, entre ceux qui plaidaient pour que l'Internet soit gouverné par une entité intergouvernementale et ceux qui s'opposaient à tout changement au régime centré sur l'ICANN.

L'Union européenne a participé activement à ce forum onusien réunissant des États et s'y est distinguée par une double particularité, d'une part, en raison de sa nature non étatique, et d'autre part, en raison de sa double représentation, le Parlement européen y accompagnant la Commission européenne. Consciente de la nécessité d'ajustements au système de gouvernance de l'Internet mais convaincue de la nécessaire complémentarité entre les différents acteurs de ce système, l'Union européenne, alors sous présidence britannique, a pris une part active à la

rédaction du texte de compromis, qui reprend plusieurs de ses propositions les plus saillantes, même s'il ignore les propositions européennes de rééquilibrage dans la gestion des ressources critiques de l'Internet (noms, numéros et adresses). MM. Laurent Sorbier et Bernard Benhamou, qui ont participé à la négociation, le premier comme conseiller au cabinet de M. Jean-Pierre Raffarin, alors Premier ministre, le second en tant que « sherpa » pour la France, ont rappelé à votre mission cette **contribution active de l'Union européenne qui transparaît dans la déclaration finale du sommet de Tunis**.

Ainsi, cet Agenda de Tunis[1] consacre l'Internet comme « *ressource publique mondiale* » et juge que « *sa gouvernance devrait constituer l'une des priorités essentielles de la société de l'information. La gestion internationale de l'Internet devrait s'opérer de façon multilatérale, transparente et démocratique, avec la pleine participation des États, du secteur privé, de la société civile et des organisations internationales. Elle devrait assurer une répartition équitable des ressources, faciliter l'accès de tous et garantir le fonctionnement stable et sécurisé de l'Internet, dans le respect du multilinguisme.* »

En outre, **les États signataires de l'Agenda de Tunis insistent sur la nécessité d'une coopération renforcée, qui reconnaît aux gouvernements une responsabilité politique – quoique non technique – sans dénier le rôle des autres parties prenantes dans le processus de décision** : « *Nous reconnaissons la nécessité de renforcer la coopération afin de permettre aux gouvernements de s'acquitter, sur un pied d'égalité, de leurs rôles et responsabilités en ce qui concerne les questions de politiques publiques internationales concernant l'Internet, mais pas les questions techniques et opérationnelles courantes qui n'ont pas d'incidence sur les questions de politiques publiques internationales. Faisant appel aux organisations internationales compétentes, une telle coopération devrait comprendre l'élaboration de principes applicables à l'échelle mondiale aux questions de politiques publiques ainsi que la coordination et la gestion des ressources fondamentales de l'Internet. À cet égard, nous exhortons les organisations chargées des tâches essentielles liées à l'Internet à favoriser la création d'un environnement qui facilite l'élaboration de ces principes*[2].»

L'Agenda de Tunis a enfin donné mandat au secrétaire général des Nations unies pour établir un forum multi-parties prenantes pour poursuivre le dialogue politique sur la gouvernance de l'Internet et faire des propositions au secrétaire général des Nations unies. Le **Forum de la Gouvernance Internet** (FGI) est donc un lieu de débat inédit, **onusien mais pourtant non interétatique**, sur la gouvernance d'Internet. Il obéit à trois principes : ouverture, multilatéralisme et transparence. En réunissant les gouvernements, les entreprises de l'Internet, la communauté technique et la société civile, le FGI évite les écueils de sommets où cette dernière doit, pour se faire entendre, organiser des sommets parallèles. Son organe central est le

[1] *En son point 29.*
[2] *Points 69-71 de l'Agenda de Tunis.*

groupe consultatif multi-parties prenantes, *Multistakeholder Advisory Group* (MAG), composé de 46 représentants des secteurs public et privé et de la société civile.

La première réunion du FGI a eu lieu en octobre 2006 à Athènes. Plusieurs réunions mondiales ont suivi, rassemblant jusqu'à plusieurs milliers de personnes (Rio de Janeiro en 2007, Hyderabad en 2008, Sharm El Sheikh en 2009, Vilnius en 2010, Nairobi en 2011, Bakou en 2012, Bali en 2013…), et des déclinaisons régionales (EuroDIG[1] pour l'Europe) et nationales du forum ont vu le jour. Un premier FGI France s'est d'ailleurs tenu le 10 mars 2014 dans les locaux du Conseil économique, social et environnemental (CESE) ; même si son organisation a pu prêter le flanc à certaines critiques, il a rendu plus visible l'implication de la France dans le dialogue mondial en cours sur la gouvernance de l'Internet. Le prochain FGI mondial est prévu pour se tenir à Istanbul en octobre 2014.

Purement consultatif, le FGI peut seulement émettre des recommandations. Son champ d'analyse dépasse la seule gestion des noms de domaine et couvre aussi bien les sujets de gouvernance sur l'Internet, comme la protection de l'enfance, la protection des données personnelles et la lutte contre la cybercriminalité, que la réduction de la fracture numérique mondiale.

À ce titre, le FGI constitue un **embryon de gouvernance mondiale et multi-parties prenantes de l'Internet**. Son efficacité reste toutefois très limitée. Comme l'a souligné Mme Nathalie Chiche, membre du Conseil économique, social et environnemental, rapporteure de l'étude *Internet : pour une gouvernance ouverte et équitable* (janvier 2014), auteur d'un rapport du CESE sur la gouvernance de l'Internet[2], auditionnée par votre mission, « *cette formule ne me paraît finalement pas très efficace pour interagir sur l'écosystème que constitue Internet, alors qu'elle me paraissait pouvoir faire office de troisième voie, entre l'autorégulation et le contrôle d'Internet* ». Le FGI permet en effet l'expression de nombreux points de vue mais, à son terme, les questions soulevées restent entières. Évoquant devant votre mission son expérience des longs tours de table, M. Philippe Boillat, directeur général des droits de l'Homme et de l'État de droit du Conseil de l'Europe, s'interroge sur les suites à donner une fois que chacun a eu tout loisir d'exposer ses idées dans ce type d'enceinte : « *And so what ? Et maintenant, que fait-on ?* ».

Si bien que **la structure inédite du FGI affiche aujourd'hui un bilan plutôt médiocre**, même si la 65ème assemblée générale des Nations unies a décidé en 2010 sa reconduction jusqu'en 2015. La commission sur la science et la technologie pour le développement (CSTD) du Conseil économique et social des Nations unies a mis en place un groupe de travail multi-parties prenantes sur la coopération renforcée (*Working group on enhanced cooperation*

[1] European dialogue on Internet governance. *Le dernier EuroDIG s'est tenu en Allemagne les 12 et 13 juin 2014.*

[2] Internet : pour une gouvernance ouverte et équitable, *janvier 2014.*

– WGEC), afin d'identifier un modèle approprié de gouvernance de l'Internet, dans la **perspective du SMSI+10 prévu en 2015**. Lors de son audition par votre mission le 3 juin 2014, Mme Axelle Lemaire a déploré que les conclusions de ce groupe de travail, annoncées pour mars 2014, ne soient toujours pas connues.

Le **FGI** se trouve d'ailleurs **concurrencé par une multitude d'événements traitant de la gouvernance de l'Internet**, comme le montre le schéma ci-après. Si bien que M. Julien Nocetti, chercheur à l'Institut français des relations internationales (IFRI), a pu **plaider** devant votre mission **pour une « gouvernance de la gouvernance de l'Internet »**.

b) Une confrontation entre deux blocs révélée à Dubaï : vers une guerre froide numérique pour la gouvernance de l'Internet ?

La succession des IGF mondiaux n'a donc pas suffi à désamorcer la pression politique croissante sur la gouvernance de l'Internet, qui augmentait à mesure du développement du réseau et de ses conséquences pour les États.

Sans doute les États-Unis ont-ils « lâché un peu de lest » en 2009, lors de la renégociation des termes du contrat qui les lient à l'ICANN : en substituant l'*Affirmation of commitments* au *Memorandum of understanding* qui leur garantissait depuis 1998 le contrôle du processus de décision interne à l'ICANN, ils offraient à cette dernière une perspective d'autonomisation et accordaient ainsi une concession amorçant à peine leur retrait de la gouvernance de l'Internet.

Mais, **durant les années qui ont suivi le SMSI de Tunis, l'opposition entre les tenants d'une gouvernance multipartenariale et les partisans de l'intergouvernemental a continué de constituer la toile de fond du débat**. L'Europe penchait plutôt pour la première option, quand la Chine, la Russie, l'Iran et l'Arabie Saoudite préféraient la seconde, et que les pays émergents, le Brésil ou l'Inde, hésitaient entre les deux.

M. Jean-Michel Hubert, ancien président de l'Autorité de régulation des télécommunications, ancien président délégué du comité stratégique pour le numérique, qui a suivi de près les négociations internationales sur l'Internet pour avoir dirigé de 2003 à 2006 la délégation française au SMSI, a également évoqué devant votre mission la tenue de l'**e-G8 à Deauville en mai 2011** : il a en effet été le « sherpa » numérique pour la France alors que notre pays présidait le G8 et avait obtenu, non sans difficulté, d'y inscrire l'Internet à l'ordre du jour. La déclaration du G8 sur l'Internet énumère très bien les enjeux attachés au développement de l'Internet, « *moyen unique d'information et d'éducation* » pour les citoyens, « *outil essentiel et irremplaçable du développement de l'activité* » des entreprises, « *levier majeur pour l'économie mondiale, la croissance et l'innovation* » – ainsi que les enjeux liés à la protection des données, à la sécurité, au droit d'auteur ou encore à la gouvernance. Les dirigeants des sept pays démocratiques les plus

industrialisés[1] et de la Russie, présents à Deauville, se sont entendus sur le « *rôle des gouvernements dans un essor équilibré d'Internet, aux côtés des utilisateurs et du secteur privé* », apportant ainsi leur appui au modèle multi-acteurs de gouvernance, tout en appelant les États à coopérer davantage.

À cette guerre de tranchées qui a donné lieu à des échanges feutrés entre 2005 et 2010, **a fini par succéder une guerre de mouvement**, comme l'a analysé devant votre mission Mme Catherine Trautmann, députée au Parlement européen et ancienne ministre de la culture et de la communication.

Le travail de la commission science et technologie au service du développement de l'ONU a ainsi débouché sur une résolution de l'Assemblée générale appelant à une coopération renforcée, comme l'avait fait l'Agenda de Tunis, mais dans le sens, cette fois, d'une tentative de contrepoids au « *multistakeholderism* » où, parmi les parties prenantes, le privé compte davantage que le gouvernemental.

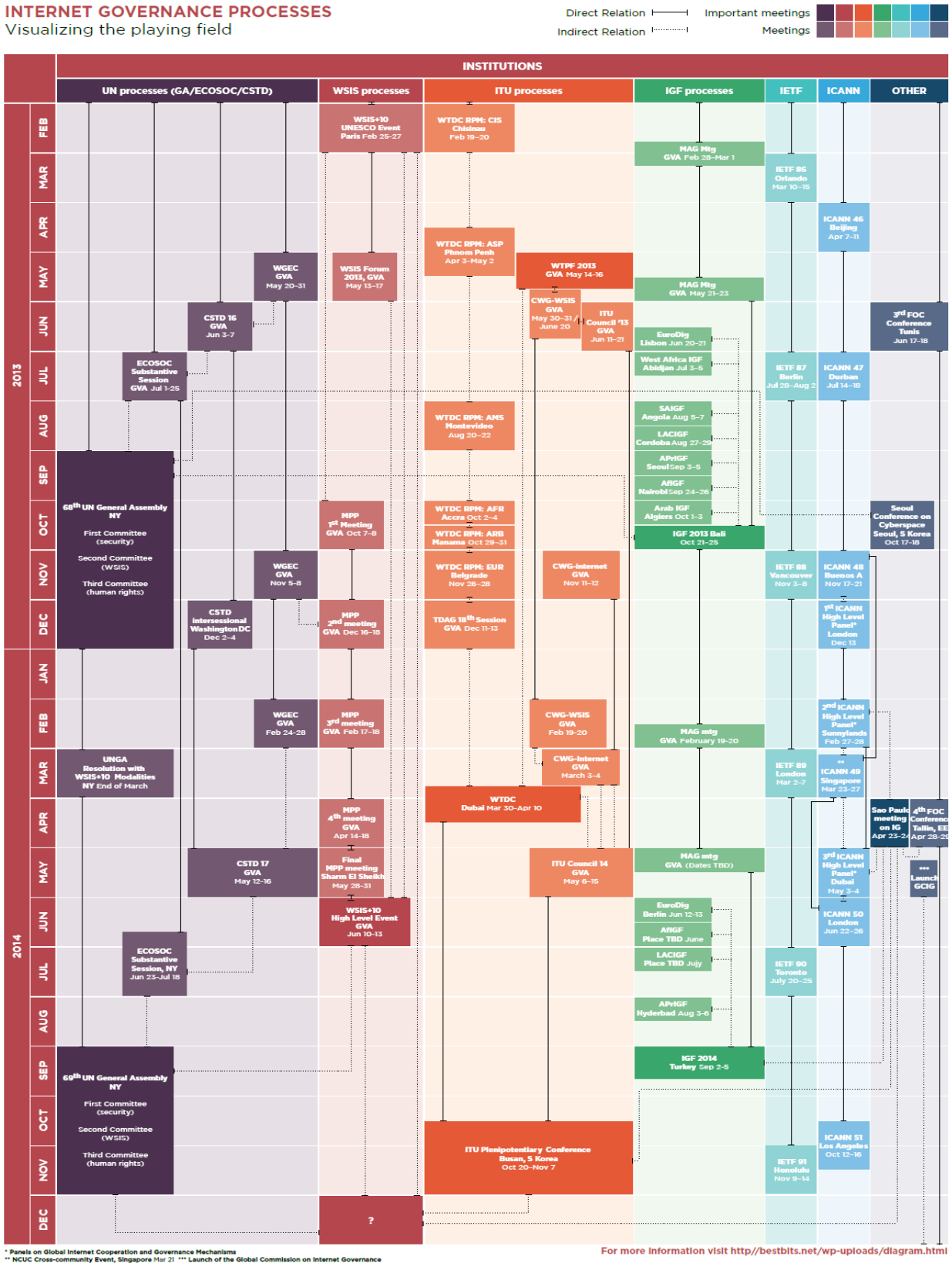
C'est à l'occasion de la conférence organisée par l'UIT à Dubaï en décembre 2012 que l'opposition s'est cristallisée entre les tenants d'une reprise en main étatique de la gouvernance de l'Internet, suspectée de conduire à plus de surveillance, de contrôle et de censure, et les tenants du « *multistakeholderism* ». Durant cette conférence qui visait à renégocier le règlement international des télécommunications rendu obsolète par les avancées technologiques et le développement de l'Internet, **une résolution non contraignante annexée à l'accord final invitait l'UIT à prendre un rôle plus important dans la gouvernance mondiale de l'Internet**.

La Chine, la Russie et les Émirats arabes unis ont exigé l'internationalisation de la gouvernance et la reconnaissance du « *droit souverain et égal de chaque État à réguler ses télécommunications* », ce qui a conduit aux divergences lors des négociations sur le nouveau règlement des télécommunications internationales (RTI). Contestant la mainmise américaine sur la gestion de la racine des noms de domaine, ces États sont parvenus à inscrire dans une résolution[2] annexée à la version révisée du RTI que « *tous les gouvernements devraient avoir égalité de rôle et de responsabilité dans la gouvernance internationale de l'Internet* », reprenant ainsi une formule proche de celle retenue par le SMSI en 2005. L'article 1er du traité adopté par 89 pays le 14 décembre 2012 proclame également le droit souverain de chaque État de réglementer ses télécommunications. 55 « nonistes » (parmi lesquels les États-Unis, la France, le Royaume-Uni, le Canada ou l'Australie) ont refusé de signer le document. Certains ont vu dans ce schisme intervenu à Dubaï entre deux blocs d'États le début d'une guerre froide numérique (*digital cold war*) dans la gouvernance de l'Internet, expression reprise en 2013 par Mme Neelie Kroes dans un de ses discours.

---

[1] *Allemagne, Canada, États-Unis, France, Italie, Japon et Royaume-Uni.*

[2] *Résolution 3 « Promouvoir un environnement propice à la croissance accrue de l'Internet », point e.*


INTERNET GOVERNANCE PROCESSES
Visualizing the playing field
Direct Relation
Indirect Relation
Important meetings
Meetings
INSTITUTIONS
UN processes (GA/ECOSOC/CSTD)
WSIS processes
ITU processes
IGF processes
IETF
ICANN
OTHER
2013
2014
FEB
MAR
APR
MAY
JUN
JUL
AUG
SEP
OCT
NOV
DEC
JAN
WSIS+10 UNESCO Event Paris Feb 25-27
WTDC RPM: CIS Chisinau Feb 19-20
MAG Mtg GVA Feb 28-Mar 1
IETF 86 Orlando Mar 10-15
ICANN 46 Beijing Apr 7-11
WGEC GVA May 20-31
WSIS Forum 2013, GVA May 13-17
WTDC RPM: ASP Phnom Penh Apr 3-May 2
WTPF 2013 GVA May 14-16
MAG Mtg GVA May 21-23
CWG-WSIS GVA May 30-31 / June 20
ITU Council '13 GVA Jun 11-21
3rd FOC Conference Tunis Jun 17-18
CSTD 16 GVA Jun 3-7
EuroDig Lisbon Jun 20-21
West Africa IGF Abidjan Jul 3-5
ECOSOC Substantive Session GVA Jul 1-25
IETF 87 Berlin Jul 28-Aug 2
ICANN 47 Durban Jul 14-18
SAIGF Angola Aug 5-7
LACIGF Cordoba Aug 27-29
APrIGF Seoul Sep 3-5
AfIGF Nairobi Sep 24-26
Arab IGF Algiers Oct 1-3
WTDC RPM: AMS Montevideo Aug 20-22
68th UN General Assembly NY
First Committee (security)
Second Committee (WSIS)
Third Committee (human rights)
MPP 1st Meeting GVA Oct 7-8
WTDC RPM: AFR Accra Oct 2-4
WTDC RPM: ARB Manama Oct 29-31
IGF 2013 Bali Oct 21-25
Seoul Conference on Cyberspace Seoul, S Korea Oct 17-18
WGEC GVA Nov 5-8
WTDC RPM: EUR Belgrade Nov 26-28
CWG-Internet GVA Nov 11-12
IETF 88 Vancouver Nov 3-8
ICANN 48 Buenos A Nov 17-21
CSTD intersessional Washington DC Dec 2-4
MPP 2nd meeting GVA Dec 16-18
TDAG 18th Session GVA Dec 11-13
1st ICANN High Level Panel* London Dec 13
WGEC GVA Feb 24-28
MPP 3rd meeting GVA Feb 17-18
CWG-WSIS GVA Feb 19-20
2nd ICANN High Level Panel* Sunnylands Feb 27-28
MAG mtg GVA February 19-20
UNGA Resolution with WSIS+10 Modalities NY End of March
CWG-Internet GVA March 3-4
IETF 89 London Mar 2-7
** ICANN 49 Singapore Mar 23-27
WTDC Dubai Mar 30-Apr 10
Sao Paulo meeting on IG Apr 23-24
4th FOC Conference Tallin, EE Apr 28-29
MPP 4th meeting GVA Apr 14-18
CSTD 17 GVA May 12-16
Final MPP meeting Sharm El Sheikh May 28-31
ITU Council 14 GVA May 6-15
MAG mtg GVA (Dates TBD)
3rd ICANN High Level Panel* Dubai May 3-4
*** Launch GCIG
WSIS+10 High Level Event GVA Jun 10-13
EuroDig Berlin Jun 12-13
AfIGF Place TBD June
ICANN 50 London Jun 22-26
ECOSOC Substantive Session, NY Jun 23-Jul 18
LACIGF Place TBD July
IETF 90 Toronto July 20-25
APrIGF Hyderbad Aug 3-6
69th UN General Assembly NY
First Committee (security)
Second Committee (WSIS)
Third Committee (human rights)
IGF 2014 Turkey Sep 2-5
ICANN 51 Los Angeles Oct 12-16
ITU Plenipotentiary Conference Busan, S Korea Oct 20-Nov 7
IETF 91 Honolulu Nov 9-14
?
* Panels on Global Internet Cooperation and Governance Mechanisms
** NCUC Cross-community Event, Singapore Mar 21 *** Launch of the Global Commission on Internet Governance
For more information visit http//bestbits.net/wp-uploads/diagram.html

UN processes (GA/ECOSOC/CSTD)	World Summit on the Information Society (WSIS) processes	International Telecommunication Union (ITU) processes	Internet Governance Forum (IGF) processes	Governance of Internet's technical resources (ICANN, IETF, ...)
Processus des Nations unies : – Assemblée générale des Nations unies (UNGA) – Conseil économique et Social (ECOSOC) – Commission pour la science et le développement technologique (CSTD) – Groupe de travail sur la coopération renforcée (WGEC)	Processus du Sommet mondial sur la société de l'information (SMSI) : Plateforme préparatoire multi-parties prenantes pour le 10ème anniversaire du SMSI (MPP)	Processus de l'Union internationale des télécommunications (UIT) : – Conférence mondiale pour le développement des télécommunications (WTDC) et réunions régionales préparatoires (WTDC RPMs) – Forum mondial pour les politiques de télécommunications et de TIC (WTPF) – Groupes de travail du Conseil (CWG) : • pour les questions internationales de politiques publiques en matière Internet (CWG-Internet) • sur la mise en œuvre des conclusions du SMSI (CWG-WSIS) – Groupe consultatif pour le développement des télécommunications (TDAG)	Processus du Forum sur la gouvernance de l'Internet (FGI) : – Groupe consultatif multi-parties prenantes (MAG) – FGI régionaux : Afrique (AflGF), Arabie (Arab IGF), Asie Pacifique (AprlGF), Europe (EuroDig), Amérique latine et Caraïbes (LACIGF), Afrique du Sud (SAIGF), Afrique de l'Ouest (West Africa IGF)	– Société pour l'attribution des noms de domaine et des numéros sur Internet (ICANN) – Groupe de travail d'ingénierie de l'Internet (IETF)
Autres : Commission mondiale sur la gouvernance de l'Internet (GCIG) ; Coalition pour la liberté en ligne (FOC)				

Sans doute l'Europe n'a-t-elle pas été la plus audible à cette conférence de Dubaï. Son infériorité numérique notoire y a certainement contribué : M. Julien Nocetti a fait observer à votre mission que, face aux 120 représentants américains présents à Dubaï, se trouvaient seulement six Allemands et quatre Français. Par ailleurs, comme l'a remarqué M. Weill lors de son audition, le discours européen est trop ciblé sur l'acquis communautaire et sans marge de négociation suffisante. Surtout, l'Europe est inaudible car la Haute représentante de l'Union pour les affaires étrangères et la politique de sécurité, en charge de la diplomatie européenne, ne s'exprime pas sur ce sujet. Et pour cause : aucun mandat ne lui a été donné, ce qui fait le jeu du camp américain.

Pourtant, votre mission partage l'analyse qu'a faite Mme Pauline Türk lors de son audition : on peut penser que **cette confrontation ouverte « *pourrait bénéficier sur le plan politique à l'Union européenne, si elle parvient à se positionner en arbitre*, *entre des États soucieux de leur souveraineté numérique mais prompts à la restriction et à censure, et les États-Unis, désireux de défendre leur maîtrise de l'outil, mais au moins autant de protéger les principes et valeurs libérales du réseau* ». En effet, de nombreux pays, dont beaucoup en développement, sont légitimement désireux d'accroître leur influence sur la gouvernance de l'Internet sans pour autant vouloir censurer ou surveiller les flux sur le réseau. Et le refus américain de toute reprise en main des États sur cette gouvernance apparaît largement hypocrite au regard de leur propre mainmise sur l'ICANN, l'une des institutions centrales de ladite gouvernance.

c) L'Union européenne peine à faire valoir une troisième voie

L'Union européenne ne doit pas se faire enfermer dans la rhétorique de la guerre froide numérique, qui pourrait laisser croire au caractère profondément hétérogène – voire irréconciliable – des deux tendances qui se sont révélées à Dubaï[1].

Mais sa parole en matière de gouvernance de l'Internet reste peu audible, souffrant d'être seulement portée par la direction générale compétente de la Commission européenne, la DG Connect, **sans être assumée dans son ensemble par le Conseil**, dont l'approche de l'Internet a été tardive et se focalise essentiellement sur la dimension de cybersécurité.

La délégation de votre mission qui s'est rendue à Bruxelles a pu le mesurer : la participation de l'Union européenne au sein du GAC de l'ICANN est légitimement assurée par cette direction générale. C'est donc naturellement la Commission qui a créé et mène le groupe de haut niveau dédié à la gouvernance de l'Internet (*High level group on Internet governance* –

[1] *« NETmundial : only a landmark event if « Digital cold war » rhetoric abandoned », Francesca Musiani et Julia Pohle, 27 mars 2014.*

HLGIG), enceinte de débats entre experts nationaux au sein duquel siège pour la France M. David Martinon. Parallèlement, depuis novembre 2012, le Conseil mène des travaux centrés sur la cybersécurité au sein d'un groupe stratégique *ad hoc*, dit « des amis de la présidence ». Il réunit les ambassadeurs chargés des affaires de sécurité, mais y participent aussi pour la France le secrétaire général adjoint du ministère des affaires étrangères, et également M. Martinon. Percevant les enjeux stratégiques en cause derrière ces questions d'apparence technique, le Conseil européen, dans ses conclusions de décembre 2013, a mandaté le Service européen d'action extérieure (SEAE), en collaboration avec la Commission européenne et avec l'Agence européenne de Défense, pour une mission d'un an afin d'améliorer les capacités européennes de cyberdéfense. Cette mission jette un pont entre la Commission et le SEAE sur les dossiers cyber, mais sous l'angle sécurité et défense, sans amorcer une véritable diplomatie européenne de la gouvernance de l'Internet.

Cette lacune est apparue à votre délégation lors de son entretien à Bruxelles avec M. Maciej Popowski, secrétaire général adjoint du SEAE, et avec Mme Linda Corugedo Steneberg, de la DG Connect de la Commission européenne. Le premier a certes indiqué que les conclusions du Conseil affaires générales de juin 2013 avaient plaidé pour une approche multi-parties prenantes de la gouvernance de l'Internet, mais il a semblé peu armé pour construire une proposition d'amélioration de ce système multi-acteurs. **S'il reconnaît que les questions de gouvernance de l'Internet ont des implications politiques, le SEAE** – doté sur ces questions de seulement trois personnes à temps plein – **porte prioritairement ses efforts sur la cyberdéfense européenne et le développement des capacités cyber des pays tiers**, au titre des instruments pour la paix et la stabilité.

Active au sein de l'ICANN, mais aussi au sein du FGI[1], **la Commission européenne a paru**, pour sa part, **plus engagée dans le débat** entre les deux approches cristallisées à Dubaï et résumées en ces termes par Mme Corugedo Steneberg : « *multistakeholderism versus top-down* ». À travers plusieurs communications[2], la Commission a mis en avant les principes de l'Internet, conformément à l'action 97 identifiée par Mme Neelie Kroes dans l'Agenda numérique pour l'Europe, que votre rapporteure a déjà présenté dans son rapport[3] sur la gouvernance européenne du numérique, écrit en 2013 au nom de la commission des affaires européennes du Sénat.

S'inspirant de l'Agenda de Tunis, **la Commission européenne défend une vision de l'Internet qu'elle résume par l'acronyme COMPACT**,

---

[1] *La commissaire européenne en charge de la stratégie numérique, Mme Neelie Kroes, a personnellement participé aux FGI de Nairobi en 2011 et Bakou en 2012, et contribué par un message vidéo à l'ouverture de celui de Bali en 2013.*

[2] *COM(1998) 111, COM(1998) 476, COM(2000) 202, COM (2009)277 et COM (2014)72.*

[3] *Rapport d'information du Sénat (2012-2013) précité n°443,* L'Union européenne, colonie du monde numérique ?, *mars 2013.*

désignant l'Internet comme un espace civiquement responsable, unifié, régi par une approche multipartenaire, promouvant la démocratie et les droits de l'homme, à l'architecture fiable et reposant sur une gouvernance transparente : « *The vision of the European Commission is summarised in the COMPACT concept : the Internet as a space of Civic responsibilities, One unfragmented resource governed via a Multistakeholder approach to Promote democracy and Human Rights, based on a sound technological Architecture that engenders Confidence and facilitates a Transparent governance both of the underlying Internet infrastructure and of the services which run on top of it* »[1].

Mais Mme Corugedo Steneberg a observé que **ces principes**, quoiqu'ayant reçu le soutien des États membres, **n'ont jamais fait l'objet d'un vote. La Commission invite donc le Conseil et le Parlement européen à établir un ensemble cohérent de principes applicables à la gouvernance de l'Internet**.

La Commission est aussi particulièrement engagée auprès des États membres dans la défense des intérêts européens menacés par l'ouverture des « .vin » et « .wine ». Mais votre mission déplore que le seul interlocuteur au Conseil pour la DG Connect soit le groupe Télécoms du Conseil[2], ce qui ampute de fait les discussions sur la gouvernance de leur dimension géopolitique et stratégique.

Votre mission n'ignore pas qu'une importante **difficulté** pour élaborer une position politique de l'Union sur les questions de gouvernance de l'Internet est **la règle de l'unanimité, qui prévaut en matière de politique étrangère et de sécurité commune**.

L'étude comparative sur la gouvernance de l'Internet à laquelle elle a fait procéder dans neuf États emblématiques de la diversité de l'Union européenne[3] – annexée au présent rapport – **atteste des divergences de sensibilités** qui existent, notamment entre des pays très alignés sur les États-Unis et souvent les plus innovants en matière numérique – **Royaume-Uni, Suède, Pays-Bas, Estonie** – et certains autres, comme l'**Italie**, qui semblent encore peu mobilisés sur le sujet, ou d'autres encore dont la position semble assez confuse, comme l'**Allemagne** où une délégation de votre mission s'est rendue début mars. Toutefois, certains États membres expriment clairement leur préoccupation à l'égard du faible poids de l'Europe dans la gouvernance mondiale de l'Internet et sont convaincus de la nécessité pour l'Union européenne d'adopter une stratégie commune et offensive : ainsi, dans un document qu'elle a transmis au groupe télécoms du Conseil en février dernier, la **Belgique** juge nécessaire de « *renforcer la coopération au niveau européen, voire de porter cette discussion au niveau du Conseil des ministres afin de permettre l'adoption de principes communs aux États*

[1] Cf. *http://ec.europa.eu/digital-agenda/en/global-Internet-and-telecommunications*
[2] *Qui contribue à la préparation des travaux du Conseil « Transports, télécommunications et énergie ».*
[3] *Allemagne, Belgique, Espagne, Estonie, Italie, Pays-Bas, Pologne, Royaume-Uni et Suède.*

membres ». De même, l'**Espagne** semble de plus en plus mobilisée : le Sénat espagnol a d'ailleurs organisé, le 16 mai dernier, une journée sur la gouvernance de l'Internet. La **Pologne**, également, estime qu'il s'agit d'une question d'importance croissante et mène actuellement une large consultation interne sur ce sujet ; elle soulève notamment la question du rôle des gouvernements dans la définition des standards techniques. Peu d'États membres ont donc pris des initiatives politiques concernant le rôle de l'Union européenne dans la gouvernance mondiale de l'Internet.

Mais l'Union européenne n'est-elle pas bien placée, voire attendue par certains pays en développement, pour explorer une troisième voie fondée sur une approche véritablement inclusive de la gouvernance d'un Internet bâti sur des valeurs démocratiques ?

Les **États-Unis** eux-mêmes ont laissé peu d'espace politique à une telle approche, **assimilant tous ceux qui interrogeaient le *statu quo* à des ennemis de la liberté** et camouflant ainsi les intérêts géopolitiques, économiques, militaires et culturels des parties prenantes qui défendent ce modèle. Mais les révélations d'Edward Snowden distillées à partir de juin 2013 sont venues déplacer les lignes.

D'ailleurs, en février 2014, la Commission européenne s'est elle-même proposée comme « médiateur » dans les futures négociations mondiales sur la gouvernance de l'Internet[1], proposition à laquelle certains États membres sont encore hostiles, comme l'atteste explicitement la réponse provenant du Royaume-Uni aux questions adressées par votre mission.

3. Le séisme Snowden en 2013 rend impossible le statu quo

Un an après les premières révélations publiées le 6 juin 2013 par le quotidien britannique *The Guardian*, les informations divulguées par M. Edward Snowden continuent à alimenter la chronique journalistique et diplomatique. Aussi les travaux menés par votre mission d'information ont été l'occasion de mesurer auprès des personnes auditionnées l'ampleur de la crise de confiance engendrée dans l'économie numérique par la surveillance généralisée mise en œuvre par certains États et la perméabilité des données personnelles détenues par les grands opérateurs de réseaux télécom ou de services Internet.

D'emblée, ce sujet a été inscrit au cœur des préoccupations de la mission, votre rapporteure estimant que « *l'affaire Prism a démontré que la gestion de l'Internet sous domination américaine ne pouvait durer en l'état* »[2]. La question qui se pose est la suivante : l'affaire Snowden et les discussions

[1] Cf. *son communiqué de presse du 12 février 2014 : http://europa.eu/rapid/press-release_IP-14-142_fr.htm*

[2] Cf. *compte rendu de la réunion constitutive du bureau de la mission commune d'information du 3 décembre 2013.*

actuelles offrent-elles une opportunité de rééquilibrage des forces en présence ?

a) Un épicentre nord-américain, une onde de choc planétaire qui n'épargne pas l'Europe

Un point sur l'origine de cette affaire et ses développements successifs apparaît nécessaire pour mieux mesurer le choc provoqué dans la communauté du renseignement et parmi les acteurs du net. Les révélations sur les pratiques de la *National Security Agency* (NSA) ont donc été mises en lumières par Edward Snowden, jeune informaticien alors âgé de 29 ans et ancien employé de la CIA puis d'un prestataire privé de la NSA en qualité d'administrateur système. Les motivations exprimées à l'appui de la communication à la presse d'une très importante documentation électronique[1] révèle le profond désaccord moral d'un employé avec les tâches dont il a eu à connaître : « *je ne peux, en mon âme et conscience, laisser le gouvernement américain détruire la vie privée, la liberté sur Internet et les libertés essentielles pour les gens tout autour du monde avec ce système énorme de surveillance qu'il est en train de bâtir secrètement*[2] ».

De fait, la surveillance de masse dénoncée par Edward Snowden couvre **un spectre très large d'activités allant des « classiques » données téléphoniques à la consultation des serveurs de grands groupes Internet** ainsi que le déchiffrement des échanges électroniques à une très large échelle ainsi que le décrit l'encadré ci-dessous.

Les principales révélations d'Edward Snowden

Liste thématique non exhaustive des révélations par voie de presse :

- **écoutes téléphoniques** : fourniture des données téléphoniques (numéros de téléphones, mails, identifiants, numéro unique d'un téléphone portable) à la NSA par l'opérateur Verizon pour les communications internes aux États-Unis et externes avec l'étranger (6 juin 2013 – *The Guardian*) ;

– **programme de surveillance PRISM** : accès aux serveurs de grands opérateurs de services Internet dont Microsoft, Yahoo, Google, Facebook et Apple intégrant la surveillance en temps réel des courriels, les communications instantanées par « Chat », la participations aux forum de discussion et la diffusion de photos et de vidéos (6 et 29 juin 2013 – *The Washington Post*) ;

[1] *Le nombre de documents reçus initialement par les journalistes du Washington Post et du Guardian s'élèverait à 15 000 ou 20 000 documents chiffrés mais le nombre de 1,7 million a été évoqué en décembre 2013 (source : http://www.cbsnews.com/news/nsa-speaks-out-on-snowden-spying/).*

[2] *Traduction des propos rapportés par l'article « Edward Snowden: the whistleblower behind the NSA surveillance revelations » publié le 10 juin 2013 par* The Guardian *: «* I can't in good conscience allow the US government to destroy privacy, Internet freedom and basic liberties for people around the world with this massive surveillance machine they're secretly building ».

– implication de la NSA dans la surveillance du Conseil de l'Europe (PRISM), des bureaux de l'Union européenne à Washington et aux Nations unies, du siège de l'ONU à New-York (29 juin 2013 – *Der Spiegel*).

– **espionnage des communications Internet et téléphoniques des participants au G20** à Londres par le *Government Communications Headquarters* (GCHQ) britannique (17 juin – *The Guardian*) ;

– **programme Tempora** : espionnage des câbles sous-marins transatlantiques par le GCHQ et transmission des informations à la NSA (21 juin 2013 – *The Guardian*) ;

– **programme X-Keyscore** : outil d'analyse de l'activité des individus sur l'Internet telle que les courriels, l'historique de navigation et l'activité sur les réseaux sociaux (31 juillet 2013 – *The Guardian*) ;

– **programme Bullrun** : décodage et exploitation des failles des systèmes de chiffrement des communications sur l'Internet utilisés par les internautes dans le cadre d'une utilisation privée et par les entreprises pour sécuriser leurs échanges électroniques (5 septembre 2013 – *New York Times*) ;

– **programme GENIE** : implantation de logiciels espions sur les ordinateurs, routeurs et logiciels pare-feux dans le but de collecter à distance des informations confidentielles ;

– **surveillance des chefs d'État** dont la Chancelière Angela Merkel (octobre 2013 – *Der Spiegel*) ;

– **collecte de 200 millions de SMS par jour** dans le monde, de manière non ciblée, pour en extraire du renseignement (16 janvier 2014 – *The Gardian*) ;

– **utilisation des données de géolocalisation des téléphones portables** pour déterminer la position de personnes qui sont ensuite visées par une frappe de drones (10 février 2014 – *The Intercept* créé par Glenn Greenwald, Laura Poitras et Jeremy Scahill) ;

– **Interception des flux des applications installées sur les smartphones** tel que le jeu Angry birds téléchargé par plus de 1,7 milliard d'utilisateurs et le logiciel de cartographie Google Map (27 janvier 2014 – *New York Times*) ;

– **collecte de « millions » d'images par jour aux fins de reconnaissance faciale** dans les bases de données de la NSA (31 mai 2014 - *New York Times*).

Pour M. Philippe Lemoine, « *dans les révélations initiales d'Edward Snowden, le dossier le plus important, c'est l'affaire Prism, c'est à dire les accords passé entre la NSA et les grandes entreprises américaines de l'Internet. On peut se demander à quel niveau ces accords ont été passés, et s'il faut en imputer la responsabilité aux dirigeants de Facebook ou de Google, ou au mécanisme du* Patriot Act*, qui fait obligation à ces entreprises d'avoir des personnels habilités secret défense, instituant de fait une double hiérarchie au sein de l'entreprise.* »

En effet, il convient de souligner que la collecte ne résulte pas seulement d'activités d'espionnage pratiqué unilatéralement par les agences de renseignement mais s'appuie également sur la fourniture de données par les grands opérateurs, conformément au **cadre légal posé par le *Patriot Act* et le *Foreign Intelligence Surveillance Act* (FISA)**.

La législation américaine en matière de surveillance

À la suite des attentats du 11 septembre 2001, les États-Unis ont souhaité élargir les pouvoirs de leurs services de renseignement afin de mieux lutter contre les menaces terroristes.

C'est dans ce contexte qu'a été adopté par le Congrès le ***US Patriot Act***[1], loi promulguée le 26 octobre 2001, prorogée deux fois, le 9 mars 2006 et le 26 mai 2011, jusqu'en juin 2015. Cette législation a été complétée le 10 juillet 2008 par le ***Foreign Intelligence Surveillance Act of 1978 Amendment Act of 2008***, dit *FAA*.

Deux dispositions de ces lois retiennent particulièrement l'attention.

La section 215 du *Patriot Act* permet à la *National Security Agency* (NSA) d'obtenir des entreprises privées américaines dans le secteur de l'Internet **un accès à des données commerciales sur la base d'injonctions judiciaires secrètes**. C'est à ce titre qu'a été pris le décret obligeant l'opérateur téléphonique Verizon à transmettre régulièrement à la NSA des détails sur les communications à l'intérieur comme à l'extérieur des États-Unis[2]. Par ailleurs, d'autres moyens de **collecte massive de données** ont été mis en œuvre, notamment en amont (programmes dits « *upstream* ») des fournisseurs d'accès, à partir des réseaux publics ou privés[3]. Ainsi, plusieurs entreprises comme Google et Facebook ont pu démentir avoir accordé un « accès direct » à leurs données aux autorités, sans que cela signifie pour autant que celles-ci n'aient pu en prendre connaissance[4].

La section 702 du *FAA* permet au procureur général et au directeur du renseignement américain d'autoriser conjointement, pour une période ne pouvant dépasser un an, **la surveillance de personnes présumées vivre hors des États-Unis à des fins de renseignement**[5]. Les citoyens ou résidents américains bénéficient des protections liées au quatrième amendement de la Constitution des États-Unis, qui interdit les perquisitions non motivées par des mandats fondés sur une base légale, protections non reconnues aux citoyens des autres pays[6].

---

[1] US Patriot Act *est un acronyme pour* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism.
http://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf

[2] *Information révélée le 5 juin 2013 par le* Washington Post *et le* Guardian*, voir l'étude sur* Les Programmes de surveillance des États-Unis et leurs effets sur les droits fondamentaux des citoyens de l'Union européenne*, commandée par la commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen, publiée en septembre 2013, p. 17.*
http://www.europarl.europa.eu/RegData/etudes/note/join/2013/474405/IPOL-LIBE_NT(2013)474405_FR.pdf

[3] *Ibid.*

[4] *Ibid., p. 23.*

[5] *Section 702 (a) du FAA :* « Notwithstanding any other provision of law, upon the issuance of an order in accordance with subsection (i)(3) or a determination under subsection (c)(2), the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information. » *http://www.gpo.gov/fdsys/pkg/BILLS-110hr6304enr/pdf/BILLS-110hr6304enr.pdf*

[6] *Comme cela a été dit par exemple par le général Michael Hayden, ancien directeur de la NSA. Voir l'étude citée du Parlement européen, p. 26.*

C'est la combinaison de ces deux dispositifs qui a rendu possibles les programmes de surveillance de masse de la NSA – notamment le programme *Prism* – portés à la connaissance du public en juin 2013 à l'occasion de « l'affaire Snowden ».

Si certaines activités de surveillance révélées par M. Edward Snowden sortent manifestement du cadre légal, il apparaît qu'une grande part d'entre elles s'inscrit en fait dans le cadre légal américain. **Le droit américain donne la possibilité aux agences de renseignement de pratiquer une surveillance de masse et permanente, laissant les non Américains sans protection, dès lors que le 4ème amendement de la Constitution américaine ne leur est pas applicable**. À cet égard, les déclarations du Général Keith Alexander, directeur de la NSA en charge de l'U.S. *Cyber Command*, ne sont guère rassurantes. S'il indique que tout au plus une soixantaine de citoyens américains font l'objet de la procédure de ciblage judiciaire, il reconnaît par ailleurs :

– collecter les données téléphoniques de 300 millions d'Américains, sans qu'il s'agisse d'écoute à proprement parler, aux fins d'analyse des métadonnées (numéros composés, durée des appels, date et heure) pour identifier les chaînes d'appel des organisations terroristes ;

– et ne pas avoir recours à une décision de justice pour pratiquer l'espionnage digital hors du sol américain.

En marge de ce cadre légal, il a également été rapporté, preuves photographiques à l'appui publiées dans la presse, que des **agents de la NSA installaient des « Chevaux de Troie »** dénommés *beacon* (cf. photos ci-dessous) **sur les routeurs CISCO** à l'insu de l'équipementier et de ses clients[1].

Matériel de routage Cisco en cours de « modification » par des agents de la NSA

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

Source : No Place to Hide, *Glenn Greenwald, 2014.*

[1] *Source :* No Place to Hide, *Glenn Greenwald, 2014.*

Pour allumer un contre-feu aux révélations concernant le piratage effectué par la NSA sur le réseau du fabricant de *smartphones* et tablettes HUAWEI[1], les États-Unis ont annoncé avoir mis en cause cinq « hackers militaires » opérant de l'espionnage industriel au profit de la Chine[2].

Si les annonces provenant de M. Edward Snowden visent principalement les États-Unis, **l'Europe n'est pas** pour autant **épargnée par cette mise en cause des activités de surveillance de masse**. Elle l'est d'autant moins que les services britanniques, allemands et français ont été cités comme des partenaires dans cette circulation d'informations. Alors que M. Philippe Lemoine a pu déplorer le silence de la France sur un tel sujet, il a souligné que « *la sensibilité est tout autre en Allemagne, où le souvenir de la Stasi est encore vivant. La révélation d'une surveillance jusque sur le portable de Mme Merkel a été la cerise sur le gâteau*. » Cela explique que l'Allemagne ait pu être en pointe dans la proposition d'un « Internet européen » dont les contours resteraient à définir plus précisément, étant entendu que la Commission européenne promeut des principes de gouvernance « *qui préservent le caractère ouvert et non morcelé du réseau* »[3].

L'opérateur britannique Vodafone a reconnu dans un rapport publié le 6 juin 2014 par le quotidien The Guardian[4] qu'il avait fait l'objet de pratiques de surveillance de son réseau effectuées par les autorités de 29 pays, parmi lesquels figurent le Royaume-Uni, l'Espagne, le Portugal, l'Italie, l'Allemagne, la République tchèque, la France, l'Australie, l'Égypte, l'Inde, ou encore le Qatar. En outre, il confirme notamment l'existence de câbles secrets fournissant aux agences gouvernementales un accès direct à ses serveurs et à son réseau téléphonique, pour au moins six pays. Deutsche Telekom, l'opérateur allemand, a publié en mai 2014 un rapport de transparence faisant état de 946 641 demandes de données d'internautes ayant téléchargé illégalement des contenus.

Ces premiers pas vers davantage de transparence sur le continent européen font suite à la publication en janvier 2014 par Verizon, premier opérateur des États-Unis avec 203 millions d'abonnés, d'un rapport détaillé des demandes d'écoutes qui lui étaient faites par le gouvernement[5], mais ils demeurent très partiels.

---

[1] *Source : Der Spiegel (22 mars 2014)*

[2] *http://www.zdnet.com/chinese-military-hackers-charged-with-cyber-espionage-against-us-companies-7000029617/*

[3] *Intervention de Mme Neelie Kroes, vice-présidente de la Commission européenne en charge de la stratégie numérique au sommet mondial de la société de l'information de Genève du 10 juin 2014.*

[4] *Source : http://www.theguardian.com/business/2014/jun/06/vodafone-reveals-secret-wires-allowing-state-surveillance*

[5] *L'opérateur a indiqué qu'il avait reçu 320 000 demandes judiciaires de récupération de données en 2013 rien qu'aux États-Unis. De son côté, AT&T, le deuxième opérateur américain a très vite suivi son concurrent Verizon en publiant lui aussi un rapport de transparence. En février, le géant américain a indiqué avoir reçu 301 816 demandes des autorités pour des écoutes téléphoniques ou*

b) Des répercussions économiques sur l'industrie qui inquiètent les acteurs du net américain

La question de la crise de confiance envers les opérateurs privés s'est posée très tôt. Ainsi, sous le titre « Le scandale FBI-NSA pourrait rebattre les cartes dans le marché du *cloud* », le journal *Le Monde* indique, au lendemain des premières révélations émanant de M. Edward Snowden : « *La révélation de l'accès du FBI et de l'Agence nationale de sécurité américaine (NSA) aux infrastructures de neuf géants américains d'Internet jette le discrédit sur ces multinationales. Le programme Prism, révélé par le Washington Post, serait un outil permettant aux services de renseignement américains d'accéder aux données des personnes situées à l'étranger, qui ne sont pas protégées par la loi américaine contre les consultations sans ordonnance.* »[1]

Les auditions menées par votre mission ont montré que la relation d'échange d'informations entre l'administration américaine et le secteur privé pouvait être vue sous l'angle d'une collaboration fructueuse. Ainsi, Me Olivier Iteanu estime que ***« ce n'est pas la National Security Agency (NSA) qui surveille les populations, mais bien Google et Facebook****. Les entreprises américaines ont été autorisées à surveiller les populations, en échange de quoi elles ont mis la main dans le pot de confiture des données. […] L'affaire Prism a été un tsunami qui a révélé la collaboration entre les géants du Web et l'État américain.* »

Mais pour M. Bernard Benhamou, « *ce que l'affaire Snowden a démontré, c'est que la sécurité des échanges sur Internet avait été volontairement affaiblie, à la demande de la National Security Agency (NSA) américaine, pour y ménager des* back doors, *des « portes de sorties » par lesquelles la NSA pouvait surveiller les échanges. Cet amoindrissement volontaire de la sécurité est une atteinte majeure à la confiance que les particuliers et les entreprises peuvent avoir dans le réseau : ces agissements, une fois révélés, ont rompu le contrat tacite qui existait jusqu'alors entre les créateurs et les usagers d'Internet, sur la sécurité de leurs activités en ligne. Les effets en ont été rapides, en particulier sur le plan économique : depuis les révélations d'Edward Snowden, l'équipementier CISCO a vu ses commandes reculer de 17 %, dans les pays émergents, qui hésitent en effet à s'équiper si cela induit un risque important de surveillance par les États-Unis.* » L'effet négatif de mauvaise réputation a donc inquiété au premier chef cet équipementier, mais par un effet de tâche d'huile, l'ensemble de l'industrie numérique semble entachée par la suspicion de collusion avec les agences de renseignement.

Le think tank *Information Technology & Innovation Foundation* (ITIF), basé à Washington, considère que **l'impact économique sur la compétitivité des entreprises américaines**, qui dominent le marché mondial du *cloud* est immédiat et important : durant les trois prochaines années, entre 10 et 20 %

encore des informations concernant ses abonnés dont un millier de demandes émanant directement de la NSA.

[1] *Source : article publié par lemonde.fr le 7 juin 2013 par Guénaël Pépin.*

des contrats des prestataires *cloud* américains avec l'étranger pourraient être annulés, soit **une perte de chiffre d'affaires évaluée de 22 à 35 milliards de dollars**[1].

De son côté, la *Cloud security alliance* a recensé, sur un panel de 500 entreprises américaines du net, un taux de 56 % de réponses accréditant la perte potentielle de contrats avec les pays non américains tels que l'Allemagne, la France, les autres pays européens mais aussi le Canada, confirmant le fait que le ralentissement de l'activité de Cisco[2] s'inscrit dans un climat de défiance généralisé.

L'appel lancé aux autorités américaines par Cisco, Apple, Google et Facebook, à la mise en place de règles de conduite pour rétablir la confiance des consommateurs[3] traduit une **véritable inquiétude de l'industrie outre-Atlantique quant à la conservation de son *leadership***.

Dans une lettre adressée le 15 mai dernier par M. John T. Chambers, PDG de Cisco system, principal équipementier de réseaux, alerte le Président des États-Unis sur l'amoindrissement de la confiance des consommateurs dans l'industrie numérique américaine, le risque de perte du *leadership* technologique et de fragmentation de l'Internet si les « *allégations des médias étaient vraies* ». Il ajoute que « *cette confiance est érodée par les révélations sur la surveillance faites par le gouvernement, rendant de ce fait difficile la tâche pour les entreprises de satisfaire les besoins de protection de la vie privée des citoyens et de se conformer aux lois des autres États* », avant de demander que l'administration américaine s'engage dans des réformes qui puissent être acceptées par les autres pays dans le monde.

c) Des secousses politiques qui appellent une initiative de la part des États-Unis et de l'Europe

Du fait de ces révélations prouvant l'immixtion entre surveillance légale et illégale, privée et étatique, **les États-Unis ont surtout perdu leur magistère moral sur l'Internet** : est brutalement tombé l'argument qui légitimait la supervision américaine sur la racine de l'Internet, à savoir qu'ils étaient par excellence le gouvernement protecteur des libertés publiques, et notamment de la liberté d'expression garantie par le premier amendement de la Constitution américaine.

Se présentant comme le promoteur d'un Internet ouvert et sûr tout en pratiquant un espionnage d'une ampleur jusqu'alors sans égale, les États-Unis sont pris dans leur propre contradiction et se trouvent sous la pression de leurs propres entreprises, victimes d'atteinte à leur réputation. Et cela, alors même que selon M. Jérémie Zimmermann, porte-parole de

---

[1] *Source :* How Much Will PRISM Cost the U.S. Cloud Computing Industry?, *Daniel Castor, ITIF août 2013.*

[2] *Les commandes de Cisco ont baissé de 25 % au Brésil, de 30 % en Russie et de près de 20 % au Mexique et en Chine.*

[3] *"Cisco boss calls on Obama to rein in surveillance" (*Financial Times *du 18 mai 2014).*

l'association « La Quadrature du net », citant une étude de la *New America Foundation*, « *seuls 3 % des attentats terroristes ont été déjoué grâce à cette surveillance de masse* ».

Les États membres de l'Union européenne ne se sont pas entendus pour réagir ensemble, mais le Parlement européen s'est mobilisé sans tarder sur le sujet : dès le 4 juillet 2013, il adoptait une résolution afin de lancer une enquête approfondie sur les programmes de surveillance des États-Unis[1]. Il a ainsi préconisé, le 18 décembre 2013, dans le cadre de ses conclusions préliminaires, une réforme du cadre américano-européen de protection des données d'ici à la fin de 2014 au plus tard et la suspension des accords *Safe Harbor* et *Terrorist Finance Tracking Program* (TFTP) ainsi que le développement d'offres européennes d'informatique en nuage, considérant que l'ensemble des données stockées dans le *cloud* des entreprises américaines peut potentiellement être consulté par la NSA et la possibilité pour les citoyens de l'Union européenne d'avoir un recours judiciaire.

À la tribune de l'ONU, en septembre 2013, **Mme Dilma Rousseff, présidente du Brésil**, s'était insurgée en termes peu diplomatiques contre la violation de la souveraineté de son pays et de la vie privée de ses concitoyens, et contre la surveillance de ses entreprises et des représentations diplomatiques. Estimant que le respect de la vie privée permet la liberté d'expression et conditionne donc la possibilité de la démocratie, elle envisageait de doter le Brésil de ses propres infrastructures Internet. Elle avait également appelé à un nouveau système mondial de supervision de l'Internet : elle préconisait que de tels mécanismes multilatéraux garantissent la liberté d'expression, la vie privée de l'individu et le respect de droits de l'homme, et plaidait pour la neutralité du réseau, afin d'empêcher toute limitation des flux pour des raisons d'ordre politique, commercial, religieux ou autre. C'est dans ce contexte que la présidente du Brésil **annonça** en octobre **l'organisation d'une conférence mondiale sur la gouvernance de l'Internet en avril 2014, à São Paulo**.

Entre temps, **le 7 octobre 2013, les dirigeants des organismes** responsables de la coordination des infrastructures **techniques de l'Internet** – les 5 registres régionaux, l'ICANN, l'IETF, le W3C, l'IAB et l'ISOC – avaient eux aussi réagi conjointement aux révélations sur la surveillance massive. Inquiets d'une possible fragmentation nationale de l'Internet, ils **ont appelé, dans la déclaration de Montevideo** sur l'avenir de la coopération pour l'Internet[2], **à accélérer la mondialisation de l'ICANN et des fonctions IANA**. Dans cette perspective, ils ont également lancé un forum de dialogue en ligne appelé « 1net »[3] et destiné à élaborer des solutions collaboratives. Comme l'a explicité devant votre mission, quelques

[1] *Cette enquête a abouti en mars 2014, avec l'adoption du rapport de M. Claude Moraes au nom de la commission des libertés civiles du Parlement européen.*
[2] *http://www.Internetsociety.org/news/montevideo-statement-future-Internet-cooperation*
[3] *http://1net.org/*

mois plus tard, M. Fadi Chehadé, président de l'ICAN : « *l'ICANN détient l'une des treize racines, la racine L, qui a comme les autres des centaines de réplications à travers le monde. L'enjeu est moins le nombre d'opérateurs que la capacité à y faire des modifications. Si vous créez « .paris », par exemple, les treize opérateurs sont automatiquement informés, et le Département du commerce américain doit donner son accord. Il est temps de substituer à cette dernière étape un mécanisme international – voilà l'enjeu de la réforme de l'IANA*. »

Travaillant de concert, l'Allemagne et le Brésil ont tenu à mobiliser les Nations unies pour souligner le caractère mondial de l'indignation soulevée par les révélations sur la surveillance massive en ligne. Ces deux pays ont donc soumis à l'**Assemblée générale des Nations unies** un projet de **résolution sur le droit à la vie privée à l'heure numérique**, qui a été adopté par consensus en **novembre 2013**. L'Assemblée de l'ONU y affirme que les droits dont chacun bénéficie dans le monde physique (*offline*) doivent être pareillement garantis sur l'Internet (*online*), y compris le droit à la vie privée. Invoquant la Déclaration universelle des Droits de l'Homme et les traités pertinents, tels que le Pacte international relatif aux droits civils et politiques et le Pacte international relatif aux droits économiques, sociaux et culturels, elle invite aussi les États à revoir leurs procédures, pratiques et législations en matière de surveillance, d'interception et de collecte de données personnelles pour assurer leur conformité à l'égard de leurs obligations découlant du droit international en matière de protection des droits de l'homme.

Ainsi que le souligne M. Mathieu Weill, « *l'**affaire Snowden a fait perdre toute légitimité morale aux États-Unis qui, jusqu'alors, se présentaient comme les défenseurs des libertés** […]. L'affaire Snowden est l'électrochoc qui permet de comprendre que le* statu quo *n'est pas tenable.* »

B. L'ÈRE DU SOUPÇON ET LES EFFORTS DE « CONTAINMENT » DU RISQUE DE BALKANISATION DU WEB

L'électrochoc Snowden a donc fait basculer l'ensemble des internautes dans une ère de soupçon à l'égard des États-Unis, qui vient accélérer une tendance à la fragmentation de l'Internet, déjà avérée.

1. La fragmentation de l'Internet, un risque déjà avéré

En donnant aux États une motivation légitime pour retrouver autant que possible leur souveraineté sur l'Internet, l'action de surveillance de masse menée par les États-Unis menace l'architecture globale de l'Internet d'un risque systémique de fragmentation en blocs. La question qui se pose alors est de savoir **comment rétablir la confiance des internautes et la sécurité en ligne tout en maintenant l'unicité du réseau**.

a) Une fragmentation de l'Internet déjà à l'œuvre par stratégie souveraine ou commerciale

Comme cela a déjà été dit plus haut, l'Internet représente un défi aux États souverains. Certains ont déjà tenté d'y répondre par le filtrage voire la censure ou même la fermeture de leur réseau. Ils cherchent ainsi à reprendre la main sur l'Internet comme instrument de puissance.

Mme Pauline Türk a évoqué devant votre mission les **tentations d'États**, souvent parmi les moins libéraux, **de développer des résistances** sous des formes et par des moyens variés, **qui vont de la tentative de prise de contrôle du réseau au boycott et à la création de réseaux indépendants**[1] : les États « *peuvent durcir la législation nationale permettant de réprimer toute une série d'infractions commises sur Internet, ce qui restreint la liberté des échanges sur le réseau, comme au Venezuela en 2010 ou en Russie en 2012. Ils peuvent prendre le contrôle d'un serveur national, ou mettre sous tutelle les fournisseurs d'accès, afin de pouvoir plus facilement ralentir ou bloquer l'accès à certains contenus, et tracer les utilisateurs : c'est le cas en Libye, Syrie, Belarus, Kazakhstan, Turquie, Thaïlande, Vietnam, Arabie Saoudite… Non seulement le principe fondamental de neutralité du réseau est mis en cause du fait d'une gestion potentiellement discriminatoire du trafic, mais cette recentralisation du réseau a déjà permis – en Moldavie en 2009, en Égypte en 2011, ou en Syrie en 2012 – à des pouvoirs autoritaires menacés de provoquer un* « Internet blackout » *de plusieurs heures ou plusieurs jours. Une soixantaine de pays seraient ainsi « à risque » de coupure généralisée, du fait de la faible décentralisation de leur réseau.* »

Certains États ont même entrepris de créer des racines alternatives au *Domain Name System* (DNS) ou de se doter de leur propre réseau, exposant leur population au risque de l'isolement et le réseau Internet, à se retrouver compartimenté en de multiples espaces virtuels partiellement communicants : « *Après la Corée du Nord en 2002 et la Birmanie en 2010, l'Iran a ainsi annoncé, en septembre 2012, le lancement de son propre réseau national, permettant de « protéger sa population des influences étrangères » et de « proposer une gamme de services localement adaptés »*. » La Chine a déjà mis en place son *Great Firewall*[2] et l'Inde travaillerait à la création d'un réseau concurrent.

M. Julien Nocetti a insisté devant votre mission sur **les causes géopolitiques et les rapports de forces ayant conduit à l'apparition de réseaux autonomes et souverains** par défiance envers le modèle dominant occidental : « *Chine, Russie, Brésil, Inde, Turquie […] ont fait le constat que l'Internet est devenu un sujet de politique étrangère au sens classique du terme, c'est-à-dire où les rapports de force entre États - et acteurs économiques soutenus par des États - jouent un rôle central. Dans des pays comme la Chine et la Russie, le numérique bouleverse les équilibres traditionnels de pouvoir […] L'Internet est*

[1] Cf. *également « La souveraineté des États à l'épreuve d'Internet »* – Revue de droit public, *Pauline Türk, décembre 2013*

[2] *Google est interdit en Chine continentale depuis le 1er juillet 2010, Facebook, Twitter, et YouTube depuis 2009.*

rapidement devenu un enjeu de stabilité et de légitimité politique pour leurs gouvernants. […] L'asile de Snowden en Russie participe, on le voit bien, d'une entreprise visant à signifier ouvertement de nouveaux rapports de force dans la géopolitique complexe de l'Internet et des données. Et cette géopolitique, la Russie l'a investie depuis longtemps : rappelons que Moscou soumet depuis 1998 des résolutions à l'ONU sur la « souveraineté de l'information » ou la « sécurité de l'information ». […] La Chine, elle, défend l'idée d'une souveraineté numérique sophistiquée qui lui permettrait de mieux contrôler ce qui se passe sur le web chinois. Pékin a acheté d'importants stocks d'adresses IP afin de favoriser la circulation des données à l'intérieur du pays. »

À côté des motifs politiques, il convient de ne pas sous-estimer les enjeux économiques, qu'il s'agisse de protectionnisme étatique à l'image de la Chine ou de stratégies purement commerciales. Ainsi, les modèles économiques des grands fournisseurs de services et de contenus reposent sur le financement publicitaire corrélé à un fichier de données d'internautes, lesquels sont autant de clients potentiels. La maîtrise de ces données constitue une source de revenu stratégique qui pousse les entreprises telles que Google, Facebook et Yahoo à restreindre leurs échanges de données, voire à rendre incompatible toute recherche mutuelle ou tout échange de contacts. Ainsi, Google et Facebook bloquent réciproquement tout transfert de données entre leurs applications depuis 2010. Plus récemment Yahoo a rompu les ponts avec Facebook et Google[1] afin de conserver la maîtrise de son application *Flickr* de partage photographique. Cette **fragmentation entre les services de réseaux sociaux** a pour objet de conserver la maîtrise respective de leurs utilisateurs et de la monétisation dont ils font l'objet sur le marché publicitaire.

Cette fragmentation des services, à distinguer de la fragmentation des réseaux ou des protocoles utilisés pour le transfert des données sur l'Internet, entrave la **portabilité des données personnelles** que souhaite voir mise en œuvre Viviane Reding, vice-présidente en charge de la justice, des droits fondamentaux et de la citoyenneté de la Commission européenne.

b) Le risque d'une balkanisation consommée

Cette fragmentation croissante de l'Internet se trouve accélérée et alimentée par les révélations de M. Edward Snowden. M. Julien Nocetti indique que de nombreux « *pays dénoncent les doubles standards de Washington qui, tout en prêchant l'abolition des frontières numériques, enregistre et exploite des* big data *sans le moindre contrôle* ».

Or, s'agissant des services comme du réseau, votre mission estime que la **fragmentation de l'Internet n'est bénéfique ni pour les États, ni pour les internautes**. Pour M. Louis Pouzin, « *la fragmentation […] existe depuis longtemps. Google, Facebook, Twitter, reposent sur ce principe. Ils sont chacun*

[1] *Source : http://www.linformaticien.com/actualites/id/33402/flickr-yahoo-rompt-les-ponts-avec-facebook-et-google.aspx*

propriétaire de leur système, qui est opaque. C'est aussi le cas en Chine, avec Baidu, même si ce système ne correspond pas du tout au même que le nôtre. La diversification des usages explose donc, ce qui peut être bon, mais demeure incontrôlée, et sous la coupe de géants qui font ce qu'ils veulent. Il n'existe aucune normalisation, ni aucun accord commercial précis entre les différents pays. On se dirige vers le chaos ! Le fait que Google, Facebook et Twitter aient des systèmes de noms différents résulte d'un choix, afin d'avoir une clientèle qui ne puisse aisément passer d'un système à l'autre. Autrement dit, la fragmentation et la diversification sont souvent voulues par les industriels, pour leur permettre d'avoir des marchés captifs, et non dans l'intérêt des utilisateurs ! »

La tentation de localiser les données dans des frontières nationales est également jugée contreproductive par M. Bertrand de La Chapelle, directeur du projet Internet et juridiction, ancien délégué spécial pour la société de l'information au ministère des affaires étrangères (2006-2010), ancien directeur au conseil d'administration de l'ICANN, qui appelle à se méfier de « *notre propension à renouer avec le cadre familier de la frontière.* » Il considère que « *pousser trop loin la logique de souveraineté, notamment en militant pour des* clouds *nationaux, pourrait nous faire perdre une bonne part des bénéfices que le partage des infrastructures et le* cloud *peuvent apporter. Certes, les abus constatés ne sont pas admissibles, mais préconiser, pour y remédier, la relocalisation des données et le* cloud *national reste une vue de court terme, qui pourrait provoquer une fragmentation, source de dommages irréparables à long terme.* » M. Fadi Chehadé, président de l'ICANN, n'est pas favorable à « *l'idée d'un Internet allemand ou européen avec des responsables allemands. La fragmentation de l'Internet serait très dangereuse. Même les Chinois, avec leurs 620 millions d'utilisateurs, n'en veulent pas : leurs applications sont utilisées par des centaines de millions d'utilisateurs hors de Chine. Personne ne veut voir se fragmenter la base d'Internet – ce qui n'interdit pas des adaptations régionales et nationales.* »

Comme l'a fait observer à votre mission M. Maurice Ronai, « ***la fragmentation, la surveillance de masse et la centralisation autour de quelques acteurs – se nourrissent et se renforcent mutuellement***. *La centralisation des usages et des trafics autour de quelques plateformes a considérablement facilité la tâche de la NSA* ». Ainsi, un Internet fracturé contredirait l'esprit d'ouverture de l'Internet et tendrait à donner des moyens de censure supplémentaires à ceux qui contrôlent ces blocs fermés.

Après les révélations d'Edward Snowden et le risque induit de balkanisation du net, le défi est donc de s'assurer de la protection de l'universalité, de l'intégrité et de l'ouverture de l'Internet.

2. Sous pression, les États-Unis annoncent la privatisation de la gestion des ressources critiques de l'Internet pour éviter la balkanisation du réseau

Les révélations d'Edward Snowden ont décrédibilisé les États-Unis comme garants de la liberté en ligne et ont mis à mal le soutien de l'industrie du net au gouvernement démocrate de M. Barack Obama. La pression politique externe s'est également accrue, poussant les États-Unis à reprendre l'initiative.

a) Une réponse d'abord hésitante des États-Unis confrontés à la colère du Brésil et de l'Allemagne face aux excès de la surveillance en ligne

En réponse à l'indignation générale, la première initiative prise par le président Obama en août 2013 fut de mandater un groupe d'experts pour proposer à la Maison blanche les moyens d'assurer la sécurité des États-Unis tout en respect leur engagement pour les libertés, de restaurer la confiance, notamment celle des alliés des États-Unis, et enfin de prévenir le risque de nouvelles « fuites ».

C'est en décembre 2013 que ces cinq experts ont remis au président Obama leur rapport, intitulé *Liberty and Security in a changing world*[1].

Ce rapport préconisait des réformes destinées à mieux canaliser les pouvoirs exorbitants qu'avait acquis la NSA, à l'égard des citoyens américains mais également non américains : il suggérait ainsi que le gouvernement américain applique de la même manière le *Privacy Act* de 1974 aux citoyens américains et non américains, et que la NSA privilégie l'espionnage ciblé plutôt que la collecte aveugle de données.

L'un des objectifs affichés du rapport était de contribuer à maintenir l'Internet sûr et ouvert, ce que les experts eux-mêmes reconnaissent comme extrêmement important. Afin de restaurer la confiance en ligne, le rapport invite notamment le gouvernement américain à être plus transparent quant au nombre et au type de requêtes qu'il adresse aux fournisseurs de communications électroniques.

En outre, il préconise la nomination d'un adjoint au secrétaire d'État en charge de la diplomatie pour les questions internationales relatives aux technologies de l'information, afin de promouvoir un modèle de gouvernance de l'Internet inclusif pour toutes les parties prenantes appropriées, et pas seulement les gouvernements.

Les conclusions de ce **rapport d'experts adressé à la Maison blanche** répondaient à la colère principalement exprimée par deux pays alliés des États-Unis, le Brésil et l'Allemagne, dont les deux dirigeantes avaient notamment appris avoir eu leur téléphone mobile espionné.

---

[1] *Richard A. Clarke, Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein et Peter Swire.*

Dans ce contexte tendu au terme de six mois de controverse sur les activités de surveillance massive aux États-Unis, le **discours sur l'état de l'Union du président des États-Unis, le 17 janvier 2014**, était très attendu. Il a annoncé des « *réformes concrètes et substantielles* » à mettre en œuvre avec le Congrès pour mieux encadrer le traitement par la communauté américaine du renseignement des données personnelles sans distinction liée à la nationalité ou au lieu de résidence des personnes visées. Affichant le souci de mieux concilier sécurité et liberté, le président Obama n'a pourtant pas convaincu les alliés des États-Unis, déçus du peu de cas qu'il faisait de leur préoccupation – plus ou moins forte selon les pays, des révélations ultérieures sur les activités de leurs propres services de renseignement expliquant sans doute l'attitude relativement conciliante de certains États démocratiques. Si le président Obama esquissait des pistes de réformes éventuelles à apporter au cadre juridique américain suite aux révélations d'Edward Snowden, ces pistes visaient essentiellement à améliorer la protection des citoyens américains à l'égard de leurs agences de renseignement. Pour les citoyens non américains, M. Obama a reconnu la nécessité de renforcer la protection de leur vie privée[1], mais sans leur garantir à terme une protection juridique solide, notamment un droit de recours en justice facile d'accès, laissant de côté les préconisations du rapport d'experts à la Maison Blanche sur ce point. Il a seulement assuré les chefs d'État et de gouvernement « *des amis intimes et alliés des États-Unis* » qu'ils ne seraient plus surveillés.

À ce stade, la réponse américaine est apparue insuffisante à restaurer la confiance dans l'Internet.

C'est pourquoi, **en février 2014, la chancelière allemande, Mme Angela Merkel, remettait de l'huile sur le feu en appelant de ses vœux un « Internet européen »**. Votre mission avait alors réagi par un communiqué[2] convenant de la nécessité, pour l'Europe, de ne pas se résigner à la perte de contrôle sur ses données, mais soulignant aussi le flou de cette proposition allemande, qui pouvait faire craindre une balkanisation du net.

En **mars 2014**, l'enquête initiée par le Parlement européen a abouti, avec l'**adoption du rapport de M. Claude Moraes au nom de la commission des libertés civiles du Parlement européen**[3]. Ce rapport juge que la

---

[1] "We will provide additional protections for activities conducted under Section 702, which allows the government to intercept the communications of foreign targets overseas who have information that's important for our national security. Specifically, I am asking the Attorney General and DNI to institute reforms that place additional restrictions on government's ability to retain, search, and use in criminal cases, communications between Americans and foreign citizens incidentally collected under Section 702".

[2] *http://www.senat.fr/presse/cp20140219.html*

[3] *Rapport du 21 février 2014 sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures (2013/2188(INI)).*

surveillance de masse mise en œuvre par les États-Unis ne fait aucun doute. Il avance plusieurs constats et recommandations visant très directement, et de manière critique, le gouvernement américain en estimant « *que les récentes révélations faites dans la presse par des lanceurs d'alerte et des journalistes, ainsi que les témoignages d'experts recueillis pendant cette enquête, les aveux des autorités et l'insuffisance de la réaction face à ces allégations, ont permis d'obtenir des preuves irréfutables de l'existence de systèmes vastes, complexes et technologiquement très avancés conçus par les services de renseignement des États-Unis et de certains États membres* […] ».

Parmi les principales recommandations, il est proposé au Parlement européen d'enjoindre aux États-Unis :

« – *d'interdire les activités de surveillance de masse aveugle ;*

– *de placer les droits des citoyens de l'Union européenne sur un pied d'égalité avec ceux des ressortissants des États-Unis ;*

– *d'adhérer à la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (convention n° 108) du Conseil de l'Europe, comme ils ont adhéré à la convention de 2001 sur la cybercriminalité, renforçant ainsi le fondement juridique commun entre les alliés transatlantiques.* »

En outre, le rapport « Moraes » estime :

– d'une part, à titre défensif, « *que l'approbation du TTIP final par le Parlement européen pourrait être menacée tant que les activités de surveillance de masse aveugle et l'interception des communications au sein des institutions et des représentations diplomatiques de l'Union européenne n'auront pas été complètement abandonnées et qu'une solution adéquate n'aura pas été trouvée en ce qui concerne les droits des citoyens de l'Union européenne en matière de confidentialité des données* » ;

– d'autre part, à titre offensif sur le plan industriel, « *que les révélations en matière de surveillance de masse qui ont provoqué cette crise peuvent être l'occasion pour l'Europe de prendre l'initiative pour mettre en place, en tant que mesure stratégique prioritaire, une capacité autonome de ressources informatiques clés* ».

b) L'annonce de l'intention des États-Unis de ne plus superviser la racine de l'Internet : une concession qui ne doit pas se transformer en mirage

Prenant tout le monde de court, **le gouvernement américain annonçait, le 14 mars 2014, son intention de se retirer de la supervision de la gestion du fichier de la zone racine du système des noms de domaine (DNS)**, c'est-à-dire des fonctions IANA que l'ICANN assure pour son compte. De nombreuses parties prenantes s'attendaient plutôt à un mouvement américain lors de la conférence NETmundial de São Paulo.

Gestionnaire historique du DNS, le gouvernement américain, et plus spécifiquement l'administration nationale des télécommunications et de

l'information (*National Telecommunications and Information Administration* – NTIA) du Département du commerce, garde aujourd'hui la responsabilité d'autoriser les changements au fichier de la zone racine, qui est la base de données contenant les listes de noms et adresses de tous les domaines de premier niveau.

C'est à cette responsabilité consistant à autoriser tout changement dans la zone racine du DNS que le gouvernement américain propose de renoncer, mais **en posant ses conditions**. **C'est à l'ICANN que la NTIA confie le processus de transition, lequel devra respecter quatre principes** :

– soutenir le modèle multi-parties prenantes ;

– maintenir la sécurité, la stabilité et la résilience du système de noms de domaine de l'Internet ;

– satisfaire les besoins et attentes des clients et partenaires mondiaux des services IANA ;

– préserver le caractère ouvert de l'Internet.

La NTIA laisse donc la main à l'ICANN, tout en indiquant que **le processus ne saurait aboutir à une solution menée par les gouvernements ou par une organisation intergouvernementale** et que le gouvernement américain devra valider la proposition de l'ICANN. Sans fixer d'échéance pour mener à bien le processus, la NTIA rappelle que le contrat sur les fonctions IANA, qui lie le Département du commerce à l'ICANN, expire le 30 septembre 2015[1].

Lors de son entrevue à **Washington** avec la délégation de votre mission, M. Lawrence Strickling, secrétaire d'État-adjoint et directeur de la NTIA, **a indiqué que cette annonce était dénuée de tout lien avec les révélations d'Edward Snowden** ; il a fait valoir que ce retrait envisagé par le gouvernement américain s'inscrivait dans la continuité de son projet de privatisation complète de la gestion du système de noms de domaine. En créant l'ICANN en 1998, le gouvernement américain avait effectivement initié un mouvement vers la « privatisation » du système de noms de domaine (DNS) : il s'était agi de transférer les fonctions auparavant assurées par l'IANA (*Internet Assigned Numbers Authority*), un organisme contractant du gouvernement américain, vers un nouvel organisme privé, à savoir l'ICANN. Le gouvernement américain s'était toutefois ménagé alors un rôle temporaire, auquel il se dit aujourd'hui prêt à renoncer « *au vu de la maturité acquise par l'ICANN et des progrès qu'elle a effectués en termes de transparence et de responsabilité comme de compétence technique* ».

Cette annonce répond à une demande ancienne, déjà exprimée par l'Union européenne lors du SMSI de 2005, mais toujours écartée par les États-Unis. Comme l'a rappelé M. Jean-Michel Hubert lors de son audition

[1] *L'*affirmation of Commitments *entre l'ICANN et le Département du commerce ne comprend pour sa part aucune date d'expiration.*

par votre mission, « *la dernière réunion préparatoire au sommet de Tunis, qui s'était tenue à Genève, avait vu le Royaume-Uni, qui assurait alors la présidence de l'Union européenne, proposer le schéma d'un nouveau modèle de coopération pour la gestion d'Internet, qui incluait des principes de politiques publiques applicables à l'échelle mondiale – et qui remettait en cause le lien privilégié entre l'ICANN et le gouvernement américain. Or cette proposition européenne, bien reçue par les États asiatiques et sud-américains, avait été repoussée sans discussion possible par les États-Unis, ce qui explique qu'il n'en n'ait pas été fait mention dans la déclaration finale de novembre 2005.* »

Le rapport des experts à la Maison Blanche de décembre 2013, évoqué plus haut, **esquissait déjà ce changement comme un élément de réponse à l'affaire Snowden** : « *Nous sommes conscients que certains changements dans les approches de gouvernance pourraient être souhaitables pour refléter l'évolution des pratiques de communications. Par exemple, il serait peut-être temps de jeter un regard critique sur la relation unique entre les États-Unis et l'ICANN. Le rôle actuel des États-Unis est un artéfact des débuts de l'Internet et pourrait ne pas être bien adapté à l'ensemble plus large des parties prenantes engagées dans la gouvernance Internet aujourd'hui. Le gouvernement des États-Unis et ses alliés, cependant, devraient néanmoins continuer à s'opposer au transfert de la gouvernance de l'Internet vers un forum, comme l'Union internationale des télécommunications, où les États-nations dominent le processus, souvent à l'exclusion des autres. Nous croyons qu'une telle évolution dans la gouvernance menacerait la prospérité, la sécurité et l'ouverture des communications en ligne* ».

L'analyse de votre mission est qu'effectivement, le moment auquel intervient cette annonce n'est pas sans lien avec « l'affaire Snowden » : intervenue quelques semaines avant la tenue du NETmundial, qui risquait de donner écho à de nombreuses revendications pour une reprise en main gouvernementale de la gouvernance de l'Internet, cette **annonce** est venue désamorcer ce risque en **mettant en cohérence le discours multi-parties prenantes des États-Unis avec l'état de fait, qui en est fort éloigné** tant qu'un seul État garde finalement la main sur la racine du DNS.

Cette annonce a aussitôt suscité des **résistances en interne aux États-Unis**. Face aux remous provoqués, la NTIA a été contrainte, quelques jours après, de publier un nouveau communiqué pour lever certains malentendus et démentir ceux qui dénonçaient le fait que les États-Unis abandonnaient l'Internet. Ce communiqué attestait aussi du soutien à l'annonce gouvernementale des grands acteurs industriels américains du net, de plusieurs *think tanks* et de certains parlementaires républicains comme plusieurs démocrates.

Il n'est pourtant **pas évident que la NTIA parvienne à convaincre le Congrès**. Une délégation de votre mission a pu s'entretenir à Washington

avec le représentant républicain John Shimkus, élu de l'Illinois[1], qui a déposé un texte[2] tendant à évaluer sérieusement la proposition du NTIA. Son objectif est de faire établir d'ici un an un rapport indépendant par le *Government Accountability Office* pour mesurer l'impact d'un tel retrait de la supervision du net et mieux cerner les parties prenantes à qui serait confiée cette supervision. Il a tactiquement fait valoir le caractère raisonnable de sa démarche, par rapport à celles engagées par deux de ses collègues, également républicains : M. Duffy, visant à interdire purement et simplement à la NTIA d'abandonner son rôle sur le DNS[3], et M. Kelly, soumettant cette décision à l'approbation formelle du Congrès[4]. Lors de l'entretien, M. Shimkus a justifié sa démarche par une méfiance globale de son parti à l'égard de l'administration Obama, relevant au passage que l'annonce de la NTIA était intervenue un vendredi après-midi, sans doute afin d'éviter trop de bruit médiatique.

Depuis cet entretien, le texte a été inscrit à l'ordre du jour de la Commission Énergie et Commerce de la Chambre des représentants et approuvé début mai ; c'est finalement par le biais d'un amendement au projet de loi annuel de financement du Département de la défense que ce texte a été adopté par la Chambre des représentants le 22 mai dernier. Inquiets d'une reprise en main de l'Internet par des régimes autoritaires et des risques de censure afférents, 17 Démocrates ont rejoint les Républicains pour adopter cette mesure. Sans doute cette dernière sera-t-elle néanmoins écartée par le Sénat américain, à majorité démocrate. Mais les élections de mi-mandat en novembre prochain pourraient faire perdre aux Démocrates cette courte majorité[5] qu'ils ont encore au Sénat…

Malgré sa contestation croissante au sein du Capitole, qui confirme les promoteurs d'une gouvernance intergouvernementale sur l'Internet dans leur mobilisation, **l'annonce du gouvernement américain a en tout cas permis aux États-Unis de ne pas se présenter au NETmundial de São Paulo en position de faiblesse** et leur a évité de s'exposer à la dénonciation d'un décalage entre le modèle multi-parties prenantes qu'ils prônent et le pouvoir qu'ils exercent en fait sur l'Internet.

Paradoxalement, la résistance que rencontre cette annonce au Congrès accrédite l'idée que la supervision du gouvernement américain sur le système des noms de domaine ne peut être considérée comme un simple « *artéfact* » des débuts de l'Internet. Elle occulte aussi le fait que **le retrait annoncé par la NTIA n'est que partiel** : comme l'a fait observer

[1] *Membre du* House Energy & Commerce Subcommittee on Communications and Technology.
[2] *H.R. 4342,* The Domain Openness Through Continued Oversight Matters *(DOTCOM), Act of 2014.*
[3] *H. R. 4398,* Global Internet Freedom, *Act of 2014.*
[4] *H. R. 4367,* Internet Stewardship, *Act of 2014.*
[5] *5 sièges de plus que les Républicains. Un tiers des sièges du Sénat doit être renouvelé en novembre prochain et les Démocrates doivent en défendre davantage (21) que les Républicains (15).*

M. Maurice Ronai à votre mission lors de son audition, on compte deux acteurs dans la gestion du serveur racine du *Domain name system* (DNS), l'ICANN et la société privée VeriSign, la première enregistrant les noms de domaine de premier niveau (TLD), la seconde effectuant dans la racine les modifications subséquentes, sur ordre du gouvernement américain. Or, en ne citant pas VeriSign dans son communiqué du 14 mars, l'administration américaine semble juger que son rôle n'est pas à débattre. Lors de sa récente audition, M. David Martinon a indiqué à votre mission que M. Strickling lui avait confirmé que les États-Unis n'avaient aucunement l'intention de faire évoluer leur **relation privilégiée avec VeriSign**, consignée dans un accord de coopération.

3. Les avancées du NETmundial de São Paulo n'épuisent pas le besoin de réforme de la gouvernance mondiale de l'Internet

Quelques semaines après cette annonce spectaculaire, s'est donc tenu, les 23 et 24 avril à São Paulo, le rendez-vous mondial sur la gouvernance de l'Internet convoqué par le Brésil, avec l'ICANN et d'autres États, dont la France.

a) Le NETmundial : des principes et une méthode de gouvernance sous onction brésilienne

C'est ainsi que la **conférence NETmundial** qui s'est tenue à São Paulo fin avril n'a pas donné lieu à la levée de boucliers redoutée contre les États-Unis, mais a plutôt été l'occasion pour le Brésil de se mettre en avant, ce qui servait aussi les objectifs de politique intérieure de Mme Rousseff en vue des prochaines élections présidentielles d'octobre. Ce d'autant plus que le Brésil venait de se doter la veille du NETmundial d'une loi-cadre sur l'Internet, *Marco civil da Internet,* consacrant les grands principes fondateurs d'un Internet ouvert, notamment la neutralité du réseau, et soumettant au juge tout retrait de contenu en ligne.

Le président de l'ICANN ayant déployé à cet effet une diplomatie active auprès du Brésil, la conférence, que Mme Rousseff imaginait initialement intergouvernementale, a finalement réuni toutes les parties prenantes et accueilli près d'un millier de personnes : représentants des gouvernements, secteur privé, société civile, communauté technique, communauté académique et utilisateurs. Mme Axelle Lemaire, qui venait d'être nommée secrétaire d'État chargée du numérique, auprès du ministre de l'économie, du redressement productif et du numérique, y a participé au nom de la France.

La conférence s'est **focalisée sur l'établissement de principes pour la gouvernance de l'Internet, ainsi que d'une feuille de route** pour le développement futur de cet écosystème. Après avoir traité l'ensemble des

contributions, un comité exécutif multipartite[1] a élaboré un projet de texte. Ce projet a été soumis à un comité multipartite de haut niveau, composé par des représentants ministériels de douze pays, dont la France[2], et douze membres de la communauté internationale multipartite. Ce comité incluait aussi des représentants de l'UIT, du Département des affaires économiques et sociales (DESA) de l'ONU et de la Commission européenne.

Votre mission considère comme une avancée significative la déclaration finale du NETmundial[3], adoptée par consensus et non contraignante.

D'emblée, le texte reconnaît l'Internet comme une ressource mondiale qui doit être gérée dans l'intérêt public. Après avoir disposé que les droits dont chacun bénéficie *offline* doivent être protégés en ligne – en accord avec les traités internationaux sur les droits de l'Homme –, **il consacre certains principes et valeurs** : liberté d'expression, liberté d'association, droit à la vie privée, accessibilité, liberté d'information et d'accès à l'information, droit au développement… Il confirme la protection dont doivent bénéficier les intermédiaires techniques. Il affirme le respect de la diversité linguistique et culturelle.

Concernant l'architecture technique de l'Internet, il affirme son unité, sa stabilité et sa résilience, son caractère ouvert et distribué, sa vocation à permettre l'innovation et la créativité. Il promeut les standards ouverts.

Enfin, il identifie plusieurs principes à appliquer au processus de gouvernance de l'Internet : multi-parties prenantes, ouvert, participatif, fondé sur le consensus, transparent, responsable, inclusif et équitable, distribué, collaboratif, permettant une participation significative de tous, accessible et agile.

Du point de vue du Gouvernement français, ce texte offre plusieurs motifs de satisfaction, comme l'a souligné M. David Martinon devant votre mission :

– la mention explicite des droits d'auteur : « *Everyone should have the right to access, share, create and distribute information on the Internet, consistent with the rights of authors and creators as established in law* » ;

– la limitation des responsabilités des intermédiaires sur l'Internet, en une formulation déjà agréée avec peine à l'OCDE : « *Intermediary liability limitations should be implemented in a way that respects and promotes economic growth, innovation, creativity and free flow of information* ». Sur ce point,

---

[1] *Composé de neuf membres internationaux, y compris des représentants de la communauté technique, civile et universitaire, ainsi que du secteur privé et du Département des affaires sociales et économiques des Nations unies.*

[2] *Ainsi que l'Argentine, le Brésil, le Ghana, l'Allemagne, l'Inde, l'Indonésie, l'Afrique du Sud, la Corée du Sud, la Tunisie, la Turquie et les États-Unis.*

[3] *Qui figure en annexe du présent rapport.*

M. Martinon dit avoir dû créer une coalition – qui l'a surpris lui-même – avec les représentants de Walt Disney et de la Fox, contre un certain nombre de représentants de la société civile ;

– la mention de la nécessaire coopération de toutes les parties prenantes dans la lutte contre les activités illégales sur l'Internet, y compris le piratage : « *In this regard, cooperation among all stakeholders should be encouraged to address and deter illegal activity* » ;

– la mention de la recherche de la diversité culturelle sur l'Internet, en ligne avec la convention de l'UNESCO sur la diversité culturelle.

Même s'il insiste sur le caractère ouvert de l'Internet, le texte n'a pas su traiter de la question de la neutralité du net, faute de consensus entre les parties prenantes présentes à São Paulo. Sans doute ce sujet sensible qui touche à la répartition de la valeur sur l'Internet apparaît-il, répertorié parmi les sujets de discorde, mais votre mission relève que c'est la première fois qu'il se trouve évoqué dans un texte de niveau international.

S'agissant de la surveillance en ligne, la rédaction retenue reprend le texte de la résolution adoptée par l'Assemblée générale des Nations unies, à l'initiative du Brésil et de l'Allemagne. On le retrouve dans la première comme dans la seconde partie de la déclaration finale du NETmundial de São Paulo. Votre mission se félicite que le texte vise à la fois la collecte et le traitement de données personnelles par les acteurs étatiques et non-étatiques.

La déclaration du NETmundial caractérise la **gouvernance multi-parties** prenantes d'une manière **souple, ce qui représente une avancée** : « *Internet governance should be built on democratic, multistakeholder processes, ensuring the meaningful and accountable participation of all stakeholders, including governments, the private sector, civil society, the technical community, the academic community and users. The respective roles and responsibilities of stakeholders should be interpreted in a flexible manner with reference to the issue under discussion* ». Les parties prenantes ne doivent donc pas avoir le même rôle et la même voix au chapitre, toutes les questions d'ordre public relevant notamment de la compétence exclusive des États. En même temps, les États ont un besoin vital et immédiat de la coopération des autres parties prenantes pour être efficaces dans ces domaines.

En outre, l'accent a été mis sur la **nécessité de la transparence et de la redevabilité** avec la reconnaissance du rôle et des responsabilités particulières des États, qui ont eux aussi à rendre des comptes à leurs citoyens : « *Governments have primary, legal and political accountability for the protection of human rights* ». La qualité d'une gouvernance *accountable* est même reconnue comme devant reposer sur des mécanismes permettant des *checks and balances* indépendants et sur des possibilités d'examen et de réparation des décisions.

La seconde partie du texte traite de la feuille de route pour le futur de la gouvernance de l'Internet. Elle réaffirme la nécessité, reconnue par l'Agenda de Tunis, d'une « coopération renforcée » sur les sujets de politique publique internationale. L'ambition de globalisation de l'ICANN y est collectivement validée et confirmée ; il est demandé de l'accélérer pour arriver à une organisation véritablement « *internationale et globale* » – les deux mots sont dans le texte – « *afin de servir l'intérêt public, avec des mécanismes de transparence et de redevabilité clairement vérifiables et faciles à mettre en œuvre, qui rencontrent les attentes des parties prenantes internes à l'ICANN et de la communauté globale* ».

Même si elle se félicite des objectifs ainsi fixés, votre mission relève que **cette feuille de route reste évasive et ne fixe pas d'étapes** pour arriver au but proclamé.

Alors que le risque était d'entériner au NETmundial une balkanisation de l'Internet aux seules fins d'échapper à la mainmise américaine, **il ressort finalement du NETmundial un texte qui condamne** heureusement ces **pratiques de surveillance, mais qui ne renonce pas pour autant à l'unicité et l'ouverture de l'Internet**. Ce résultat, obtenu en deux jours de conférence préparés en seulement six mois, constitue une réelle avancée. Votre mission salue le fait qu'à l'invitation d'une grande démocratie de l'hémisphère Sud – le Brésil –, le NETmundial valide l'Internet comme nouveau média mondial d'expression libre.

b) Mais la réforme de l'écosystème de gouvernance de l'Internet reste à faire

Les conclusions du NETmundial affirment et réaffirment la nécessité d'impliquer toutes les parties prenantes, dans le respect de « leur rôle respectif », ce qui s'apparente à la formule de l'Agenda de Tunis adopté en 2006 à l'issue du SMSI organisé par l'ONU. Mais la référence – quinze fois dans le texte – au modèle « *mutistakeholders* » relève de l'incantation, comme si son énonciation suffisait à le rendre effectif. Cela n'a d'ailleurs pas suffi à convaincre certains États, au premier chef l'Inde, grande démocratie qui n'a pas souscrit aux conclusions du NETmundial. **Le rôle des parties prenantes, et particulièrement celui des États, reste effectivement à débattre**, même, voire surtout, si les États-Unis renoncent à superviser le système.

Ainsi, l'avancée que représente la déclaration du NETmundial laisse ouvertes plusieurs questions, d'autant plus qu'elle consacre le caractère démocratique de la gouvernance multi-parties prenantes et qu'elle insiste sur sa redevabilité.

D'une part, **l'ICANN reste fondamentalement américaine**, même si elle déploie des efforts d'internationalisation. Comme l'a fait valoir M. Fadi Chehadé, président de l'ICANN, à votre mission, le siège social de l'ICANN devrait être répliqué : en complément du siège de Los Angeles s'ajoute déjà le bureau « *hub* » d'Istanbul, et il est prévu d'en créer un autre à Singapour. En outre, des bureaux d'enregistrement devraient être ouverts à Pékin et

Montevideo, en plus de Washington et Bruxelles. En matière linguistique, la libéralisation des noms de domaine génériques de premier niveau a été ouverte à des candidatures en caractères non latins, comme les idéogrammes chinois ou les caractères arabes. En outre, l'ICANN s'est fixé comme objectif de traduire l'ensemble du site ICANN.org dans les six langues des Nations unies – y compris le français – pendant l'année en cours. Néanmoins, l'enracinement de l'ICANN reste américain : sa déclaration d'engagement envers les États-Unis prévoit explicitement que l'ICANN s'engage à avoir son siège aux États-Unis. Et, comme l'a fait observer M. David Martinon à votre mission, les membres du *board* qui ne sont pas Américains ont tous eu une expérience académique ou professionnelle anglo-saxonne, qui amoindrit la diversité culturelle effective de ce conseil d'administration.

D'autre part, **l'ICANN est dotée de pouvoirs accrus, sans que la responsabilité qui devrait les accompagner soit bien établie** : elle assume les fonctions IANA dont la supervision doit être mondialisée selon des modalités qui restent à inventer ; et de surcroît, elle s'est trouvée désignée par le gouvernement américain comme maître d'œuvre de la transition annoncée, ce qui rend plus aiguë la question de sa redevabilité (*accountability*) globale dans l'écosystème de gouvernance de l'Internet.

L'exigence posée par les États-Unis de voir la discussion menée par l'ICANN, alors même qu'elle en est un sujet central, **sera assurément défiée** par d'autres organisations ou par des gouvernements. Pour reprendre les termes de la contribution du Gouvernement français au NETmundial, « *l'ICANN incarne à la fois le succès et les lacunes du modèle multi-parties prenantes de gouvernance d'Internet* ».

En choisissant de confier à l'ICANN l'organisation de la transition, **les États-Unis consacrent une forme de « monopole privé » de l'ICANN sur le DNS et la coordination des serveurs racine**, qui constituent des ressources critiques essentielles au bon fonctionnement de l'Internet. M. Louis Pouzin a notamment fait observer à votre mission que l'ICANN avait la possibilité de taxer librement les détenteurs de noms de domaine Internet de premier niveau – chacun devant s'acquitter d'une redevance annuelle –, alors même que leur nombre va connaître un accroissement considérable à la faveur de l'ouverture de la deuxième génération de noms de domaine de premier niveau génériques (gTLD). Votre mission relève que **l'ICANN se nourrit ainsi d'un marché en extension**, celui des noms de domaine génériques, quand, parallèlement, de nombreux États du monde cherchent par tout moyen à imposer les opérateurs de l'économie numérique qui déploient des stratégies d'optimisation fiscale particulièrement agressives à leurs dépens.

Certes, l'ICANN a pris des initiatives : une résolution du *board* datée du 17 février 2014 a créé six groupes de conseil du président de l'ICANN dédiés à améliorer l'*Affirmation of Commitments*, les processus de prise de décision et la structure institutionnelle de l'ICANN, sa structure légale, les

processus pour le système des serveurs racines, la transparence et l'obligation de rendre des comptes vis-à-vis de toutes les parties prenantes, ainsi que la gouvernance de l'Internet.

Mais cet élan prometteur s'est déjà s'essoufflé. À la réunion de l'ICANN de Singapour, en mars, il a été indiqué que ces groupes de travail n'existaient plus. À la suite de l'annonce de la NTIA, l'ICANN a préféré s'engager sur deux chantiers : le premier est un dialogue public sur le mécanisme à mettre en place pour remplacer le rôle de supervision du gouvernement des États-Unis ; le second dialogue concerne la capacité de l'ICANN à rendre des comptes « *devant la communauté ICANN mondiale* ».

Or, selon M. David Martinon, **la nouvelle de sa prochaine « désaméricanisation » donne à l'ICANN une plus grande envie de liberté** : ainsi, dans le dossier du « .vin » et « .wine », révélateur de la volonté réelle de l'ICANN de s'émanciper et d'être redevable, « *on voit les progrès en matière d'émancipation plus que de redevabilité* ».

Pour reprendre le qualificatif utilisé par M. Eli Noam, professeur à Columbia University, lors de son entretien à New York avec la délégation de votre mission, **l'ICANN apparaît « *de plus en plus impériale* »**. Quelle est sa légitimité ? Devant qui est-elle responsable ? Quels intérêts sert-elle ? Quelles voies de recours propose-t-elle ?

Ces questions valent assurément pour l'ICANN, mais doivent aussi être traitées **pour l'ensemble de l'écosystème en charge de la gouvernance de l'Internet**.

Autant de questions que votre mission souhaiterait voir appréhendées par l'Union européenne pour proposer une nouvelle gouvernance de l'Internet conforme à ses valeurs démocratiques et aux droits de l'homme.

CHAPITRE II : UNE OPPORTUNITÉ HISTORIQUE POUR GARANTIR UN AVENIR DE L'INTERNET CONFORME AUX VALEURS EUROPÉENNES

L'Union européenne doit faire entendre sa voix dans le débat en cours sur la future gouvernance de l'Internet. Mais il est certain que sa crédibilité sera d'autant plus forte qu'elle aura, en interne, repris son avenir numérique en mains pour conquérir un poids réel dans le cyberespace.

Il n'est assurément pas facile pour l'Union européenne d'intervenir dans une discussion que les États-Unis ont engagée mais qu'ils veulent voir menée par l'ICANN. Toutefois, le climat engendré par les révélations d'Edward Snowden lui offre une opportunité historique de se poser comme médiateur pour inventer une gouvernance de l'Internet fidèle à ses valeurs.

I. L'UNION EUROPÉENNE, MÉDIATEUR POUR UNE GOUVERNANCE GARANTISSANT UN INTERNET OUVERT ET RESPECTUEUX DES DROITS FONDAMENTAUX ET DES VALEURS DÉMOCRATIQUES

Entre le modèle *multistakeholder*, qui ne manque pas d'ambiguïtés, et le modèle intergouvernemental, qui rappelle légitimement le rôle spécifique des États, **l'Union européenne peut défendre une approche équilibrée et nuancée. Son propre processus de construction, fondé sur le principe de subsidiarité, la qualifie particulièrement pour jouer ce rôle**. Comme l'indique la Commission européenne dans sa dernière communication[1] sur la gouvernance de l'Internet, « *l'Union européenne occupe une position idéale pour jouer un rôle dans la bonne gouvernance de l'Internet, car elle continue à évoluer vers une société en réseau moderne, avec une décentralisation du pouvoir et des décisions* ».

À ce titre, votre mission estime que l'Union européenne devrait proposer une refonte ambitieuse de la gouvernance de l'Internet : d'une part, sanctuariser les principes de l'Internet qui en font un bien commun ; d'autre part, constituer les enceintes de gouvernance en un réseau devant rendre des comptes à la communauté mondiale quant au respect de ces principes.

[1] *COM(2014)72 du 12 février 2014.*

A. REFONDER LA GOUVERNANCE DE L'INTERNET AUTOUR D'UN TRAITÉ ASSURANT LE RESPECT DES DROITS FONDAMENTAUX ET DES VALEURS DÉMOCRATIQUES

La communauté de l'Internet fonctionne de manière informelle sur le mode du consensus. Elle est donc foncièrement hostile à encadrer la gouvernance de l'Internet par des textes contraignants, encore moins s'ils sont négociés entre États. Pourtant, les États ne sont-ils pas légitimes à vouloir prendre leurs responsabilités concernant l'avenir global de l'Internet, espace qu'ils partagent avec leurs citoyens et leurs entreprises ?

1. Reconnaître l'Internet comme un bien commun mondial et sa gouvernance comme un dialogue entre technique et politique

Il est certain que la vision de la gouvernance de l'Internet que l'Union européenne doit porter dépend de sa vision de l'Internet lui-même. L'enjeu de la gouvernance de l'Internet n'est pas le même si l'on considère l'Internet comme une infrastructure technique parmi d'autres, au même titre que les autoroutes – auxquelles l'expression « autoroutes de l'information » a pu les assimiler –, ou comme un nouvel espace commun porteur de libertés nouvelles.

a) L'Internet, un bien commun, ni privé, ni public

Si l'Internet se définit comme réseau de réseaux, il n'est pas simple de déterminer son statut juridique, ni sa nature, privée ou publique.

Les catégories traditionnelles du droit et de la théorie économique s'articulent autour de l'opposition entre privé et public. Pour la théorie économique, les biens privés sont exclusifs et privatifs et relèvent de la logique marchande ; les biens publics, qui répondent à deux critères (non exclusivité ou non excluabilité d'une part, non rivalité ou extensibilité d'autre part), bénéficient à tous et sont exploités par tous indépendamment du bénéfice individuel retiré, à l'instar de l'éclairage public. Le droit, pour sa part, distingue entre bien et service. Le bien peut faire l'objet d'un droit de propriété, qui porte sur la chose elle-même (*abusus*), sur la jouissance de cette chose (*usus*) ou encore sur l'appropriation des fruits de cette jouissance (*fructus*). À l'inverse, le service ne repose pas sur le transfert d'un droit de propriété. Le service qualifié de « public » est rendu dans l'intérêt général, si besoin grâce à des prérogatives exorbitantes du droit commun et dans le respect de principes généraux, tels la continuité, l'égalité et l'adaptabilité. Mais des services non publics peuvent aussi s'acquitter de missions d'intérêt général. Et il n'existe pas nécessairement de lien entre le caractère public d'un service et l'appropriation publique des biens sur lequel repose ce service.

Vox Internet, programme de recherche soutenu par l'Agence nationale de la recherche (ANR), a tenté en 2005 d'**appliquer ces notions à l'Internet[1].** Cette confrontation **aboutit à une impasse qui tient à la nature de l'Internet** : il repose sur des protocoles de communication universelle, TCP/IP, qui ne sont pas juridiquement des biens, mais des programmes développés sous licence libre, ce qui signifie que l'inventeur a renoncé à ses droits privatifs et permet à chaque licencié d'utiliser et d'améliorer sa création, s'il respecte certaines conditions. De même, les noms de domaine (DNS) ne peuvent faire l'objet d'un droit de propriété : le « .fr » n'est pas la propriété de l'État français, qui s'acquitte seulement d'une redevance pour son usage. Juridiquement, l'Internet ne peut donc être considéré comme un bien. Il ne saurait non plus constituer un service public, qui repose sur une souveraineté territorialement limitée.

À la rigueur pourrait-on faire référence à la notion inédite de « *service public international* », comme l'a fait devant votre mission Mme Pauline Türk. Il est vrai que les principes du service public ne sont pas étrangers à ce qu'est devenu l'Internet. Comme M. Nicolas Colin l'a souligné lors de son audition, « c*e qui me frappe, c'est la parenté entre les principes qui président aux grandes plateformes et les lois de Rolland, qui ont théorisé les grands principes du service public : continuité, mutabilité, égalité. Les grandes plateformes ont compris que le succès industriel passe par la continuité du service, que la mutabilité est la condition d'adaptation à l'évolution des techniques – les applications doivent ainsi s'adapter aux évolutions des systèmes d'exploitation. Elles mettent, enfin, tous les utilisateurs à égalité – tout le monde peut, par exemple, ouvrir un compte chez Apple et créer une application.* » M. Éric Scherer, directeur de la prospective à France Télévisions, vice-président du groupement des éditeurs de services en ligne (GESTE), a même déclaré à votre mission qu'à ses yeux, « *Internet est devenu un service public, dès lors qu'il est le média du XXIe siècle, et qu'en tant que tel il n'appartient à personne, parce qu'il est à tout le monde* ».

En termes économiques, l'Internet pourrait être assimilé à un bien public, mais impur au regard des deux critères déjà évoqués : en sont exclus ceux qui n'ont pas acquis le droit d'user d'un nom de domaine ou payé un abonnement ; la saturation des bandes passantes peut en outre rendre rivaux les utilisateurs de l'Internet…

Par ailleurs, l'Internet repose sur l'existence et l'usage de réseaux physiques, constitués pour l'essentiel de biens privés (éventuellement affectés à un service public), quoiqu'interconnectés grâce à l'utilisation (privative ou non) du domaine public.

---

[1] Cf. *l'annexe 4 : « Bien public, bien privé, bien commun : approche juridique, approche économique », du rapport du séminaire Vox Internet :* Gouvernance de l'Internet : l'état de fait et l'état de droit*, 2005 :*
http://www.csi.ensmp.fr/voxinternet/www.voxinternet.org/article2bf6.html?id_article=12&lang=fr

Comme le montre l'analyse de Vox Internet, l'**Internet** déstabilise les constructions juridiques et économiques traditionnelles et **transcende la dichotomie public/privé**. Le rapport de Vox Internet souligne toutefois que le web est une application qui repose sur un mode d'interaction informatique, dit client-serveur[1], ce qui fait reposer la ressource économique que constitue l'Internet sur une responsabilité partagée et une logique de création et d'exploitation mixte public/privé. Ainsi, **le caractère commun de la ressource, ce partage sans lequel l'Internet ne saurait fonctionner et la dimension qu'il a prise justifient de qualifier l'Internet de bien commun, notion plus politique que juridique ou économique mais déjà opérante** en matière de santé, d'environnement, de droits de l'homme... et d'autres sujets débordant du cadre national et ayant un impact sur le présent, mais aussi sur le futur.

Cette qualification de l'Internet comme bien commun fonde l'action des États pour assurer que cette ressource profite à tous et empêche d'adhérer à l'objectif, affiché par le gouvernement américain[2], d'une privatisation complète de sa gouvernance. Elle est d'ailleurs sous-jacente dans la déclaration du NETmundial, qui reconnaît l'Internet comme « *une ressource mondiale qui devrait être gérée dans l'intérêt public* ». **Peut-on se reposer sur le secteur privé pour assurer l'intérêt public ?** L'intervention de l'État est toutefois redoutée de la communauté de l'Internet car elle vise aussi à ce que l'usage qui est fait de ce bien commun ne porte pas atteinte à l'ordre établi, ce qui peut conduire à filtrer, voire censurer les flux circulant sur l'Internet.

C'est pourquoi la responsabilité de l'Internet doit être confiée à tous ses bénéficiaires : de même que certains éléments du patrimoine « commun » bénéficient d'un régime particulier, à la fois protecteur et contraignant, de même l'**Internet pourrait faire l'objet d'un régime qui organise une responsabilité partagée pour assurer que nul – État, entreprise ou individu – ne porte atteinte à son intégrité.**

Votre mission valide donc la démarche multi-parties prenantes qui implique aussi bien les États que le secteur privé, la communauté technique, la communauté académique, la société civile et les internautes. Comme indiqué dans la déclaration du NETmundial, il importe d'insister sur le rôle respectif de chacune des parties prenantes et de l'ajuster en fonction des sujets. Dans leur déclaration Montevideo d'octobre 2013, les enceintes de gouvernance de l'Internet appellent à mondialiser l'ICANN pour assurer la participation « *sur un pied d'égalité* » des diverses parties prenantes. Ce pied d'égalité, d'ailleurs très théorique, ne doit pas être nécessairement l'horizon absolu de la gouvernance de l'Internet. **Le débat sur cette gouvernance devrait précisément porter sur la nature du rôle de chacun et les *checks and***

[1] *L'architecture client-serveur s'appuie sur un poste central, le serveur, qui envoie des données aux machines clientes, en réponse à leurs requêtes.*
[2] Cf. *supra.*

***balances* dans l'*approche* multi-parties prenantes de l'Internet, et non pas se réduire à un positionnement manichéen pour ou contre le *modèle* multi-parties prenantes.**

Il est globalement admis par tous que les États ont une responsabilité particulière pour les questions d'ordre public : droits de l'homme, cybersécurité, cybercriminalité, fiscalité… Mais les tenants du *statu quo* voudraient les tenir écartés des aspects techniques de la gouvernance de l'Internet, comme si ces aspects ne contribuaient pas à son développement dans l'intérêt public.

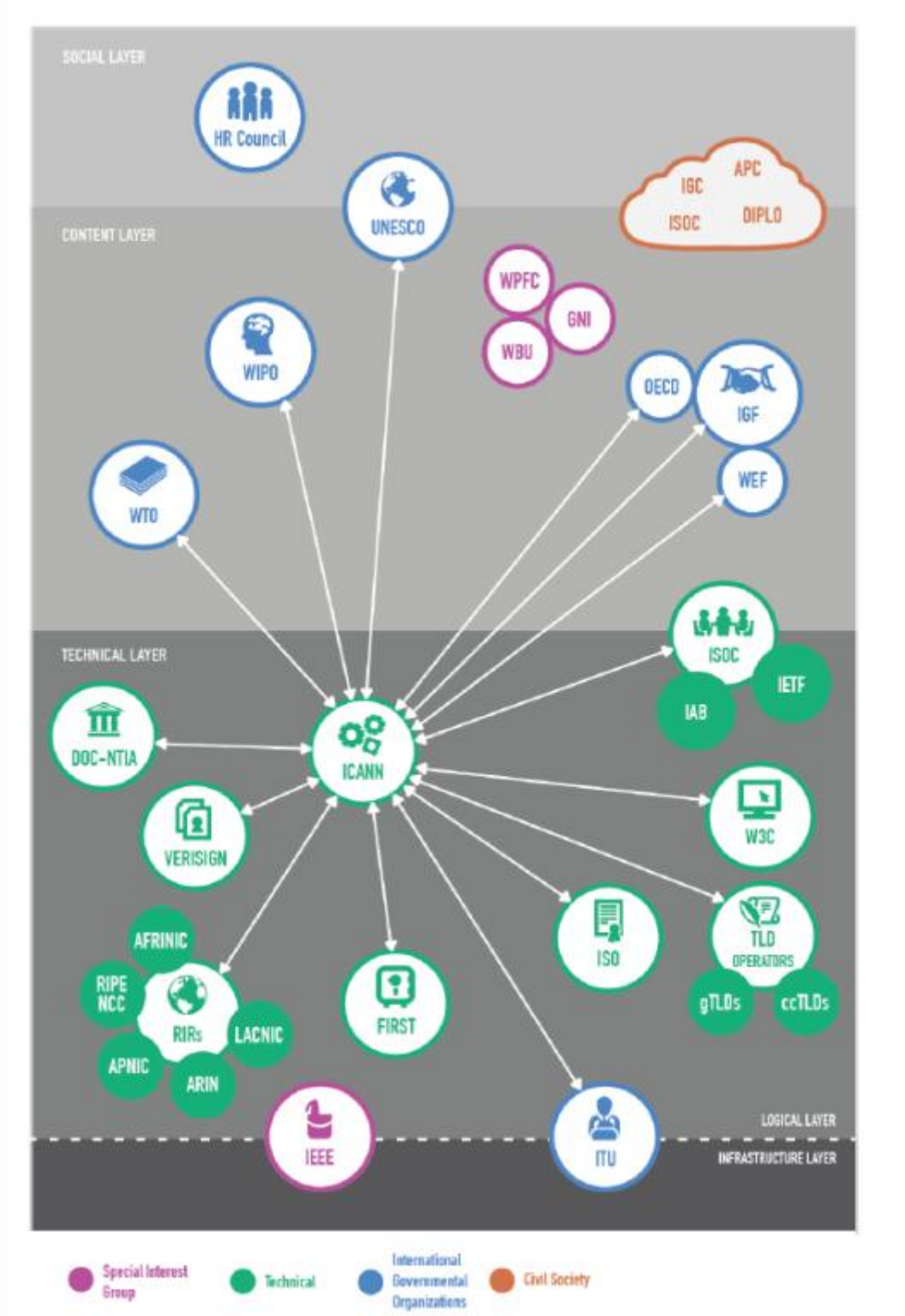
b) L'architecture technique de l'Internet est politique et concerne tous les acteurs

Votre mission reconnaît que **l'intervention étatique fait courir le risque de polluer les discussions d'ordre technique par des considérations politiques qui leur sont étrangères**, ce qui peut freiner les négociations, comme on le constate en matière climatique. **Le risque aussi** est **de ralentir les décisions** et d'empêcher leur adaptation aux évolutions techniques, particulièrement rapides sur l'Internet.

Sans méconnaître le bien-fondé de ces arguments qui appellent à la prudence, votre mission estime toutefois que confier la gouvernance technique à la seule communauté Internet repose sur une vision trompeuse de l'Internet.

L'essor de l'Internet, qui repose sur le respect de protocoles techniques communs, s'est fait sur des infrastructures télécoms existantes et a permis le développement d'applications nouvelles permettant la circulation de contenus. Cette structuration en couches est souvent invoquée pour justifier l'établissement d'une distinction entre la gouvernance de l'Internet et la gouvernance sur l'Internet. La première serait exclusivement d'ordre technique, quand la seconde viserait à réguler les flux de contenus accessibles en ligne.

Cette vision d'un Internet en couches est bien illustrée dans ce récent rapport publié en février 2014 par le panel de l'ICANN, dirigé par M. Vinton Cerf, sur le rôle de l'ICANN dans l'écosystème de gouvernance de l'Internet :


SOCIAL LAYER
HR Council
UNESCO
APC
IGC
ISOC
DIPLO
CONTENT LAYER
WPFC
GNI
WBU
WIPO
OECD
IGF
WEF
WTO
TECHNICAL LAYER
ISOC
IETF
IAB
DOC-NTIA
ICANN
VERISIGN
W3C
AFRINIC
RIPE NCC
RIRs
LACNIC
APNIC
ARIN
ISO
TLD OPERATORS
gTLDs
ccTLDs
FIRST
IEEE
ITU
LOGICAL LAYER
INFRASTRUCTURE LAYER
Special Interest Group
Technical
International Governmental Organizations
Civil Society

Groupes d'intérêt spécial	Organismes techniques	Organisations gouvernementales internationales	Société civile
IEEE : *Institute of Electrical and Electronics Engineers* WPFC: *World Press Freedom Committee* GNI : *Global Network Initiative* WBU : *World Broadcasting Union*	ICANN : Société pour l'attribution des noms de domaine et des numéros sur Internet DOC-NTIA : *National Telecommunications and Information Administration* (Département du commerce américain) VERISIGN RIRs : *Regional Internet Registries* (AFRINIC, RIPE, NCC, APNIC, ARIN, LACNIC) FIRST ISO : Organisation internationale de normalisation TLD operators : opérateurs de noms de domaine du premier niveau (gTLDs, ccTLDs) W3C : *World Wide Web Consortium* ISOC : *Internet Society* IAB : *Internet Architecture Board* IETF : *Internet Engineering Task Force*	HR Council : Conseil des Droits de l'homme de l'ONU WTO : *World Trade Organization* (OMC) WIPO : *World Intellectual property organization* (OMPI) UNESCO : *United nations educational, scientific and cultural organization* OCDE : Organisation de coopération et de développement économique IGF : *Internet Governance Forum* WEF : *World Economic Forum* ITU : *International Telecommunication Union* (UIT)	APC : *Association for progressive communications* IGC ISOC : *Internet Society* DIPLO

L'insistance avec laquelle les enceintes de gouvernance de l'Internet soulignent le caractère étroit de leur mandat et son champ exclusivement technique contribue à entretenir ce concept de **séparation entre technique et politique**, qui **résiste** pourtant **difficilement à l'examen**.

Une contestation précoce de cette séparation fallacieuse est provenue dès 2000 du Professeur **Lawrence Lessig**, de la *Harvard Law School* : **il a fait valoir que le code informatique représentait une nouvelle forme de loi**. Dans son célèbre article « *Code is Law* »[1], il écrivait : « *Nous sommes à l'âge du cyberespace. Il possède lui aussi son propre régulateur, qui lui aussi menace les libertés. Mais, qu'il s'agisse d'une autorisation qu'il nous concède ou d'une conquête qu'on lui arrache, nous sommes tellement obnubilés par l'idée que la liberté est*

[1] « *Code is Law - On Liberty in Cyberspace* », *Harvard Magazine, janvier 2000.*

intimement liée à celle de gouvernement que nous ne voyons pas la régulation qui s'opère dans ce nouvel espace, ni la menace qu'elle fait peser sur les libertés. ***Ce régulateur, c'est le code : le logiciel et le matériel qui font du cyberespace ce qu'il est****. Ce code, ou cette architecture, définit la manière dont nous vivons le cyberespace. Il détermine s'il est facile ou non de protéger sa vie privée, ou de censurer la parole. Il détermine si l'accès à l'information est global ou sectorisé. Il a un impact sur qui peut voir quoi, ou sur ce qui est surveillé. Lorsqu'on commence à comprendre la nature de ce code, on se rend compte que, d'une myriade de manières, le code du cyberespace régule. […] Si nous ne comprenons pas en quoi le cyberespace peut intégrer, ou supplanter, certaines valeurs de nos traditions constitutionnelles, nous perdrons le contrôle de ces valeurs. La loi du cyberespace – le code – les supplantera.* » De façon prémonitoire, M. Lawrence Lessig s'inquiète déjà du respect de la vie privée en ligne : « *S'il n'existe aucune incitation à protéger la vie privée – si la demande n'existe pas sur le marché, et que la loi est muette- alors le code ne le fera pas* ».

Les révélations sur le programme Bullrun en ont récemment apporté la démonstration : les agences de renseignement anglo-saxonnes ont pris le contrôle sur l'établissement de normes de chiffrement et collaboré avec des fournisseurs de solutions de chiffrement pour intégrer – dès leur conception - des portes dérobées, ainsi qu'avec des fournisseurs de services Internet pour récupérer des certificats de chiffrement. Le *Guardian* et le *New York Times* ont notamment indiqué que les agences avaient déployé beaucoup d'efforts sur les principaux protocoles ou technologies utilisés sur l'Internet (HTTPS/SSL, VPN) pour pouvoir intercepter et déchiffrer en temps réel des volumes considérables de données circulant en ligne. Ainsi, le droit à la vie privée est tributaire de considérations techniques : **les choix concernant le code sont des choix de valeurs et l'élaboration de normes techniques n'est pas étrangère au projet politique**. L'IETF en est elle-même convenue en prenant, pour la première fois, une position politique par la publication, en mai 2014, d'une norme ou plus précisément d'une *Request for consideration* (RFC) qui affirme que « *la surveillance tous azimuts est une attaque technique qui devrait être atténuée dans la conception des protocoles de l'IETF, quand c'est possible* » [1].

Il paraît donc difficile, après Snowden, de prendre pour acquise la vision du rôle des États qui ressort de l'Agenda de Tunis élaboré par le SMSI en 2005 et qui permettait « *aux gouvernements de s'acquitter, sur un pied d'égalité, de leurs rôles et responsabilités en ce qui concerne les questions de politiques publiques internationales concernant l'Internet, mais pas les questions techniques et opérationnelles courantes qui n'ont pas d'incidence sur les questions de politiques publiques internationales* ». Les conclusions du sommet de São Paulo marquent précisément une légère inflexion sur ce point : la feuille de route dessinée à cette occasion appelle à un meilleur dialogue entre les communautés techniques et non-techniques, pour « *améliorer la compréhension*

[1] *http://www.rfc-editor.org/rfc/rfc7258.txt*

mutuelle concernant les implications politiques des décisions techniques et les implications techniques de la prise de décision politique ».

Lors de son audition par votre mission, Mme Isabelle Falque-Pierrotin a illustré ces **interférences croissantes entre droit et technique**.

Elle a ainsi évoqué la décision du 8 avril 2014 de la Cour de justice de l'Union européenne, qui a invalidé la directive sur la conservation des données de connexion[1] en raison d'un défaut de proportionnalité dans l'atteinte au droit des personnes. La Cour estime que le législateur européen a failli en ne prévoyant pas la nécessité de localiser en Europe les serveurs qui traitent ces données. Cette position est effectivement intéressante en ce qu'elle dit que le respect des principes juridiques nécessite d'établir une règle technique allant dans le sens de la constitution d'un *cloud* souverain.

Inversement, il peut être nécessaire de traduire en normes techniques ce que dit le droit. Par exemple, la présidente de la CNIL a jugé fondamental de définir ce qu'est l'anonymisation des données car, à l'heure du *big data*, leur croisement permet la réidentification des internautes, même lorsqu'ils ont fait le choix de l'anonymat. Elle a indiqué que la CNIL avait procédé à cet exercice de réidentification sur un site de rencontres en ligne et s'était aperçue que cette opération prenait moins de dix minutes, malgré l'utilisation de pseudonymes. C'est pourquoi le G 29 a émis un avis appelant l'Europe à définir un standard d'anonymisation tant sur les principes (projet de règlement, conventions internationales) que sur leur traduction technique.

Cela signifie que **pour être respectée dans ses orientations, l'Europe doit être présente dans la gouvernance technique**.

M. Lawrence Lessig attire lui-même l'attention sur les **risques d'une privatisation absolue de la gouvernance de l'Internet** : « *Quand l'État se retire, la place ne reste pas vide. Les intérêts privés ont des objectifs qu'ils vont poursuivre. En appuyant sur le bouton antiétatique, on ne se téléporte pas au Paradis. Quand les intérêts gouvernementaux sont écartés, d'autres intérêts les remplacent. Les connaissons-nous? Sommes-nous sûrs qu'ils sont meilleurs ?* »[2].

2. Pérenniser par un traité les principes d'un Internet respectueux des droits fondamentaux et des valeurs démocratiques, tels qu'identifiés à la conférence NETmundial

Reconnaissant l'Internet comme bien commun, votre mission considère qu'il serait utile de sanctuariser ce qui fait le caractère précieux de

[1] *Directive 2006/24/CE du PE et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE.*
[2] Cf. infra *encadré sur l'invalidation de la directive* « data retention ».

l'Internet – son unité, son ouverture, son interopérabilité… – dans un texte fondateur à l'échelle mondiale afin de rendre ces principes opposables aux divers acteurs intervenant dans sa gouvernance. L'Union européenne devrait en être le fer de lance.

a) Des principes déjà identifiés comme fondateurs pour préserver la nature de l'Internet

Chaque État tente sur son territoire d'exercer sa souveraineté sur l'Internet. Les conflits de loi se multiplient et, parallèlement, les grandes plateformes de l'Internet étendent le nombre d'internautes soumis aux conditions générales d'utilisation – *terms of use* – qu'elles fixent pour leurs services.

Ces conditions d'utilisation sont en voie de devenir à bas bruit la constitution supranationale de l'Internet. Comme l'a souligné devant votre mission M. Boris Beaude, « ***le principal problème posé par Internet, c'est qu'il n'y a pas d'acteur politique à son échelle pour répondre aux questions politiques posées par les pratiques sur le réseau****, c'est que les États, dont la souveraineté est affaiblie par la mondialisation, ne sont pas à la bonne d'échelle d'action – et qu'il n'y a pas d'autre acteur politique pertinent à une échelle plus large que la leur* ».

Depuis plusieurs années, **diverses enceintes ont déjà éprouvé le besoin de proclamer des principes directeurs pour encadrer l'évolution de l'Internet**.

Ainsi, **l'Union européenne** a porté au SMSI un certain nombre de principes – l'ouverture et l'interopérabilité de l'Internet, la promotion d'une gouvernance multi-acteurs, la responsabilité des États dans la préservation de l'intérêt général, le rôle central du secteur privé dans la gestion quotidienne de l'Internet… –, que le SMSI n'a pas endossés mais que la Commission européenne a consignés dans les communications qu'elle a publiées, précédemment évoquées.

Parallèlement, **le Conseil de l'Europe**, qui réunit 47 pays, y compris la Russie – les États-Unis y ont un statut d'observateur – a également travaillé sur la gouvernance de l'Internet. Son Comité des ministres a ainsi identifié dix principes de gouvernance de l'Internet dans une déclaration du 21 septembre 2011[1].

Ayant étudié différentes problématiques juridiques, réglementaires et techniques, mais aussi l'éducation, la sécurité des infrastructures, les informations critiques ou la protection des données, **l'OCDE** a elle aussi développé une certaine expertise en matière d'Internet. M. Andrew Wyckoff, directeur de la science, de la technologie et de l'industrie à l'Organisation, a

[1] *http://www.coe.int/t/informationsociety/documents/CM%20Dec%20on%20Internet%20Governance%20Principles_fr.pdf*

ainsi évoqué devant votre mission les 14 « *Internet principles* »[1] élaborés à Paris, en 2011, à l'occasion d'une réunion de l'OCDE avec un certain nombre de pays non membres – Lituanie, Colombie, Costa Rica, ... 38 États y ont d'ores et déjà adhéré.

À l'occasion de sa réunion à Deauville en 2011, **le G8** a également identifié les grands principes de gouvernance de l'Internet[2].

À ces efforts pour identifier des principes généraux pour la gouvernance de l'Internet, s'ajoutent les initiatives prises par certaines organisations compétentes sur certaines matières interférant avec l'Internet : les droits de l'homme en ligne avec la Charte des droits de l'homme et des principes pour l'Internet[3] établie au sein du Forum de Gouvernance de l'Internet de l'ONU, la cybercriminalité avec la convention du Conseil de l'Europe, la protection des données avec la Convention 108 du Conseil de l'Europe…

L'UNESCO elle-même, sous l'égide de laquelle a été adoptée en 2005 la Convention sur la protection et la promotion de la diversité des expressions culturelles, a entrepris en novembre 2013 une étude sur l'Internet, conformément à la décision de sa conférence générale. Elle a identifié quatre thèmes : accès à l'information et à la connaissance, liberté d'expression, vie privée et dimension éthique de la société de l'information. Ses premières consultations l'ont déjà amenée à soutenir la nécessité pour l'Internet de respecter les droits de l'homme, d'être libre, accessible à tous et soutenu par la participation de nombreux intervenants. L'UNESCO entend ainsi contribuer elle aussi à l'élaboration de principes de gouvernance de l'Internet.

Mais toutes ces **tentatives** sont **partielles : soit en termes géographiques**, certaines étant régionales, d'autres visant un « club » d'États (G8), **soit en termes sectoriels** (comme dans le cas de l'UNESCO). Aucune n'a l'envergure universelle requise par l'Internet.

b) Des principes fondateurs qu'il est temps de consacrer

De nombreuses personnalités auditionnées par votre mission ont plaidé pour l'adoption de principes mondiaux pour encadrer l'évolution de l'Internet et ne pas figer le pouvoir de fait que les États-Unis détiennent sur le réseau pour des raisons historiques.

Ainsi, M. Jacques Toubon, ancien ministre, délégué de la France pour la fiscalité des biens et services culturels, a jugé devant votre mission « *que l'Union européenne devrait plaider […] pour que la gouvernance mondiale de l'Internet soit à tout le moins l'objet d'un certain nombre de principes écrits et*

[1] *http://www.oecd.org/sti/ieconomy/49258588.pdf*
[2] *http://www.diplomatie.gouv.fr/fr/IMG/pdf/Declaration_G8_Generale_20110527.pdf*
[3] *http://Internetrightsandprinciples.org/site/wp-content/uploads/2014/06/IRPC_booklet_3rded_English.pdf*

négociés, sans que ceux-ci demeurent l'apanage d'un certain nombre d'entreprises, ni de l'administration américaine qui travaille avec ces entreprises ! »

M. Bernard Benhamou, ancien délégué aux usages de l'Internet, a pareillement appelé « *à l'adoption de principes généraux qui empêcherait les États de faire comme s'il n'existait aucune forme d'opposabilité juridique, en particulier lorsque leurs actions peuvent avoir des conséquences sur l'ensemble de l'activité économique, sociale et politique désormais mise en œuvre* via *les réseaux. Il convient de substituer une logique de responsabilité internationale à l'actuelle logique du " pas vu, pas pris "…* ».

Mme Pauline Türk a fait valoir que les déclarations de principes et plans d'action issus des sommets mondiaux de la société de l'information avaient le mérite de la souplesse et de l'adaptabilité, dans un domaine mouvant et technique. Mais elle a aussi jugé « *qu'une formalisation plus contraignante de ces principes, qui aurait pour effet d'augmenter leur portée normative, permettrait de donner un socle commun aux débats relatifs aux questions politiques et diplomatiques essentielles qui sont désormais liées au développement d'Internet. Il s'agit à la fois de consacrer et de définir des principes aux interprétations parfois divergentes : la liberté d'information ou le droit à la vie privée, par exemple. Il s'agit aussi de concilier des principes potentiellement contradictoires : la diversité et l'unicité, la liberté d'expression et la sécurité publique, la solidarité et le respect de l'autonomie, le droit à la vie privée et la transparence …* »

Pour sa part, M. Bertrand de La Chapelle a déclaré à votre mission : « *nous avons aujourd'hui besoin d'un métasystème et de principes qui permettent l'interopérabilité de systèmes de gouvernance hétérogènes* ».

M. Boris Beaude a pointé du doigt l'opportunité du moment pour convenir de tels principes : « *nous sommes à un moment très propice à la décision, il faut agir sans tarder : l'Union européenne, les États-Unis et un grand nombre de pays, notamment africains, peuvent s'entendre sur des principes* ».

Seule Mme Norodom a fait part de ses réserves à l'égard d'un instrument juridique supranational : « *Peut-on établir une Constitution de l'Internet ? Quel pourrait en être, tout d'abord, l'instrument ? Il semble difficile de passer par une convention internationale contraignante. Peut-il exister un droit international spécifique au cyberespace ? Il est six principes que l'on voit fréquemment énoncés : liberté, protection de la vie privée, coopération interétatique, égalité d'accès aux technologies, pour éviter la fracture numérique, coopération civile et neutralité du net, enfin. Mais tous ces principes, hormis les deux derniers, n'étant pas spécifiques à l'Internet, il n'est pas sûr qu'ils puissent donner lieu à un* jus communicationis ».

La Commission européenne elle-même, dans sa récente communication de février 2014[1], ne préconise « *aucun nouvel instrument*

[1] *COM(2014)72.*

juridique international permettant de traiter les questions liées à la gouvernance de l'Internet ».

Il est vrai que l'on peut s'interroger sur la nécessité de formaliser un nouveau texte dédié à l'Internet alors qu'existent déjà des instruments puissants comme la Déclaration universelle des Droits de l'Homme, le Pacte international relatif aux droits civils et politiques, le Pacte international relatif aux droits économiques, sociaux et culturels, la Convention européenne des droits de l'Homme ou la Charte des droits fondamentaux de l'Union européenne...

Pourtant, et au regard notamment de l'affaire Snowden, il apparaît que l'**Internet, malgré sa dimension technique, est de nature à rendre impossible l'exercice des droits** protégés par ces divers instruments **ou, au contraire, peut contribuer à leur respect**. C'est pourquoi votre mission estimerait aujourd'hui utile de consacrer au plus haut de la hiérarchie des normes les spécificités de l'Internet qui en font le caractère précieux.

c) Donner force contraignante aux principes du NETmundial en les érigeant en traité international et en les faisant adopter par les internautes

L'agenda de Tunis, adopté à l'issue du sommet mondial sur la société de l'information en 2005, reconnaissait la nécessité de renforcer la coopération entre États concernant l'Internet et visait l'élaboration de principes communs : « *Faisant appel aux organisations internationales compétentes, une telle coopération devrait comprendre l'élaboration de principes applicables à l'échelle mondiale aux questions de politiques publiques ainsi que la coordination et la gestion des ressources fondamentales de l'Internet* ».

La récente conférence de São Paulo, pourtant hors du cadre onusien, **a permis la première élaboration d'un texte d'envergure mondiale, adopté par acclamation** : dans sa première partie, ce document identifie les principes fondamentaux de gouvernance de l'Internet sur lesquels un consensus de toutes les parties prenantes s'est dégagé à l'échelle mondiale.

Cette avancée historique doit être capitalisée : l'Union européenne devrait proposer de donner force contraignante à ces principes, élaborés d'une manière multi-parties prenantes et donc dotés d'une légitimité reconnue. Le tableau ci-après confirme cette légitimité en permettant de visualiser combien les principes proclamés au NEtmundial sont proches de ceux identifiés ces dernières années par la Commission européenne, le Conseil de l'Europe, l'OCDE, l'e-G8 de Deauville ou même dernièrement par le Brésil dans sa loi-cadre adoptée en avril 2014.

NETmundial (2014)	Commission européenne (2011 et 2014)	Conseil de l'Europe (2011)	OCDE (2011)	e-G 8 (2011)	Brésil (2014)
Respect en ligne des droits reconnus *off line*	x				
Droits de l'homme et valeurs partagées dont :	x	x	x	x	x
– Liberté d'expression			x	x	x
– Liberté d'association			x	x	
– Droit à la vie privée			x	x	x
– accessibilité					x
– liberté d'information et d'accès à l'information			x	x	x
– droit au développement				x	
Protection des intermédiaires	x		x		x
Diversité culturelle et linguistique	x	x	x		x
Internet comme espace unifié et non fragmenté	x	x	x		x
Sécurité, stabilité et résilience de l'Internet	x	x	x	x	x
Architecture ouverte et distribuée	x	x	x	x	x
Environnement permettant l'innovation durable et la créativité	x	x	x	x	x
Principes de gouvernance de l'Internet :	x	x	x		x
– multi-parties prenantes	x	x	x	x	x
– gouvernance ouverte, participative, conduite par le consensus		x	x		x
– transparente	x	x	x	x	x
– redevable	x	x	x		x
– inclusive et équitable	x		x		
– distribuée	x	x			
– collaborative			x		x
– permettant une participation significative		x		x	x
– promouvant de faibles barrières à l'accès	x	x			x
– agile			x	x	
– défendant des standards ouverts	x	x			x

Les principes du NETmundial représentent donc une synthèse acceptable des diverses tentatives déjà esquissées pour fonder la gouvernance mondiale de l'Internet sur des principes unanimement partagés.

Néanmoins, il faut reconnaître que le texte du NETmundial de São Paulo ne met pas explicitement l'accent sur la responsabilité des États dans la gouvernance de l'Internet, responsabilité qui figure parmi les dix principes identifiés par le Conseil de l'Europe[1]. Mais, aux yeux de votre mission, **la formulation assez flexible retenue dans la déclaration du NETmundial pour définir le caractère multi-partenarial de la gouvernance permet de ménager aux États un rôle adapté** dans les processus qui seront construits sur le fondement de ce texte.

Sans doute peut-on aussi regretter que **la neutralité du net ne figure pas expressément** parmi les principes du NETmundial mais, comme on l'a vu à l'occasion de la conférence, il serait très difficile de s'entendre sur la définition de ce principe : il divise aussi bien les acteurs privés – les fournisseurs de contenus et les opérateurs télécoms y étant généralement hostiles, pour des raisons différentes – que les États – les États-Unis n'envisageant la neutralité que sous l'angle des réseaux de télécommunications alors qu'elle trouve à s'appliquer plus largement aux terminaux, systèmes d'exploitation, plateformes…

En tout état de cause, votre mission estime que **la consécration du principe d'ouverture de l'Internet et de son architecture de bout en bout (*end-to-end)* représente déjà un acquis considérable susceptible de préserver l'innovation en ligne**. De surcroît, le texte du NETmundial réaffirme la nécessité de préserver l'Internet comme un « *environnement permettant l'innovation durable et la créativité* » et d'éviter toute barrière « *discriminatoire et non raisonnable à l'entrée de nouveaux utilisateurs* ».

Entre ouvrir, sur le sujet sensible de la neutralité du net, une négociation longue et difficile, à l'issue incertaine, et capitaliser sur l'accord – certes imparfait – dégagé entre parties prenantes à São Paulo pour construire sans attendre, sur cette base, un nouveau modèle de gouvernance, votre mission penche pour la seconde branche de l'alternative. Il lui apparaît **plus réaliste et efficace d'avancer ainsi plutôt que de défendre le lancement d'une nouvelle négociation**, dont il n'est pas évident de savoir

[1] Cf. *point 3.* « Responsabilités des États » *:* « Les États ont des droits et des responsabilités en matière de politiques publiques internationales relatives à l'Internet. Dans l'exercice de leur souveraineté, ils devraient, sous réserve de ce que permet le droit international, s'abstenir de toute action qui porterait directement ou indirectement atteinte à des personnes ou à des entités ne relevant pas de leur compétence territoriale. En outre, toute décision ou action nationale entraînant une restriction des droits fondamentaux devrait être conforme aux obligations internationales et, en particulier, être prévue par la loi, être nécessaire dans une société démocratique et respecter pleinement le principe de proportionnalité et le droit à un recours indépendant, assorti de garanties juridiques et procédurales adéquates. »

s'il vaut mieux l'initier avec les États-Unis voire le Brésil pour ensuite l'ouvrir aux autres États du monde, avec le risque de ne pas réussir à entraîner l'adhésion d'un nombre suffisant d'États, et donc d'entériner une nouvelle fragmentation du cyberespace, ou s'il vaut mieux la mener d'emblée au niveau mondial avec le risque de ne jamais aboutir.

Seule la consignation des principes du NETmundial dans un traité international serait de nature à les rendre opposables. Comme l'a fait valoir devant votre mission M. Maurice Ronai, « *un traité de cette nature conférerait un statut quasi constitutionnel aux principes architecturaux de l'Internet. Les gouvernements signataires pourraient ainsi faire valoir leur souveraineté, veiller au respect de leur législation sur leur territoire, à condition toutefois de ne pas porter atteinte à ces principes. Les gouvernements pourraient continuer à se livrer à l'espionnage, sans nuire à l'intégrité de l'Internet, la NSA devant alors s'interdire un certain nombre de pratiques.* »

Ériger ces principes en traité serait une manière éloquente pour les États de reconnaître le bien-fondé de l'approche multi-parties prenantes qui a conduit à leur adoption tout en prenant leurs propres responsabilités concernant l'avenir de l'Internet. L'Union européenne devrait prendre l'initiative de le proposer à ses partenaires, à commencer par les États-Unis. Lors de son déplacement à Washington, votre mission a toutefois été frappée par le manque d'allant de l'administration américaine envers cette perspective : M. l'ambassadeur Daniel Sepulveda, sous-secrétaire d'État adjoint en charge de ces questions, a rappelé à la délégation de votre mission les prérequis posés par la NTIA pour son retrait de la supervision de la zone racine du DNS, mais a paru réticent à élargir le débat aux principes généraux de la gouvernance de l'Internet et sceptique à la perspective de toute *Magna Carta*.

Le Brésil pourrait en revanche être un allié plus motivé pour soutenir cette initiative, et entraîner derrière lui plusieurs jeunes démocraties. Comme l'a analysé M. Julien Nocetti devant votre mission, le Brésil est « *l'incarnation même du* swing state*, un État qui n'hésite pas à critiquer ouvertement Washington sur ses doubles standards et exige l'internationalisation des ressources critiques de l'Internet, tout en réaffirmant son soutien à la gouvernance multi-acteurs* ». En adoptant une loi-cadre sur l'Internet – *Marco civil da Internet* –, ce pays manifeste son besoin de poser des principes de gouvernance ; il pourrait donc appuyer une démarche mondiale de même nature, afin de doter l'Internet d'une forme de constitution. L'Europe pourrait d'ailleurs adopter elle aussi un cadre législatif équivalent, calqué sur les principes dégagés à São Paulo.

Ceci impose au préalable que l'Union européenne parvienne à parler d'une seule voix, comme l'y a récemment exhortée Mme Neelie Kroes, commissaire européen en charge du numérique, à l'occasion du discours qu'elle a prononcé à Genève le 10 juin 2014 dans le cadre d'une

réunion consacrée au sommet mondial de la société de l'information : « *Trouvons une position claire et une voix claire dans ce débat global* »[1].

En complément, l'Union européenne pourrait initier une forme de ratification en ligne de ces principes, en proposant aux internautes d'y apporter leur soutien : émergerait ainsi, par le haut – les États – et par le bas – les internautes –, une consécration de principes dont la légitimité de l'élaboration est reconnue par tous. Des actions de sensibilisation devraient préalablement être organisées afin d'éviter que seules les personnes les plus impliquées ne soient à même de participer à cette consultation en ligne. L'**Internet offre en effet le moyen de mobiliser ses utilisateurs pour assurer sa pérennité comme espace de liberté**. L'Union l'a déjà bien compris et, depuis le traité de Lisbonne, offre à ses concitoyens la possibilité de se connecter en ligne pour lancer ensemble une initiative citoyenne européenne (ICE)[2] : un million de citoyens européens, en provenance d'un quart des États membres, peuvent ainsi inviter la Commission européenne à faire une proposition sur un sujet qui leur tient à cœur. On pourrait imaginer que soit lancée une forme d'initiative citoyenne mondiale invitant les États à s'accorder par un traité sur les principes du NETmundial afin d'assurer à l'Internet un avenir conforme aux valeurs démocratiques et respectueux des droits et libertés.

Mme Anke Domscheit-Berg, spécialiste E-Government au sein du Parti pirate, qu'une délégation de notre mission a rencontrée à Berlin, a évoqué l'exemple islandais : en 2011, une nouvelle Constitution y a été élaborée sur la base des propositions de 900 citoyens tirés au sort, ensuite retravaillées par un groupe de 25 experts désignés par la population.

Le besoin d'une telle *Magna Carta* avait d'ailleurs été reconnu en mars 2014 par M. Tim Berners-Lee, l'un des pères fondateurs du web, qui l'a répété lors de la conférence de São Paulo[3].

Proposition n° 1 : inviter les États membres de l'Union Européenne à s'entendre pour proposer la consécration des principes du NETmundial de São Paulo, à la fois par un traité international ouvert à tous les États et par une forme de ratification en ligne par les internautes.

B. CONSTRUIRE UN RÉSEAU MONDIALISÉ, LÉGITIME ET RESPONSABLE D'ENCEINTES DE GOUVERNANCE

Il ne s'agit pas simplement de proclamer des principes : il faut également veiller à ce que l'architecture technique de l'Internet et les

[1] *http://europa.eu/rapid/press-release_SPEECH-14-447_en.htm*
[2] *Voir règlement (UE) n° 211/2011 du Parlement européen et du Conseil du 16 février 2011 relatif à l'initiative citoyenne.*
[3] *http://www.huffingtonpost.com/tim-bernerslee/Internet-magna-carta_b_5274261.html*

enceintes de gouvernance dont le mandat est technique continuent de les garantir. À cette fin, **l'Union européenne doit proposer les moyens de mettre la gouvernance de l'Internet en conformité avec les principes du NETmundial**.

Pour reprendre les termes de M. Lawrence Lessig dans son article déjà cité : « *Tout comme la Constitution contrôle et limite l'action du Congrès, les valeurs constitutionnelles devraient contrôler et limiter l'action du marché. Nous devrions examiner l'architecture du cyberespace de la même manière que nous examinons le fonctionnement de nos institutions*. »

Votre mission estime que l'Union européenne doit clairement s'afficher comme force de proposition, dans un contexte où **plusieurs initiatives parallèles** ont déjà été prises pour tenter de concevoir une nouvelle architecture de gouvernance. On peut en relever deux qui impliquent de hauts dirigeants européens.

D'une part, en janvier 2014, deux grands *think tanks* occidentaux ont lancé à Davos un collectif chargé de déterminer en deux ans comment l'Internet doit être piloté et protégé. Cette **Commission mondiale sur la gouvernance de l'Internet**, lancée par le *Centre for International Governance Innovation* (CIGI) au Canada et l'institution britannique Chatham House, est **dirigée par Carl Bildt, ministre suédois des Affaires étrangères**. Mais l'alignement de la Suède sur la position américaine en la matière ne permet pas d'espérer une grande audace dans les conclusions que rendra cette commission dans dix-huit mois.

D'autre part, en novembre 2013, un **panel** a été constitué sur le fondement d'un partenariat **entre l'ICANN et le *World Economic Forum* (WEF)** pour étudier la coopération mondiale à propos de l'Internet et les mécanismes de gouvernance. **Présidé par le président de l'Estonie, M. Toomas Ilves, et vice-présidé par M. Vinton Cerf**, ce panel a rendu son rapport fin mai 2014[1]. Il plaide pour un écosystème de gouvernance de l'Internet collaboratif et décentralisé. Il est frappant de constater que ce rapport n'aborde en aucune manière la place que devraient tenir les gouvernements dans l'écosystème de gouvernance qu'il dessine : les gouvernements n'y sont cités qu'à chaque énumération des parties prenantes, au même titre donc que le secteur privé, la société civile et les communautés académique et technique. Le rapport convient néanmoins qu'il laisse certaines questions ouvertes, dont celle-ci : *« comment réconcilier le rôle des gouvernements nationaux pour protéger et respecter les droits de l'homme en ligne sans fragmenter l'Internet ? »* Autant dire qu'il esquive la question centrale qui se pose, à l'heure où l'avenir de la gouvernance de l'Internet est à inventer.

[1] Towards a collaborative, decentralized Internet governance ecosystem, *report by the panel on global Internet cooperation and governance mechanisms, mai 2014.*

1. Globaliser la gouvernance d'Internet sur le fondement des principes du NETmundial

L'Union européenne devrait s'appuyer sur les principes identifiés au NETmundial de São Paulo pour proposer une véritable globalisation de la gouvernance de l'Internet, qui s'articulerait autour d'un réseau d'enceintes ayant à rendre des comptes devant une assemblée mondiale, garante du respect desdits principes.

a) Formaliser l'existence d'un réseau d'enceintes pour une gouvernance distribuée et transparente

Mis à part certains membres du Congrès américain, chacun s'accorde aujourd'hui sur la nécessité de sortir l'Internet du giron des États-Unis qui a perdu sa légitimité.

Des mécanismes de gouvernance mondiale de l'Internet sont à inventer, dans le respect des principes du NETmundial : des processus multi-parties prenantes et démocratiques, permettant la participation « *de toutes les parties prenantes du monde entier* » – dont le rôle respectif dépendra des sujets –, fonctionnant par consensus « *dans la mesure du possible* » et sur un mode ouvert, distribué, agile, collaboratif, transparent et redevable.

La NTIA a par avance cadré la transition en refusant toute solution qui serait menée « *par les gouvernements ou par une organisation intergouvernementale* ».

L'option consistant à confier la gouvernance de l'Internet à l'Union internationale des télécommunications garde la faveur de nombreux États, notamment ceux en développement, particulièrement attachés à une institution de l'ONU qui donne à chaque État un poids équivalent et dont le secteur « développement » fournit une aide pour promouvoir l'accès aux télécommunications.

L'UIT leur apparaît en effet comme **le candidat « naturel » pour traiter de l'Internet** : institution spécialisée des Nations unies pour les technologies de l'information et de la communication (TIC), l'UIT attribue dans le monde entier des fréquences radioélectriques et des orbites de satellite, élabore les normes techniques qui assurent l'interconnexion harmonieuse des réseaux et des technologies et s'efforce d'améliorer l'accès des communautés défavorisées aux TIC.

Dès sa création, l'UIT a été fondée sur les partenariats public-privé. Elle compte aujourd'hui 193 pays membres et plus de 700 entités du secteur privé et établissements universitaires. Malgré cela, son fonctionnement reste largement intergouvernemental, chaque pays ayant une voix, et ne permet pas de satisfaire à l'exigence d'une gouvernance « multi-parties prenantes » pour l'Internet. De fait, la société civile ne juge pas l'UIT suffisamment légitime pour traiter certains sujets, comme celui des usages.

Dès lors qu'elle écartait l'option de l'UIT, votre mission a examiné l'opportunité de centraliser dans une autre institution la gouvernance de l'Internet. En effet, l'intervention de multiples enceintes dans cette gouvernance qui résulte de l'histoire de l'Internet, est source de complexité, et la tentation de simplifier le système en le centralisant est évidente. **Mais il est apparu à votre mission que les insuffisances du système actuel de gouvernance ne tenaient pas tant à l'éclatement des structures**, dont le fonctionnement conjoint a fait la preuve de son efficacité, **qu'à l'opacité de leurs interactions et à leur défaut de légitimité**.

Votre mission recommande donc d'**améliorer la transparence du système de gouvernance, tout en conservant son caractère distribué : ceci implique de formaliser les missions, engagements et interactions des différentes enceintes de gouvernance de l'Internet afin de les constituer en réseau**.

Elle propose ainsi d'élaborer des déclarations d'engagements, du type de l'*Affirmation of commitments* à laquelle l'ICANN est partie (celle-ci devant être revue et corrigée), pour les registres Internet, le W3C, l'IETF, l'IAB, les gestionnaires de serveurs racines, les opérateurs de noms de domaine de premier niveau ou l'UIT afin de préciser leurs rôles respectifs dans la gouvernance de l'Internet. **La distribution de responsabilités entre les institutions de cet écosystème dote la gouvernance d'une forme de résilience comparable à celle dont jouit l'Internet grâce à son architecture distribuée.**

En cela, votre mission rejoint les conclusions du rapport rendu en février 2014 par le panel stratégique mis en place par l'ICANN sous la présidence de M. Vinton Cerf, sur le rôle de l'ICANN dans l'écosystème de gouvernance de l'Internet[1]. Le panel y défend la vision d'un réseau de relations, certaines déjà formalisées, d'autres encore informelles, et insiste sur le caractère vivant et dynamique de cet écosystème afin de s'adapter à l'émergence de problèmes ou à leur solution. Il estime que « *ce réseau de relations formalisées va créer une structure flexible, élastique et défendable qui peut évoluer au fil du temps et qui n'a pas de point de contrôle central fragile. La structure permet la création et la sortie d'entités de l'écosystème et les modifications d'engagements de pair à pair sans nécessiter, pour répondre aux évolutions, un total accord de toutes les parties de l'écosystème à la fois.* »

Cette entreprise de formalisation ne devra pas laisser de côté l'opérateur en charge de la maintenance du fichier racine du DNS, aujourd'hui **VeriSign**. Votre mission ne comprendrait pas que la position particulière de VeriSign, qui édite, publie et distribue le fichier de la zone racine, reste en dehors des débats en cours, ce qui permettrait aux États-Unis de garder discrètement la main sur la racine du système des noms de domaine.

[1] *Strategy panel,* ICANN's role in the Internet Governance Ecosystem, *février 2014 – https://www.ICANN.org/en/system/files/files/report-23feb14-en.pdf*

Formaliser ouvertement les relations entre enceintes de gouvernance du net devra également conduire à **interroger l'attribution de la gestion de domaines, notamment ceux en « .com » et « .net » à VerisSign[1] ou ceux en « .org » à l'ISOC**. Il faudrait en effet questionner la légitimité de ces organismes à être bénéficiaires des ressources financières qu'apporte la gestion de ces extensions très répandues.

Si votre mission soutient l'établissement de telles déclarations d'engagement bilatérales, comme suggéré par le panel présidé par M. Vinton Cerf, elle ne se range pas à l'idée, défendue par ledit panel, de compléter cela par un faisceau de déclarations d'engagements entre l'ICANN et les gouvernements. À ses yeux, le réseau de gouvernance doit rendre des comptes à une enceinte globale et non pas à chaque gouvernement, ce qui n'est pas incompatible avec la faculté offerte à chaque gouvernement de faire appel d'une décision de l'ICANN.

Proposition 2 : asseoir la gouvernance de l'Internet sur un réseau de relations transparentes en formalisant les rôles et interactions entre l'ICANN, les registres Internet, le W3C, l'IETF, l'IAB, l'UIT, les gestionnaires de serveurs racine, les opérateurs de noms de domaine de premier niveau…

b) Transformer l'IGF en Conseil mondial de l'Internet, coordinateur légitime et mondial des enceintes de gouvernance

C'est pourquoi votre mission propose de miser sur l'*Internet Governance Forum* (IGF), enceinte aujourd'hui la plus légitime par son caractère onusien et en même temps multi-parties prenantes, pour l'ériger en un **Conseil mondial de l'Internet** (*Global Internet Council - GIC*), **chargé de veiller au respect des principes du NETmundial au nom de la communauté internationale**. Cette transformation pourrait se faire à l'occasion du traité déjà évoqué pour consacrer les principes du NETmundial.

L'IGF souffre aujourd'hui de sa difficulté à conclure ses débats. Ce lieu de dialogue **n'a pas su produire ce que le NETmundial a réussi à accomplir** : s'accorder sur des principes de gouvernance et sur une feuille de route. Comme l'a analysé Mme Axelle Lemaire devant votre mission, « *à court terme, l'incapacité du sommet sur la gouvernance mondiale à générer des décisions consensuelles et opérationnelles pose problème. D'autant qu'existe un problème de financement du secrétariat général, qui dépend d'États, mais aussi d'acteurs privés, de plus en plus réticents à mettre la main au portefeuille.* »

À moins de renoncer à lui confier tout rôle, chacun s'accorde sur la nécessité de renforcer l'IGF. La Commission européenne, dans sa récente communication sur la gouvernance de l'Internet, plaide précisément en ce sens.

[1] *Qui gère aussi les « .tv », « .cc », « .edu », « .jobs » et « .name ».*

Un groupe de travail chargé d'apporter des améliorations à l'IGF – auquel la France n'a pas participé, ce que déplore votre mission – avait adopté en mars 2012 un rapport suggérant de permettre à l'IGF de produire des résultats et d'accroître ses liens avec les autres entités impliquées dans la gouvernance de l'Internet[1].

Transformer l'IGF en Conseil mondial de l'Internet (GIC) reprendrait l'un des modèles d'organisation de la gouvernance de l'Internet qui avaient été soumis pour examen au SMSI en 2005. Le groupe de travail sur la gouvernance de l'Internet envisageait notamment la création d'un Conseil mondial de l'Internet composé de membres désignés par chaque État, mais assurant aussi la participation d'autres parties prenantes : « *Ce conseil reprendrait les fonctions relatives à la gouvernance de l'Internet sur le plan international qu'exerce actuellement le Département du commerce du gouvernement des États-Unis* »[2]. Il pourrait aussi être chargé d'approuver les règles et procédures applicables aux mécanismes de règlement des différends, voire faire fonction d'arbitre si nécessaire.

Pour échapper à son incapacité actuelle, **l'IGF/GIC aurait besoin d'être doté d'un secrétariat plus étoffé et structuré et d'un bureau** composé de représentants désignés par chaque collège de parties prenantes, afin de mieux préparer et cibler l'ordre du jour de ses réunions.

Mais il n'est pas possible d'envisager ce renforcement sans revoir les modalités actuelles du **financement** de l'IGF, qui reposent sur des contributions volontaires : pourrait notamment s'envisager **la délégation au GIC d'une extension de noms de domaine rémunératrice**, ou, à défaut, par le biais d'un subventionnement de l'ICANN. Mais cette seconde solution instaurerait un rapport de dépendance entre l'ICANN et le GIC qui serait préjudiciable à l'autorité dont serait investi le GIC. **Les enceintes de gouvernance devraient en effet conclure avec le GIC une déclaration d'engagements leur enjoignant de venir rendre compte régulièrement de leur action devant le GIC** : sans être une instance d'appel proprement dite, le GIC permettrait d'invoquer les principes du NETmundial pour contester publiquement telle ou telle décision d'une enceinte de gouvernance.

En effet, votre mission estime que « *l'auto-évaluation et l'examen par les pairs* », que recommande la Commission européenne dans sa communication déjà évoquée, ne sauraient suffire à assurer la responsabilisation des acteurs de l'espace Internet.

Même les normes techniques, dont la contestabilité juridique paraît délicate à organiser, **feraient ainsi l'objet d'un contrôle à l'aune des principes du NETmundial**. Dans sa communication de février 2014, la Commission européenne préconise précisément de mettre en place des mécanismes structurés pour permettre aux parties prenantes de participer

[1] *http://unctad.org/meetings/en/SessionalDocuments/a67d65_en.pdf*
[2] *http://www.wgig.org/docs/WGIGReport-French.pdf*

aux décisions techniques, de les examiner et de formuler des observations de manière régulière, afin de garantir la compatibilité des décision techniques avec les droits humains et avec l'ensemble des principes du NETmundial. Votre mission estime que ce contrôle fait défaut : M. Edward Snowden a révélé l'influence qu'avait pu avoir un État sur les standards techniques afin de rendre possible la surveillance.

Mais d'autres **conflits d'intérêts** ont également été portés à l'attention de votre mission : ainsi, le membre du W3C que la délégation de votre mission a rencontré à Boston, M. Le Hégaret, a reconnu que le modèle économique du *web* reposait largement sur le financement par la publicité et qu'à ce titre, les grands du net avaient un conflit d'intérêts direct quand il s'agissait de protéger la vie privée. De même, il a indiqué à la délégation que le mode de financement du W3C le rendait vulnérable aux intérêts privés : ainsi, en ce qui concerne l'interopérabilité des protocoles pour les télévisions numériques, le W3C n'a pas réussi à lever les fonds car Google avait un conflit d'intérêt par rapport à sa propre plateforme vidéo. Le W3C n'a en effet pas obtenu de recevoir les financements issus des extensions en « .web » comme il l'avait demandé. Ceci plaide à nouveau pour une mise à plat et une plus grande transparence dans les modes de financement des enceintes de gouvernance de l'Internet.

La **composition** de l'IGF/GIC devrait également être rendue plus **transparente pour assurer sa représentativité et sa légitimité**, d'autant plus que son poids dans l'écosystème de gouvernance de l'Internet serait augmenté. **Chaque partie prenante devrait déterminer les modalités de désignation de ses représentants au GIC, selon des règles publiques**, au lieu de laisser le dernier mot sur les nominations au Secrétaire général de l'ONU, naturellement plus soucieux d'équilibre géographique que de compétence en matière d'Internet.

Afin d'accroître la participation au GIC de toutes les parties prenantes, le rapport du groupe de travail de l'ONU de 2012 suggérait notamment d'impliquer des parlementaires dans ses travaux. Pour encourager la participation de ces derniers, la possibilité d'organiser pendant chaque GIC une session spécifique leur étant dédiée pourrait effectivement s'envisager.

En tant qu'institution onusienne, le GIC serait aussi bien placé pour contribuer à construire les capacités des pays en développement et favoriser ainsi leur participation à la gouvernance de l'Internet.

Les déclinaisons nationales et régionales du GIC offriraient l'occasion de lui faire remonter les préoccupations locales et nourriraient ainsi le contrôle qu'il effectue, selon un schéma fidèle au principe de subsidiarité dont l'Union européenne est familière.

Proposition n° 3 : transformer le Forum pour la Gouvernance de l'Internet en Conseil mondial de l'Internet, doté d'un financement propre et chargé de contrôler la conformité des décisions des enceintes de gouvernance aux principes dégagés au NETmundial.

Afin de soutenir cette transformation de l'IGF, votre mission suggère que l'Union européenne se propose pour accueillir en 2015 l'événement célébrant les dix ans du SMSI.

Proposition n° 4 : accueillir en Europe la célébration des dix ans du Sommet mondial pour la société de l'information en 2015 pour promouvoir cette nouvelle architecture mondialisée de la gouvernance de l'Internet.

2. Refonder l'ICANN pour restaurer la confiance dans le système des noms de domaine

La réforme de l'ICANN est aujourd'hui admise comme nécessaire par toutes les parties, même celles qui n'envisagent pas d'évolution globale de l'écosystème de gouvernance de l'Internet. En effet, les révélations sur la surveillance massive exercée par les autorités américaines sur l'Internet grâce à l'affaiblissement des standards de l'IETF, ont conduit à la remise en cause du pouvoir exorbitant détenu à l'ICANN par les États-Unis sur le système des noms de domaine, sans qu'un lien, sinon politique, soit clairement établi entre ces deux sujets. La fin annoncée de la supervision de la racine par les États-Unis oblige à penser une transition vers un système nouveau : la boîte de Pandore est ouverte.

Inévitablement, la dimension de cette réforme à venir de l'ICANN fait débat : **la réflexion sur de nouvelles modalités de supervision de la racine** – et donc sur le rôle dévolu aux États dans cette supervision – **a entraîné un débat collatéral sur la redevabilité de l'ICANN** et, plus globalement, sur **sa légitimité**, d'autant plus que cette entité a été désignée maître d'œuvre d'une réforme dont elle est l'objet.

a) Pour une WICANN assumant les fonctions IANA sous supervision mondiale

Sans doute **le système IANA/ICANN/NTIA** a-t-il fonctionné techniquement, mais il n'est pas tenable politiquement ni institutionnellement. Il **crée de la défiance** là où il devrait y avoir de la confiance. Il s'agit de conforter le fonctionnement technique satisfaisant du système de noms de domaine tout en s'assurant de sa résilience à long terme, ce qui implique d'envisager la survenue d'événements certes rares mais possibles : fraude interne, conflit de personnes au sein du management, tentative de prise de contrôle par des parties prenantes...

Votre mission considère que **le statut juridique de l'ICANN, société de droit californien, n'est pas en mesure d'inspirer une confiance pérenne** dans le système des noms de domaine et donc, par ricochet, dans tout le système Internet qui en découle. Dans l'*Affirmation of commitments* qui lie l'ICANN au Département du commerce américain, obligation est faite à celle-ci d'avoir son siège aux États-Unis. Cette disposition ne pourra plus figurer dans la nouvelle déclaration d'engagements.

Il pourrait être envisagé de transformer l'ICANN en organisation internationale : ceci exige un traité intergouvernemental, qui peut être rédigé avec la participation des parties prenantes. La gestion de l'air ou de la mer, ressources globales également, a de même été confiée à des organisations internationales, l'Organisation de l'aviation civile internationale (OACI) et l'Organisation maritime internationale (OMI). Ces agences spécialisées de l'ONU fonctionnent sur le mode « un État, une voix » mais rien n'interdit de conserver à l'ICANN, même de statut issu du droit international, une **gouvernance multipartite**.

Une autre solution pourrait être de refondre l'ICANN sur un fondement juridique hybride, s'inspirant du modèle du **Comité international de la Croix Rouge** : bien que relevant du droit privé suisse, le CICR se voit reconnaître une personnalité juridique internationale au même titre que les organisations intergouvernementales en vertu d'un statut souvent qualifié de *sui generis*. Même si son existence ne découle pas en soi d'un mandat conféré par des gouvernements, ses activités – fournir protection et assistance aux victimes de conflits armés – sont prescrites par la communauté internationale des États et fondées sur le droit international, en particulier sur les Conventions de Genève. Cette « option suisse » avait d'ailleurs été envisagée par le président de l'ICANN il y a quelques mois : lors de son audition par votre mission en février dernier, il avait indiqué avoir présenté au conseil d'administration de l'ICANN des initiatives ambitieuses, « *sur lesquelles il vient de me donner le feu vert. Premièrement, créer une structure légale internationale parallèle – peut-être en Suisse*. » Ce projet est resté lettre morte depuis, comme si l'annonce du gouvernement américain exonérait l'ICANN de se lancer dans des réformes structurelles.

Cette société mondiale pour l'attribution des noms de domaine et numéros sur l'Internet (*World* ICANN, soit WICANN) serait chargée des fonctions IANA qu'assume l'ICANN actuelle. Elle conserverait un fonctionnement multipartite et « *bottom up* » comparable à celui de l'ICANN aujourd'hui. Comme l'envisageait l'une des options étudiées par le groupe de travail de l'ONU sur la gouvernance de l'Internet en 2005, **le rôle des États y serait double** :

– une fonction de supervision des changements dans la racine, en substitution du Département du commerce du gouvernement des États-Unis. Ce rôle (pouvoir de veto ou d'approbation) serait attribué à un comité de contrôle dont les membres seraient désignés par le collège étatique du

Conseil mondial de l'Internet parmi les représentants des signataires du traité consacrant les principes du NETmundial, marquant ainsi la **nature critique pour les États de la cartographie de l'Internet que dessine le fichier racine du DNS**, ou à défaut désignés par le Conseil mondial de l'Internet dans son ensemble, à la condition qu'un droit de veto spécifique soit reconnu au territoire auquel se rapporte l'extension géographique concernée par le changement[1]. Selon votre mission, **associer les seuls pays signataires de ce traité à la supervision du fichier racine serait la condition qui permettrait aux États-Unis d'accepter une telle supervision mutualisée de l'ICANN**. Les gouvernements signataires pourraient ainsi faire valoir leur souveraineté, à condition toutefois de ne pas porter atteinte aux principes consacrés par le NETmundial ;

– une fonction consultative auprès du conseil d'administration de cette WICANN, comparable au rôle du GAC aujourd'hui. Ce rôle pourrait être tenu par deux représentants des États, afin de permettre l'expression de tendances. À l'étude, votre mission ne juge pas nécessaire de rendre décisionnaires les États au conseil d'administration, ce qui les exposerait à une forme de responsabilité au titre des décisions de l'ICANN ; en revanche, le maintien des États dans un rôle consultatif au *board* ne peut s'entendre qu'**à la condition que soit mis en place un vrai droit de recours**, transparent et indépendant, contre les décisions de l'ICANN, accessible notamment aux États.

Il importe en effet de mettre en place les exigences fixées à São Paolo en matière de redevabilité de cette WICANN : « *Independent checks and balances, as well as review and redress* ».

Proposition n° 5 : refonder l'ICANN pour en faire une WICANN (World ICANN) de droit international ou, de préférence, de droit suisse sur le modèle du Comité international de la Croix Rouge, et organiser une supervision internationale du fichier racine des noms de domaine en substitution de la supervision américaine.

b) Garantir la redevabilité de la WICANN et un réel droit de recours

Les mécanismes de redevabilité déjà mis en place au sein de l'ICANN portent surtout sur la revue globale des structures et des processus, et de manière insuffisante sur la revue des décisions individuelles. La légitimité des contrôleurs de cette redevabilité est également questionnée[2].

Votre mission estime que **la redevabilité de la WICANN doit s'organiser sur deux plans** :

[1] *La NTIA a reconnu en 2005 l'intérêt légitime des gouvernements dans la gestion de leur propre domaine de premier niveau géographique :* cf. *http://www.ntia.doc.gov/other-publication/2005/us-principles-Internets-domain-name-and-addressing-system*

[2] Cf. supra.

– une responsabilité globale de la WICANN au titre des fonctions critiques qu'elle exerce. Cette responsabilité passe par des processus d'évaluation indépendants – et non pas internes – du service rendu par la WICANN. Elle implique **que le *board* de la WICANN rende compte de sa politique devant une assemblée**, qui pourrait être soit une assemblée générale interne à la WICANN mais obéissant à des règles claires et légitimes pour la nomination de ses membres issus des diverses parties prenantes, soit, de préférence, le Conseil mondial de l'Internet conçu précisément pour être l'instance multi-parties prenantes de contrôle de l'ensemble de l'écosystème de gouvernance de l'Internet. Cette assemblée générale ou le GIC pourrait avoir pour attributions d'approuver les comptes, sur le rapport d'un auditeur externe tel un commissaire aux comptes, de modifier éventuellement les statuts de la WICANN, d'approuver les candidatures au *board* présentées par les parties prenantes, de donner leur avis sur les conditions de rémunération des dirigeants et membres du *board* et d'intervenir sur les conflits d'intérêts ;

– un mécanisme d'appel des décisions prises par la WICANN : les dispositifs prévus dans les statuts actuels de l'ICANN (*ombudsman, request for consideration* et *independant panel review*) présentent de graves insuffisances en termes d'impartialité ou d'accessibilité, notamment financière. Et l'ultime solution du recours devant le juge se fait devant les cours californiennes dont ressort l'ICANN, ce qui implique d'être présent sur place et d'avoir les moyens financiers pour cette procédure coûteuse. Il est donc essentiel de prévoir un mécanisme de recours indépendant et accessible, permettant la révision d'une décision, voire sa réparation. L'idéal serait qu'il soit judiciaire, si la juridiction dont ressort la WICANN n'est plus américaine mais suisse. À défaut, on peut envisager de confier au GIC (ou à son bureau) un rôle d'arbitre, dans la mesure où cet organe collégial multi-parties prenantes est moins exposé au risque de capture par des intérêts privés qu'un arbitre individuel, à condition que les représentants de l'industrie des noms de domaine soient tenus à l'écart dans l'exercice de ces fonctions arbitrales relatives aux noms de domaine.

Proposition n° 6 : rendre la WICANN responsable devant le Conseil mondial de l'Internet ou, à défaut, devant une assemblée générale interne et donner au Conseil ou à cette assemblée le pouvoir d'approuver les nominations au conseil d'administration de la WICANN et les comptes de cet organisme.

Proposition n° 7 : mettre en place un mécanisme de recours indépendant et accessible, permettant la révision d'une décision de la WICANN, voire sa réparation.

c) Éviter les conflits d'intérêts

Votre mission estime que le fonctionnement actuel de l'ICANN ne garantit pas que celle-ci échappe aux intérêts privés, alors qu'elle est chargée de gérer une ressource critique de l'Internet dans l'intérêt public.

Comment assurer que l'ICANN sert bien l'intérêt public, et non son propre intérêt ? Le gouvernement américain ne semble pas préoccupé par cette question, tant il est certain que les résultats d'un processus de coordination privé – parce que plus apte à répondre de façon souple aux besoins évolutifs de l'Internet – reflètent l'intérêt public.

Pourtant, l'évolution technique du DNS semble surtout bénéficier à l'industrie du nommage. Ainsi, l'ouverture de nouvelles extensions génériques profite surtout à l'ICANN. M. Louis Pouzin relevait que cette ouverture contribuerait à augmenter le nombre d'adresses IP, ce qui compliquait le routage et faisait la joie du plus grand constructeur de routeurs, l'américain Cisco !

Même si l'ICANN a procédé ces deux dernières années à un passage en revue de ses pratiques en matière d'éthique et de conflits d'intérêts, la main gardée par le *board* sur la mise en œuvre des recommandations ou sur l'appréciation des conflits d'intérêts n'a pas changé fondamentalement la donne.

D'une part, le *board* cumule deux fonctions : élaborer la politique des noms de domaine (décision d'ouverture de nouvelles extensions par exemple) et décider individuellement des délégations et redélégations des extensions, qu'elles soient génériques ou relatives à des codes pays. Ainsi l'élaboration des politiques et leur mise en œuvre sont entre les mêmes mains, ce qui peut conduire des membres du *board* à favoriser, à travers les politiques qu'il détermine, les intérêts d'acteurs, notamment privés, susceptibles d'en bénéficier et liés auxdits membres.

D'autre part, ces membres sont en partie désignés aujourd'hui par le comité de nomination selon des règles édictées par le *board* lui-même, et sont souvent issus de la communauté de l'ICANN ; ces procédés de cooptation nuisent à la représentativité et à la légitimité du *board*.

Votre mission propose donc, pour remédier à ces deux déficiences :

– d'établir une séparation fonctionnelle entre la WICANN et les fonctions opérationnelles IANA. Ces missions seraient assurées par une structure fonctionnellement séparée de l'ICANN, mais qui en serait le prestataire. Ainsi, l'élaboration des politiques de délégation/redélégation des extensions continuerait de se faire au sein de l'ICANN, par le ccNSO (pour les extensions géographiques) et le GNSO (pour les extensions génériques), avec validation par le *board*. Les décisions individuelles relatives aux délégations et redélégations de noms de domaine seraient, en application de la politique approuvée au *board*, prises par une instance *ad hoc*

(comité IANA), dont les membres ne seraient pas directement concernés par la délégation/redélégation ;

– de définir des critères d'indépendance pour la majorité des membres du *board*. Par exemple, la limitation du nombre de mandats successifs, l'interdiction de siéger au *board* pour deux parties prenantes successivement, la non-implication dans l'industrie des noms de domaine...

Proposition n° 8 : établir une séparation fonctionnelle entre la WICANN et les fonctions opérationnelles IANA pour distinguer ceux qui élaborent les politiques de ceux qui attribuent individuellement les noms de domaine.

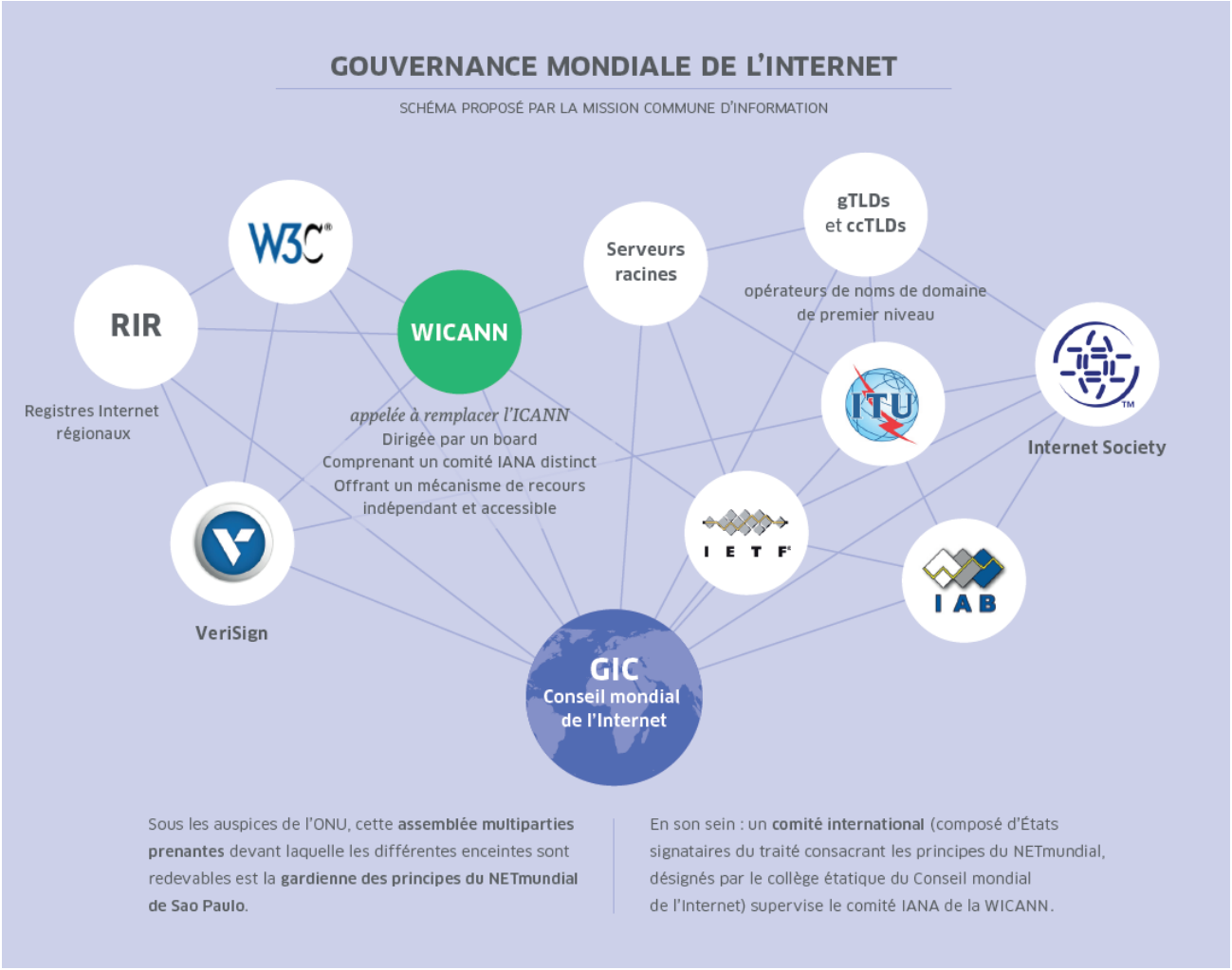
Proposition n° 9 : définir des critères d'indépendance pour l'essentiel des membres du *board* de la WICANN.

Dans le contexte actuel de suspicion à l'égard de la composition du *board*, la décision de la NTIA de confier à l'ICANN la transition vers un nouveau système de supervision de la fonction IANA ajoute encore à la confusion des rôles. **L'ICANN peut-elle valablement mener la conversation lancée par la NTIA et gérer la ressource critique des noms de domaine, objet-même de cette conversation ? Le conflit d'intérêts est ici patent**. À cet égard, l'AFNIC, qui reconnaît la nécessité de constituer un groupe directeur pouvant organiser et superviser le processus de transition, est très réservée sur les mécanismes proposés par l'ICANN pour constituer un tel groupe. L'ICANN entend en effet soumettre sa composition à son *board* ou à la présidente du GAC. Votre mission soutient, comme l'AFNIC, que les diverses composantes de l'ICANN doivent être en mesure de désigner directement leurs représentants au sein de ce groupe directeur pour ne désavantager aucune partie prenante et respecter le caractère transparent et démocratique du processus, conformément aux conclusions du NETmundial.

Pour assurer la crédibilité du débat et la pérennité du système à venir, **l'Union européenne doit exiger que**, conformément aux conclusions du NETmundial, **le groupe directeur envisagé par l'ICANN pour organiser la transition soit composé de membres désignés par les parties prenantes de l'ICANN** selon des modalités transparentes et démocratiques et inclue aussi des représentants des **autres parties prenantes non représentées aujourd'hui à l'ICANN** (gouvernements non présents aujourd'hui au sein du GAC et communauté académique).

Proposition n° 10 : exiger avant tout que le groupe directeur prévu par l'ICANN pour organiser la transition soit composé de membres désignés par les parties prenantes de l'ICANN selon des modalités transparentes et démocratiques et inclue également des représentants des autres parties prenantes non représentées aujourd'hui à l'ICANN.

Le schéma ci-dessous propose une présentation synthétique du système de gouvernance de l'Internet que recommande votre mission :


GOUVERNANCE MONDIALE DE L'INTERNET
SCHÉMA PROPOSÉ PAR LA MISSION COMMUNE D'INFORMATION
W3C
RIR
Registres Internet régionaux
WICANN
appelée à remplacer l'ICANN
Dirigée par un board
Comprenant un comité IANA distinct
Offrant un mécanisme de recours indépendant et accessible
Serveurs racines
gTLDs et ccTLDs
opérateurs de noms de domaine de premier niveau
ITU
Internet Society
VeriSign
IETF
IAB
GIC
Conseil mondial de l'Internet
Sous les auspices de l'ONU, cette **assemblée multiparties prenantes** devant laquelle les différentes enceintes sont redevables est la **gardienne des principes du NETmundial de Sao Paulo**.
En son sein : un **comité international** (composé d'États signataires du traité consacrant les principes du NETmundial, désignés par le collège étatique du Conseil mondial de l'Internet) supervise le comité IANA de la WICANN.

Au-delà du positionnement clair que votre mission voudrait voir adopté par l'Union européenne sur le sujet de la gouvernance *stricto sensu* de l'Internet, elle considère que la parole de l'Union européenne à l'échelon mondial sera d'autant plus crédible que l'Union européenne aura repris en main son propre avenir numérique.

II. L'UNION EUROPÉENNE DOIT REPRENDRE EN MAIN SON DESTIN NUMÉRIQUE POUR PESER DANS LA GOUVERNANCE DU NET

L'Union européenne doit se doter d'une ambition politique pour se positionner sur l'Internet. Cette ambition passe par une régulation économique des acteurs de l'Internet opérant sur le sol européen, par la finalisation d'un régime juridique exigeant mais réaliste de protection des données, par l'élaboration d'une vraie stratégie industrielle en matière numérique et par une appropriation citoyenne de l'Internet.

A. UNE RÉGULATION OFFENSIVE DE L'ÉCOSYSTÈME NUMÉRIQUE EUROPÉEN POUR UNE MEILLEURE RÉPARTITION DE LA VALEUR

La régulation des acteurs qui font partie de l'écosystème européen du numérique doit permettre d'améliorer la répartition de la valeur au bénéfice des acteurs européens, sans sacrifier le principe de neutralité du net.

La **neutralité du net** est présentée comme une des composantes essentielle du triptyque « liberté, universalité et neutralité » régissant le fonctionnement de l'Internet. Ce principe fait l'objet de nombreux rapports et « enflamme » la toile dès lors qu'il est remis en cause. Pourtant, que recouvre vraiment cette notion dont toutes les personnes auditionnées par votre mission sont convenues de dire qu'elle continue à faire débat car située au cœur de puissants intérêts souverains et industriels cherchant à l'orienter à leur profit ?

L'Union européenne, attachée à préserver l'ouverture de l'Internet, ne doit pas se laisser enfermer dans une vision piégeuse de la neutralité de l'Internet mais assortir l'exigence de neutralité d'une régulation offensive des plateformes de l'Internet, grâce aux leviers de la fiscalité et de la politique de concurrence.

1. Concrétiser l'ambition de neutralité du net…

a) La neutralité du net : entre vision idéaliste et application pratique

Le 3 avril dernier, le Parlement européen a adopté la définition suivante de la neutralité du net : « neutralité du réseau, le principe selon lequel l'ensemble du trafic Internet est traité de façon égale, sans discrimination, limitation ni interférence, indépendamment de l'expéditeur, du destinataire, du type, du contenu, de l'appareil, du service ou de l'application », dans le cadre de l'examen du projet de règlement européen relatif au marché unique des télécommunications, qui est à présent examiné par le Conseil de l'Union européenne[1].

[1] *Proposition de règlement du Parlement européen et du Conseil établissant des mesures relatives au marché unique européen des communications électroniques et visant à faire de l'Europe un continent connecté (COM(2013)627).*

Cette rédaction est conforme au principe posé originellement par M. Tim Wu, professeur de droit à l'université Columbia à New York, qui le définissait en 2003 de la manière suivante :

– la neutralité du net ou la neutralité du réseau est un principe qui garantit l'égalité de traitement de tous les flux de données sur l'Internet ;

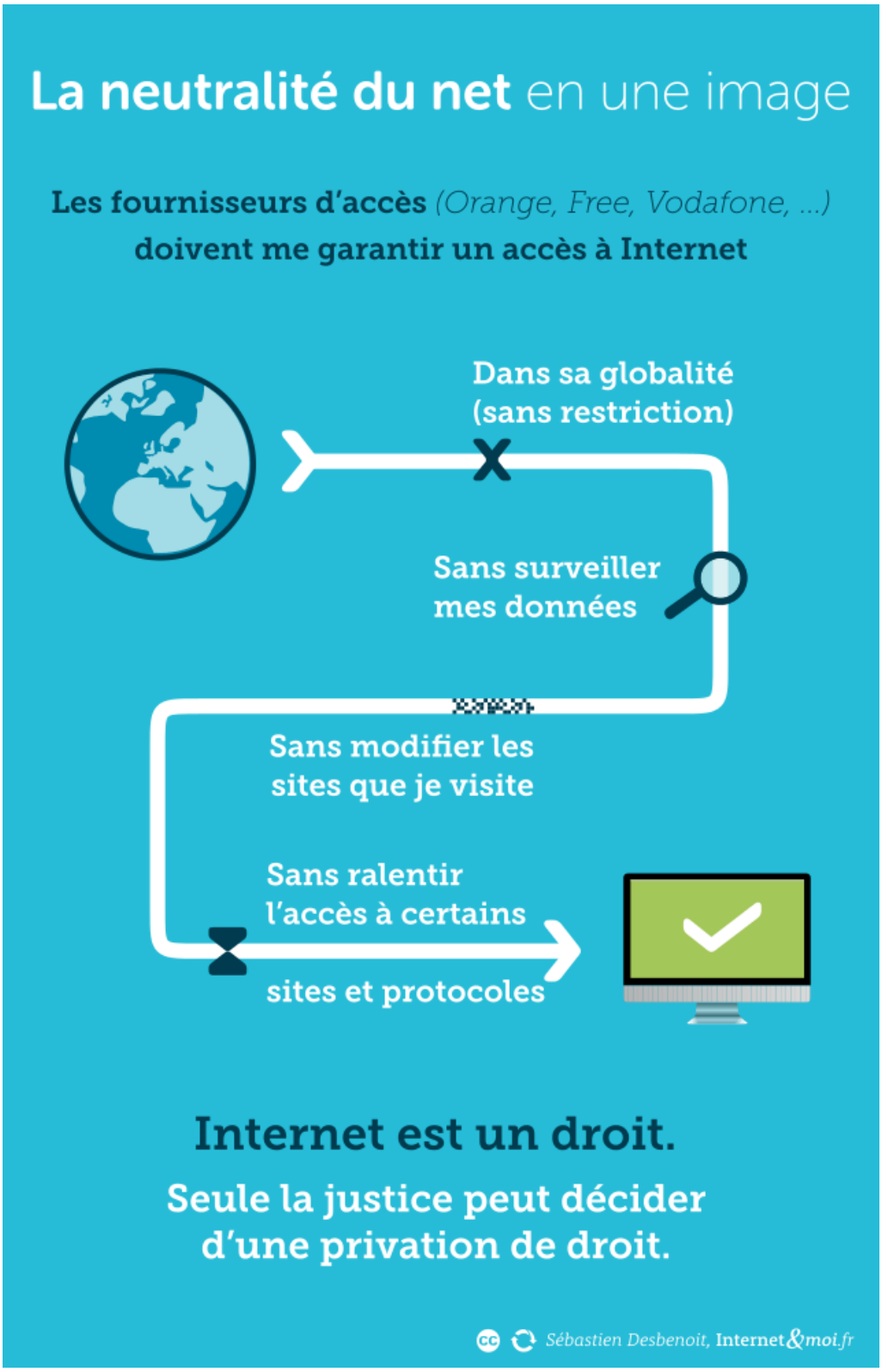
– le principe exclut ainsi toute discrimination à l'égard de la source, de la destination ou du contenu de l'information transmise sur le réseau[1].

Sous cet angle, il apparaît d'ailleurs préférable et plus conforme à la définition d'origine de parler de « neutralité du réseau » plutôt que de neutralité de l'Internet dans son ensemble. En effet, l'expression anglo-saxonne de *net neutrality* correspond à la contraction de la locution *network neutrality* utilisée dans l'étude des discriminations dans l'usage de la bande passante à haut débit.

Au départ purement technique, ce principe de fonctionnement du réseau s'est mué en droit subjectif pour les utilisateurs, ceux-ci considérant qu'il s'agit d'un droit de circulation et d'accès libre et non discriminé à tout type de contenus ou services. L'infographie présentée ci-dessous est représentative de ce que le concept de neutralité recouvre du point de vue de l'internaute.

[1] *Tim Wu, "Network Neutrality, Broadband Discrimination"*, Journal of Telecommunications and High Technology Law, *vol. 2, p. 141, 2003 - http://papers.ssrn.com/sol3/papers.cfm?abstract_id=388863*

Illustration du concept de neutralité du net du point de vue de l'internaute



Source : site www.Internetetmoi.fr par Sébastien Desbenoit

La neutralité de l'Internet est désormais érigée au rang de droit fondamental dont se prévalent les utilisateurs du réseau. À l'appui de cette affirmation, M. Jérémie Zimmermann, porte-parole de l'association « La Quadrature du net », citait devant votre mission la décision du 10 juin 2009 relative à la loi HADOPI, dans laquelle le Conseil constitutionnel a estimé qu'« *aux termes de l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789 :* « La libre communication des pensées et des opinions est un des droits les plus précieux de l'homme : tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi » ; *qu'en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions, ce droit implique la liberté d'accéder à ces services* »[1].

Le principe de neutralité du réseau justifie les limitations que le législateur européen a prévues concernant la responsabilité des intermédiaires techniques.

Les régimes de responsabilité civile et pénale des acteurs de l'Internet

Le régime de responsabilité civile et pénale des acteurs de l'Internet repose en droit français essentiellement sur un ensemble de directives européennes ainsi que sur les dispositions de l'article 6 de la loi pour la confiance dans l'économie numérique de 2004[2].

Ces dispositions distinguent trois acteurs :

- les opérateurs et fournisseurs d'accès à Internet (FAI), qui permettent au public d'accéder à des services de communication en ligne ;

- les fournisseurs d'hébergement Internet ou hébergeurs, qui « *assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services* » ;

- les éditeurs de service, qui incluent les éditeurs de contenus, notamment les éditeurs de service de presse en ligne.

Les FAI et les hébergeurs étant considérés comme de simples prestataires techniques, ils sont soumis à un principe de responsabilité civile et pénale limitée. Le législateur a en effet estimé que ceux-ci n'ayant pas la main sur les contenus, ils ne pouvaient être tenus pour responsables à raison de ces derniers.

[1] *Conseil constitutionnel, décision n° 2009-580 DC du 10 juin 2009 sur la loi favorisant la diffusion et la protection de la création sur Internet.*

[2] *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.*

En revanche, leur responsabilité peut être engagée dès lors qu'ils agissent sur ces contenus ou en ont connaissance. Tel est le cas pour un FAI « *dans les cas où soit [il] est à l'origine de la demande de transmission litigieuse, soit [il] sélectionne le destinataire de la transmission, soit [il] sélectionne ou modifie les contenus faisant l'objet de la transmission* »[1] L'hébergeur ne peut, quant à lui, voir sa responsabilité engagée que si le destinataire du service agit sous son autorité ou son contrôle, s'il avait effectivement connaissance du caractère illicite des informations stockées ou de faits et circonstances faisant apparaître ce caractère ou, dès le moment où il en a eu connaissance, il n'a pas agi promptement pour retirer ces données ou en rendre l'accès impossible.

C'est pourquoi, **ni les FAI ni les hébergeurs ne sont soumis à « *une obligation générale de surveiller les informations qu'[ils] transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicite* »**. Ils doivent toutefois :

- procéder à une « *surveillance ciblée et temporaire* » à la demande de l'autorité judiciaire ;

- **« *mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance* » des contenus faisant l'apologie des crimes contre l'humanité, incitant à la haine raciale ou à la violence, portant atteinte à la dignité humaine, ou des contenus pédopornographiques** ;

- « ***informer promptement les autorités publiques compétentes de toutes activités illicites*** *[…] qui leur seraient signalées* » et « *rendre publics les moyens qu'[ils] consacrent à la lutte contre ces activités illicites* » ;

- **conserver les données techniques de nature à permettre l'identification des personnes** pour les besoins de la recherche, de la constatation et de la poursuite des infractions.

Les éditeurs de service, quant à eux, doivent désigner un directeur de publication, pénalement responsable en cas d'infraction de presse conformément à la loi de 1982 sur la communication audiovisuelle[2].

La détermination du régime de responsabilité dépend donc de la qualification juridique du prestataire, elle-même fonction de la nature du service fourni. Les nouveaux acteurs de l'Internet aux activités multiples tels Google échappant à ces catégories prédéfinies, le juge est conduit à qualifier et apprécier la responsabilité de ceux-ci au cas par cas selon l'activité qui se trouve au cœur du litige[3].

Remettre en cause la neutralité exposerait par conséquent les intermédiaires techniques à ne plus pouvoir bénéficier de ce régime aménagé de responsabilité.

Si ce principe n'est pas remis en cause frontalement, tous les acteurs du numérique semblant soutenir la neutralité du net dans leurs manifestations

[1] *Art. L. 32-3-3 du code des postes et communications électroniques.*

[2] *Loi n° 82-652 du 29 juillet 1982 sur la communication audiovisuelle.*

[3] Cf. *TGI de Paris, 3ème chambre, 13 mai 2009, L'Oréal et autres contre eBay France et autres :* « Il ressort de ces dispositions que les régimes de responsabilité "aménagés" ne sont attachés qu'aux activités précédemment définies. Il convient en conséquence de rechercher le statut de l'activité faisant grief, un intermédiaire technique dans la prestation de services qu'il offre pouvant avoir différentes activités dont les unes bénéficient du régime de responsabilité "aménagé" et dont les autres relèvent de la responsabilité de droit commun, étant précisé que le régime "aménagé" étant un régime d'exception au droit commun, son champ d'application doit être apprécié strictement. »

d'intentions, c'est dans son application concrète qu'apparaissent des limitations d'ordre technique, économique ou commercial, témoignant des divergences d'interprétation du concept.

À cet égard, il est intéressant de noter que si le débat demeure aussi foisonnant et passionné, c'est parce que ce « pseudo » droit n'est pour l'heure pas fixé dans le droit positif en terme de règle contraignante, ni au niveau national, ni au niveau européen, ni au niveau mondial. Il s'agit encore à ce stade très largement d'une règle implicite et tout l'enjeu demeure d'en saisir les intérêts stratégiques.

b) La neutralité du net : des principes et des points de vue différents à la croisée d'intérêts économiques puissants

En titrant que la neutralité du net est bonne pour Google mais pas pour les consommateurs – *« Net Neutrality: Good for Google, Not Consumers »* -, le *Wall Street Journal* pose la question du partage de la charge des réseaux par lesquels transitent les contenus. Il met ainsi clairement en exergue l'opposition frontale entre opérateurs de réseaux et fournisseurs de services dans le débat sur le partage des coûts d'infrastructures, lutte économique dont les internautes consommateurs sont les observateurs passifs même s'ils supportent finalement les coûts du réseau en dernier ressort[1].

Dans une approche de régulation technico-économique de l'acheminement du trafic sur l'Internet, l'ARCEP a remis un rapport au Parlement et au Gouvernement sur la neutralité de l'Internet[2] en septembre 2012 qui se concentrait sur les problématiques de financement des réseaux :

– le débat sur la « neutralité de l'Internet » pose la question de savoir quel contrôle les acteurs de l'Internet ont le droit d'exercer sur le trafic acheminé : les opérateurs doivent-ils s'en tenir strictement au respect du principe d'égalité de traitement, tel qu'imaginé par les concepteurs de l'Internet ou peuvent-ils bloquer des services, ralentir certaines applications, prioriser certaines catégories de contenus ?

– la neutralité du réseau est-elle compatible avec la croissance soutenue du trafic, notamment mobile, et avec la nécessité de financer les investissements qui en résultent ?

L'ARCEP s'en tient à une définition technique de la neutralité de l'Internet selon laquelle les réseaux de communications électroniques doivent

[1] « Mobile bandwidth demand has grown more than 100% each year on average since the iPhone was introduced in 2007. Demand for wired broadband—DSL, Ethernet and FiOS—grows 30%-40% a year. The majority of bandwidth is now consumed by video over the Internet. YouTube (an application run by Google) and Netflix account for roughly 50% of peak Internet traffic, meaning the carriers' networks are twice as large as they would be without these two sites. The most vocal supporters of net neutrality are the biggest benefactors of the free bandwidth that comes with it. That's because they want consumers to foot the bill » *(*Wall Street Journal*, 1er mai 2014).*

[2] *Source : http://www.arcep.fr/uploads/tx_gspublication/rapport-parlement-net-neutralite-sept2012.pdf*

transporter tous les flux d'information de manière neutre, c'est-à-dire indépendamment de leur nature, de leur contenu, de leur expéditeur ou de leur destinataire. La traduction concrète de ce principe trouve son application sur le plan technique dans le procédé dit du *best effort*. Cela signifie que les données sont acheminées par les opérateurs « le mieux possible », en mobilisant les ressources disponibles (obligation de moyens) mais sans garantie de qualité, ou obligation de résultat. En contrepartie, l'utilisateur doit être certain que l'information qu'il envoie sera prise en charge par le réseau aussi bien que celle d'un autre utilisateur : « *pas mieux certes, mais pas moins bien* ».

Mais les termes du débat ont évolué à mesure de l'augmentation de la gamme des services offerts (messagerie, images, vidéo) et du flux ainsi généré. À l'origine technique, le débat s'est déplacé sur le terrain économique. L'ARCEP en décrit bien les tenants et aboutissants : « *la croissance rapide du trafic de l'Internet et les constantes évolutions des usages et des services à forte valeur ajoutée suscitent de vifs débats sur l'équilibre de cet écosystème* » :

– d'une part, les opérateurs soulignent la pression que fait peser la croissance soutenue des trafics sur le dimensionnement des réseaux ;

– d'autre part, les utilisateurs (internautes comme fournisseurs de contenus et d'applications) rappellent tous les bénéfices tirés d'un modèle neutre, notamment le foisonnement d'innovations et d'usages qu'il a entraîné, et attirent l'attention sur le fait qu'une atteinte aux principes de fonctionnement de l'Internet pourrait remettre en cause son développement.

Trois types d'enjeux sont soulevés :

– l'investissement et l'augmentation des capacités ;

– la gestion de trafic et la gestion de la rareté de la bande passante (*via* une différenciation des flux transitant sur les réseaux, par exemple en priorisant certains services ou en en ralentissant d'autres), opérées par les opérateurs ;

– la qualité de service dont bénéficie l'utilisateur final.

Pour autant, à la lumière des auditions, il apparaît que les intérêts de chaque partie sont croisés :

– du point de vue de l'utilisateur, internautes et petites entreprises, la revendication de neutralité vise à maintenir un accès libre et indiscriminé à tous les contenus et applications, sous-entendu au meilleur prix ;

– du point de vue des opérateurs, il s'agit de fournir une bande passante à leurs clients et utilisateurs en maîtrisant le coût des infrastructures et en le redistribuant sur les abonnements mais aussi sur les accords d'interconnexion ; s'affranchir de l'impératif de neutralité permettrait aux opérateurs d'accroître la participation financière des fournisseurs de contenus qui tirent un revenu publicitaire ou commercial de l'utilisation des réseaux. En cela, la position des opérateurs n'est pas forcément contradictoire avec celle de l'internaute, qui serait ainsi dispensé d'une part de la charge que représente le financement des réseaux ;

– du point de vue des fournisseurs de contenus et d'applications (FCA), il s'agit de préserver la capacité de distribution sans discrimination à tous ses utilisateurs ; néanmoins il serait faux de penser que cette position épouse totalement celle des internautes car pour ce fournisseur, l'internaute est un client source de revenu direct ou indirect par la publicité. Le fournisseur de contenus et d'applications a tout intérêt à minimiser son coût d'accès au réseau dont il tire des bénéfices commerciaux. Mais d'un autre côté, compte tenu de la rareté de la bande passante, il lui est également indispensable de s'assurer de la qualité de l'acheminement de ses données, au regard des nouveaux modèles économiques de création de valeur, notamment par la vidéo, forte consommatrice de débit. Pour cela, on a vu que certains FCA étaient prêts à payer l'opérateur pour bénéficier de la meilleure qualité de service. À leur manière, les fournisseurs de contenus et d'applications, du moins les plus puissants déjà installés et disposant d'une large assise financière, ont aussi leur intérêt à remettre en cause la neutralité des réseaux.

D'ailleurs, le fournisseur de vidéo à la demande Netflix, très gros consommateur de bande passante aux États-Unis – 34 % du trafic en Amérique du Nord durant les heures de pointe – vient d'accepter de payer aux opérateurs Comcast et Verizon une redevance pour bénéficier d'un débit maximal[1].

C'est la gestion de ces intérêts croisés qui nécessite la mise en place d'une régulation adaptée, qui fait l'objet de discussions au niveau européen mais aussi américain.

c) Un débat d'actualité relancé par la Federal Communications Commission (FCC) : quelle frontière entre discrimination, gestion du trafic légitime et accords d'acheminement prioritaire ?

Le texte adopté par le Parlement européen reflète l'idée selon laquelle la priorisation du trafic peut être justifiée pour certains flux, dans le respect du principe de non-discrimination.

Ainsi, l'article 23 du projet de règlement prévoit que « *les fournisseurs d'accès à l'Internet, les fournisseurs de communications électroniques au public et les fournisseurs de contenus, d'applications et de services sont libres de proposer des services spécialisés aux utilisateurs finaux. Ces services ne sont proposés que si la capacité du réseau est suffisante pour les fournir en plus des services d'accès à l'Internet et s'ils ne portent pas atteinte à la disponibilité ou à la qualité des services d'accès à l'Internet. Les fournisseurs proposant un accès à l'Internet aux utilisateurs finaux n'opèrent pas de discrimination entre des services ou des applications équivalents sur le plan fonctionnel*. » En d'autres termes, il convient que les accords passés entre les fournisseurs d'accès Internet et les fournisseurs de ces services spécialisés ne nuisent pas à la qualité de l'accès à d'autres contenus.

[1] *Source : http://www.lemonde.fr/economie/article/2014/05/17/aux-etats-unis-l-autorite-de-regulation-ouvre-la-voie-a-un-Internet-a-deux-vitesses_4420451_3234.html*

Il est donc envisagé de laisser une marge de liberté aux opérateurs en matière de « gestion de trafic raisonnable ». Pour le Parlement européen, un opérateur peut par exemple décider de donner temporairement priorité à un contenu ou un service très demandé, au détriment du reste du réseau. Le texte propose que cette gestion de trafic puisse être mise en œuvre dans quatre cas :

– dans le cas d'une loi, d'une décision de justice ou pour empêcher un « *crime sérieux* » ;

– pour « *préserver l'intégrité et la sécurité* » du réseau, d'un service Internet ou de l'appareil de l'internaute, contre les virus et les attaques ;

– pour empêcher de recevoir des informations non sollicitées comme le *spam* si l'internaute l'a explicitement permis ;

– pour limiter les effets d'une congestion temporaire du réseau, avec pour limite de devoir traiter de la même manière des contenus équivalents.

L'ARCEP recommande que les pratiques de gestion de trafic, mises en œuvre par exception à la règle générale de non-différenciation du traitement des flux sur l'accès à l'Internet, respectent cinq critères généraux : pertinence, proportionnalité, efficacité, transparence et non-discrimination des acteurs. L'enjeu sera donc d'en vérifier l'application eu égard aux tentations commerciales de souscrire des accords préférentiels à titre onéreux, ainsi qu'en laisse la possibilité le projet voté par le Parlement européen : « *Pour être en mesure de fournir des services spécialisés aux utilisateurs finaux, les fournisseurs de contenus, d'applications et de services et les [FAI] doivent être libres de conclure des accords pour transmettre les volumes de données ou le trafic concernés avec une qualité définie ou avec une capacité dédiée* ».

De l'autre côté de l'Atlantique, la *Federal Communications Commission* (FCC), l'autorité de régulation des communications américaine, a dû revoir les règles qu'elle avait adoptées en décembre 2010 pour garantir un Internet libre, ouvert, transparent et non discriminatoire. La base juridique de sa décision a en effet été annulée par les juges. La FCC a donc élaboré de nouveaux mécanismes qu'elle a publiés en mai 2014 et dont l'adoption définitive est prévue avant la fin de l'année. La FCC y adopte une position souple à l'égard du principe de neutralité, interprétée par certains comme un abandon pur et simple de ce principe. Or la FCC n'a pas validé le principe de facturation aux fournisseurs de service pour accéder à un traitement de faveur sur les réseaux[1]. Elle soulève en revanche la question de savoir si l'on peut interdire à un fournisseur d'accès de bloquer ou de ralentir le débit d'un site trop gourmand en termes de données transmises aux fournisseurs d'accès ou de réclamer une participation financière aux fournisseurs de contenus et d'applications pour bénéficier du meilleur débit possible.

Le débat reste vif et le président de la FCC, M. Tom Wheeler, réaffirme publiquement son attachement à un Internet ouvert, rapide et robuste : « *This*

[1] *Source : http://www.fcc.gov/document/protecting-and-promoting-open-Internet-nprm (site de la FCC)*

agency supports an Open Internet. There is ONE Internet. Not a fast Internet, not a slow Internet; ONE Internet ». Cet attachement a été confirmé à votre mission lors de l'entretien qu'a eu sa délégation avec la FCC à Washington. M. Howard Shelanski, conseiller à la Maison Blanche, a également indiqué à la délégation que le président Obama avait réaffirmé l'importance du principe de la neutralité du net.

De son côté, auditionnée par votre mission d'information, Mme Axelle Lemaire a clairement réaffirmé sa volonté de voir inscrire le principe de neutralité du net dans le droit français et européen et rejeté toute idée d'un Internet fractionné.

d) La neutralité doit également s'imposer aux plateformes de services ?

La neutralité du net comporte également d'autres enjeux qu'économiques :

– enjeux culturels, sociétaux voire éthiques avec la préservation des libertés fondamentales et de la diversité culturelle ;

– neutralité face au pouvoir légitime de blocage et de filtrage (sur décision juridictionnelle ou administrative) ;

– neutralité dans la fourniture de contenus ou d'applications par les fabricants de terminaux ou les plateformes de services.

Le Conseil national du numérique[1] (CNNum) s'est prononcé à l'unanimité en faveur d'une reconnaissance législative du principe de neutralité des réseaux, censé garantir l'accès universel aux contenus en ligne, par une modification de la loi de 1986 sur la liberté de communication.

Mais le CNNum propose également d'étendre aux services le concept de neutralité, considérant que l'Internet « *n'est plus seulement un réseau physique mais aussi et surtout un ensemble de services. Il est inutile d'imposer la neutralité en amont si on ne change pas les règles en aval.* » Le CNNum souhaite donc étendre cette neutralité aux services Internet tels que les moteurs de recherche, les réseaux sociaux et autres fournisseurs d'applications.

Imposer la neutralité aux moteurs de recherche permettrait d'éviter que Google, qui détient 95 % de ce marché en Europe, ne favorise ses propres services face à la concurrence. Votre mission convient qu'il est **paradoxal que, d'une part, Google se prévale du principe de la neutralité en matière de réseau, s'assurant ainsi que les services qu'il distribue sont acheminés sans entrave et, que d'autre part, il ne respecte pas ce même principe dans son cœur de métier : l'affichage des résultats de recherche entre ses propres services et ceux des autres acteurs du marché**.

Le rapport sur la neutralité des plateformes publié par le CNNum le 13 juin 2014 présente ces plateformes comme des goulets d'étranglement entre le consommateur et les entreprises qui souhaitent lui proposer des services et

[1] *Avis n°2013-1 Net Neutralité du 1er mars 2013.*

méritent, de ce fait, d'être régulées[1]. Or, aujourd'hui, la régulation ne pèse que sur les opérateurs FAI.

Aux yeux de votre mission, sauvegarder la neutralité implique donc de renforcer la régulation de fournisseur de contenus et d'applications. À cet égard, elle encourage la nouvelle Commission européenne à soumettre sans délai une proposition législative à cette fin. Cela requiert aussi une accélération des processus de traitement des plaintes en matière de concurrence, dans la mesure où l'écosystème de l'Internet évolue à grande vitesse : quelques années pour résoudre le cas Google peuvent être fatales pour les nombreuses entreprises qui subissent de la part de Google un abus de position dominante.

Proposition n° 11 : saisir la Commission européenne pour qu'elle soumette sans délai une proposition législative visant à réguler les fournisseurs de contenus et d'application, afin que la neutralité s'applique non seulement aux réseaux mais aussi aux services.

2. … l'assortir d'une régulation forte en matière de concurrence et de fiscalité

a) La régulation concurrentielle, une arme à mettre au service d'une conception étendue de la neutralité

La question de l'intégration verticale constitue un défi majeur au regard de la neutralité, en ce qu'elle réduit la liberté de choix des utilisateurs et diminue le caractère concurrentiel de l'offre de services. La politique de la concurrence représente à cet égard une arme puissante que l'Union européenne devrait mieux affûter pour l'adapter à la vitesse d'évolution des marchés numériques.

Le cas Google illustre la lenteur avec laquelle sont aujourd'hui traités les abus de position dominante sur l'Internet.

Il est reproché depuis 2010 à Google d'abuser de sa position dominante sur le marché européen de la réservation en ligne (90 %) pour promouvoir ses propres services dits « verticaux » tels que Google Shopping, Google Hotel Finder, Youtube, par des conditions d'affichage préférentielles dans ses pages de résultats, ses concurrents sectoriels n'apparaissant qu'en position inférieure dans les résultats de recherche. A notamment été mis en lumière le fait que les modifications pratiquées unilatéralement par Google sur son algorithme de recherche influaient négativement sur la visibilité de ses concurrents : ainsi, les mises à jour de l'algorithme *Panda* ont provoqué en 2013 une perte de 16 % de l'audience des comparateurs de prix indépendants.

[1] *Source : http://www.cnnumerique.fr/plateformes/ (rapport remis le 13 juin 2014 à M. Arnaud Montebourg, ministre de l'économie, du redressement productif et du numérique et à Mme Axelle Lemaire, secrétaire d'État chargée du numérique).*

Le commissaire européen à la concurrence, M. Joaquin Almunia, a retenu quatre griefs contre Google :

– la manipulation des résultats de recherche (défaut d'objectivité des algorithmes utilisés par Google) ;

– l'utilisation d'informations de sites tiers en tant que « données Google » (pratique proche du vol) ;

– des clauses de contrats abusives avec ses partenaires ;

– la restriction à la portabilité des campagnes de publicité de Google vers les autres sites.

La DG concurrence a opté pour la voie négociée, enjoignant à Google de faire des propositions d'engagement. En 2013, deux tests de marché ont été effectués sur la base des propositions de modifications faites par le moteur de recherche mais toutes deux se sont heurtées au refus des acteurs du secteur.

Quatre années après le lancement de la procédure, aucune mesure contraignante ou accord n'est intervenu, laissant ainsi libre cours au renforcement de la position dominante de Google. Auditionné le 28 janvier 2014 conjointement par la commission des finances et la commission des affaires européennes, M. Joaquin Almunia indiquait que « *la Commission européenne est pour sa part convaincue qu'il y a des abus. Pour tenter de résoudre le problème, deux voies s'offrent à nous. La première est d'adresser à l'entreprise une communication de griefs, qui ouvre une période de deux ans, pendant laquelle l'entreprise répond, et à l'issue de laquelle nous prononçons une décision, susceptible de recours devant la Cour de justice de l'Union européenne. Il faut attendre entre quatre et huit ans pour obtenir une sentence définitive. Cela n'a pas grand sens dans un secteur où l'innovation est si rapide. La seconde solution est d'ouvrir des négociations avec Google, c'est ce que nous avons choisi de faire. Dans quelques mois, ce travail de deux années aboutira à des engagements précis et juridiquement contraignants. Alors il faudra à nouveau choisir entre signer un accord avec cette entreprise - ce sera la troisième génération de compromis - ou lancer une communication de griefs.* »

En tout état de cause, quelle que soit la procédure employée, il s'agit d'un constat d'inadaptation des modalités de résolution des situations d'abus de position dominante. En effet, à l'ère de l'accélération des innovations technologiques, un délai si long n'est plus concevable quand on sait, par exemple, que Twitter, société *leader* dans le *microblogging*, n'a été créée qu'en 2006 et sa version française, fin 2009.

Outre la nécessité d'améliorations procédurales, votre mission plaide pour une plus grande audace de la Commission européenne en matière de régulation concurrentielle des fournisseurs de services en ligne, afin de défendre les petits acteurs du marché, dont font souvent partie les Européens. À ce titre, elle a relevé les propos tenus par M. Pierre-Jean Benghozi, membre du collège de l'ARCEP : « *Le seul moyen de contrer la montée en puissance des* over the top *est de mettre en place un principe de séparation, pour éviter une intégration verticale des*

acteurs contrôlant plusieurs strates de la chaîne de valeur que les protocoles IP avaient conduit à séparer, et assurer la neutralité, afin, par exemple, qu'une application développée sur certains terminaux ne soit pas discriminée sur d'autres, que l'on puisse accéder à l'Applestore à partir d'un terminal fonctionnant avec Androïd. »

Ces propos font écho à ceux tenus par MM. Nicolas Colin et Henri Verdier, dans leur livre commun *L'âge de la multitude* [1]: après avoir reconnu la nécessité de faire bénéficier les plateformes d'un régime de responsabilité aménagé, ils invitent à soumettre celles-ci à des sujétions pour empêcher tout abus de leur position dominante et donc préserver l'innovation. En cas de non-respect de ces engagements, ils estiment que ces plateformes devraient être exposées à des mesures ressortant des autorités de concurrence, comme la « désintégration » verticale entre l'application et la plateforme dont elle est issue, la « désintégration » horizontale par marché, l'obligation pour la plateforme de mettre ses ressources à la disposition du marché en contrepartie d'une redevance… Il s'agit ainsi de remettre « *à disposition du marché la valeur captée auprès de la multitude* ».

Proposition n° 12 : solliciter la Commission européenne pour améliorer les procédures de la politique de concurrence et les rendre plus réactives face aux abus de position dominante en ligne.

Proposition n° 13 : demander à la Commission de mettre en place un principe de séparation pour éviter l'intégration verticale des acteurs de l'Internet contrôlant de plus en plus de strates de la chaîne de valeur.

b) Une fiscalité rénovée pour faire contribuer les acteurs du numérique

Tout en veillant au principe de neutralité sur l'Internet, l'Union européenne ne doit pas s'abstenir de recourir à un moyen efficace de redistribution entre acteurs de l'écosystème numérique européen : la fiscalité.

Les pratiques d'optimisation fiscale des grands groupes de l'Internet ont été amplement documentées, notamment par les rapports successifs de M. Philippe Marini, président de la commission des finances du Sénat[2], et le rapport « Collin et Colin » précité.

Les deux problématiques principales d'érosion des assiettes fiscales portaient sur la taxe sur la valeur ajoutée (TVA) et l'impôt sur les sociétés. Sur ces deux volets, les grandes entreprises du numérique exploitent la concurrence fiscale à laquelle se livrent les États, y compris au sein de l'Union européenne, afin de minimiser leur charge fiscale.

[1] Cf. L'âge de la multitude, *Nicolas Colin et Henri Verdier, Ed. Armand Colin, 2013, p.222 sq.*
[2] *Rapports n° 398 (2009-2010) du 7 avril 2010 « L'impact du développement du commerce électronique sur les finances de l'État » et n° 614 (2011-2012) du 27 juin 2012 «* Une feuille de route pour une fiscalité numérique neutre et équitable ».

La distorsion de concurrence fiscale intracommunautaire relative à la **TVA applicable aux services électroniques** prendra fin au 1er janvier 2015. En effet, jusqu'à cette date, lorsqu'un opérateur établi dans l'Union européenne fournit ce type de services à un particulier établi dans l'Union ou à un assujetti dans le même État membre, le lieu de prestation continue d'être fiscalement celui où le prestataire est établi. C'est ce dernier point qui constitue la source d'optimisation fiscale des grands groupes établis dans des pays membres à basse fiscalité (notamment Amazon et iTunes au Luxembourg). À partir du 1er janvier 2015, de nouvelles règles seront applicables : la TVA due sur les services électroniques sera celle du pays du consommateur final. Entre 2015 et 2019, il subsistera un régime transitoire durant lequel une partie de la TVA continuera à être perçue par le pays du prestataire. Ce ne sera donc qu'à partir du 1er janvier 2019 que la TVA sera perçue dans son intégralité par le pays de résidence du consommateur final.

La fuite des recettes fiscales liées à **l'impôt sur les sociétés** ne peut, pour sa part, être résolue que par une modification des règles internationales en vigueur au sein de l'OCDE pour le rattachement des bénéfices des sociétés établies hors des frontières d'un pays à raison du chiffre d'affaires qu'elles y réalisent. Ce cas de figure est illustré par l'établissement du siège de Google en Irlande à partir duquel est faite la facturation des services de régie publicitaire pour les autres pays européens. La presse a révélé en 2012 que l'administration fiscale française aurait notifié à l'entreprise un redressement fiscal de près d'un milliard d'euros, fondé sur l'existence d'un « établissement stable » en France[1]. Pour mémoire, en 2011, Google France n'avait déclaré que 150 millions d'euros de chiffre d'affaires, pour un impôt sur les sociétés de 5,5 millions d'euros, alors que son chiffre d'affaires réel est estimé à près de 1,4 milliard d'euros.

Pour engager un processus de réforme de l'imposition des bénéfices, deux initiatives ont été prises, la première, dans le cadre de l'OCDE et, la seconde, à l'échelle européenne.

Les ministres des finances du Royaume-Uni, de l'Allemagne et de la France ont saisi en juin 2012 l'OCDE, laquelle a lancé le **projet BEPS** (*Base erosion and profit shifting*) destiné à préparer un plan d'action pour lutter contre l'érosion des bases d'imposition et les transferts de bénéfices vers les États à fiscalité basse ou nulle. Ce programme vise à lutter contre les stratégies fiscales agressives, les problématiques de distorsion entre masse taxable et profit dans les prix de transfert, la redéfinition de la notion d'établissement stable[2] et le traitement des régimes fiscaux « trop » favorables par le rétablissement de dispositifs anti-abus. L'objectif de ces travaux est la **remise d'un rapport en septembre 2014** recensant les principaux problèmes posés par l'économie numérique et les mesures permettant de les résoudre dans le cadre de l'élaboration d'un modèle de

[1] *Source : http://www.lemonde.fr/technologies/article/2012/10/30/le-fisc-francais-pourrait-reclamer-un-milliard-d-euros-a-google_1783397_651865.html*

[2] *L'établissement stable se définit par la présence de locaux et de personnels.*

convention multilatérale qui serait proposé au consensus des États parties prenantes avant la fin 2015.

Au niveau européen, M. Algirdas Semeta, commissaire à la fiscalité, a mis en place, le 22 octobre 2013, un **groupe d'experts dans le domaine de la taxation de l'économie numérique présidé par M. Vitor Gaspar**, ancien ministre des finances du Portugal, sur la question de la fiscalité du numérique, « *afin de réunir de l'expertise de haut niveau venant d'entreprises du secteur numérique, d'experts en fiscalité et de chercheurs, dans le but de préparer et de cadrer une voie sur ce sujet sensible* ». Le rapport final remis le 28 mai 2014 conclut que « *l'économie numérique ne nécessite pas un régime fiscal distinct* » mais qu'il peut « *s'avérer nécessaire d'adapter les règles actuelles pour tenir compte de la numérisation de notre économie* ». Il appelle à la suppression des entraves au marché intérieur, y compris les obstacles fiscaux, et la création d'un environnement plus favorable aux entreprises grâce à **une réglementation fiscale neutre, simplifiée et coordonnée**. Dans le domaine de la fiscalité des entreprises, le groupe d'experts recommande aux États membres d'adopter une position commune dans le cadre du projet BEPS pour en obtenir des « *retombées bénéfiques dans l'ensemble de l'Union européenne*[1] ».

La neutralité du net doit s'accompagner d'une régulation fiscale afin de rendre plus juste la répartition de la valeur entre tous les acteurs.

Proposition n° 14 : encourager les autres États membres victimes de l'optimisation fiscale des multinationales du numérique à exercer avec notre pays une pression continue sur les États membres complices de cette situation.

Proposition n° 15 : soutenir l'aboutissement des réformes fiscales en cours en matière de TVA et d'impôt sur les sociétés, pour mieux faire contribuer les fournisseurs de services en ligne aux charges publiques des États européens.

3. …et la compléter par de nouvelles modalités pour faire vivre la culture européenne sur l'Internet

Une meilleure répartition de la valeur entre les différents acteurs de l'écosystème de l'Internet implique aussi que l'Union européenne invente de nouveaux moyens pour financer la création culturelle et rémunérer les auteurs.

[1] Report of the Commission Expert Group on Taxation of the Digital Economy, *mai 2014, accessible à l'adresse suivante : http://ec.europa.eu/taxation_customs/resources/documents/taxation/gen_info/good_governance_matters/digital/report_digital_economy.pdf*

a) Un enjeu crucial de financement pour assurer une juste rémunération de la chaîne de création culturelle

L'Internet bouleverse en effet le monde de la culture et le plonge dans un univers beaucoup plus large que celui dont il est issu. Les librairies sont concurrencées par la distribution à distance et par le livre numérique[1], la presse écrite par l'information en ligne, la musique et le cinéma par les services de *streaming* et de téléchargement, l'audiovisuel par les services de vidéo à la demande… Peut-on encore imposer des obligations de diffusion d'œuvres françaises et européennes ou des obligations de financement de la production aux acteurs audiovisuels, concurrencés par l'offre culturelle en ligne d'éditeurs de services vidéo non établis en France donc non soumis à de telles obligations ? Peut-on maintenir une chronologie des médias quand l'accès aux œuvres cinématographiques est possible sur l'Internet ?

Votre rapporteure a adressé un questionnaire à la direction générale des médias et des industries culturelles (DGMIC) du ministère de la culture et de la communication. La réponse reçue fait état de « ***tensions économiques entre les opérateurs de communications électroniques et les fournisseurs de contenus et d'applications qui soulèvent la question du partage équitable de la valeur, indispensable pour rémunérer notamment les acteurs de la création, dont les contenus sont une des raisons majeures du développement de l'Internet*** ».

[1] *À ce sujet, le 26 juin 2014, le Sénat a définitivement adopté la proposition de loi, qui autorise, pour les livraisons à domicile, l'application d'une remise de 5 % du prix de vente sur les frais de livraison mais en interdit la gratuité, afin de défendre le secteur des librairies qui assure une animation culturelle indispensable, notamment en zone rurale.*

Le partage de la valeur et l'exploitation en ligne des œuvres culturelles

Le rapport LESCURE « Acte II de l'exception culturelle », remis au Président de la République et à la ministre de la culture et de la communication en mai 2013, a mis en exergue les déséquilibres du partage de la valeur liée à l'exploitation en ligne des œuvres culturelles, que ce soit entre titulaires de droits et éditeurs de services en ligne ou entre les créateurs et leurs éditeurs/producteurs.

1. *Dans le domaine du livre*, la question du partage de la valeur s'est posée assez tôt, notamment s'agissant de la rémunération des créateurs. En 2011, une mission sur le contrat d'édition numérique des livres a été confiée à M. Pierre SIRINELLI et a abouti à la signature d'un accord cadre en mars 2013 entre le Conseil permanent des écrivains (CPE) et le Syndicat national de l'édition (SNE). La solution retenue est celle d'une modification législative articulée avec un code des usages qui précisera les obligations réciproques des parties et notamment les conditions de rémunération, de reddition des comptes… Les taux de rémunération et les modes de gestion relèveront de la négociation des parties et d'un choix individuel.

Concernant le marché du livre numérique, la loi n° 2011-590 du 26 mai 2011 relative au prix du livre numérique a permis de réguler le marché : en donnant à l'éditeur, à l'instar de la loi Lang de 1982, le pouvoir de fixer, pour le livre numérique, un même prix de vente pour tous les revendeurs, qu'ils opèrent depuis la France ou depuis l'étranger, cette loi devrait permettre de créer pour les acteurs français les conditions d'une concurrence équitable.

Eu égard à la problématique de la territorialité de la loi inhérente aux services prestés en ligne et qui intéresse l'ensemble des secteurs, il est important de souligner que cette loi s'applique aux distributeurs établis à l'étranger et commercialisant des livres numériques sur le territoire français. Cette disposition, qui avait dans un premier temps fait l'objet d'un avis circonstancié de la Commission européenne, qui mettait en doute sa conformité avec le droit de l'Union européenne, n'a au final pas fait l'objet d'une procédure d'infraction par la Commission.

2. *Dans le domaine de la musique en ligne*, la question du partage de la valeur issue de l'exploitation des œuvres sur l'Internet est *de facto* un enjeu majeur dans la mesure où cette partie du marché est devenue de plus en plus importante au fil des années : en 2013, le chiffre d'affaires généré par les exploitations numériques s'élevait à 125,8 M€, soit 26 % du marché de la musique enregistrée.

La réflexion sur le partage de la valeur y a également été engagée relativement tôt puisque plusieurs rapports successifs (rapport « Création et Internet » de 2010 – mission ZELNIK-TOUBON-CERUTTI –, médiation HOOG, rapport LESCURE) ont identifié et qualifié le problème, et esquissé successivement des voies de solutions visant à rétablir un partage équilibré de la valeur.

Plus récemment, le rapport de M. Christian PHELINE, intitulé « Musique en ligne et partage de la valeur. État des lieux, voies de négociation et rôle de la loi » et remis le 18 décembre 2013 à la ministre de la culture et de la communication, a dressé un état des lieux précis et documenté des pratiques contractuelles, d'une part entre plateformes de musique en ligne et ayants droit et, d'autre part, entre producteurs phonographiques et artistes-interprètes, permettant d'envisager des pistes de meilleure répartition de la valeur issue de l'exploitation des œuvres musicales sur l'Internet.

Concernant la relation entre les producteurs phonographiques et les artistes interprètes, son analyse a consisté à extraire les données pertinentes fournies par les acteurs du

marché (producteurs phonographiques, artistes, avocats, sociétés de gestion collective…) afin d'établir un état des lieux objectif des pratiques contractuelles et des rémunérations relatives à chaque typologie de contrats (contrats d'artiste, contrats de licence et autoproduits). Ce rapport montre *in fine* que la rémunération des artistes-interprètes varie selon les catégories de producteurs et d'un marché à l'autre (ventes physiques ou ventes numériques).

Afin d'assurer une plus grande transparence et une plus juste rémunération des artistes-interprètes, notamment pour l'exploitation numérique de leurs œuvres, M. Pheline propose de mieux encadrer les pratiques contractuelles dans le but d'assurer une meilleure protection à la partie réputée la plus faible. Il encourage notamment les négociations au sein de la filière musicale pour définir un partage plus équilibré et transparent des revenus générés par la musique en ligne et préconise que, si ces négociations échouaient, des dispositions législatives soient inscrites dans le projet de loi sur la création artistique, notamment sur le principe d'une gestion collective obligatoire.

Par ailleurs, pour améliorer les relations entre les producteurs et les plateformes de musique en ligne, le rapport préconise qu'à défaut d'autorégulation par l'élaboration d'un code des usages soient insérés dans la loi les principes posés par la charte HOOG des « 13 engagements pour la musique en ligne ».

3. *Pour le cinéma et l'audiovisuel*, le débat sur le partage de la valeur entre les éditeurs de services et les producteurs de contenus semble relativement apaisé à ce stade dans le cadre des exploitations en vidéo à la demande. En revanche, la rémunération des auteurs soulève d'importantes difficultés depuis la dénonciation du protocole de 1999 puisque certains auteurs sont rémunérés dans le cadre d'une gestion individuelle, tandis que d'autres continuent de relever de la gestion collective de la Société des auteurs-compositeurs dramatiques (SACD). Par ailleurs, les comédiens ne reçoivent quasiment aucune rémunération au titre de l'exploitation en ligne. À ce sujet, le rapport LESCURE engage à la négociation interprofessionnelle en vue de la signature d'accords collectifs prévoyant des rémunérations minimales pour les auteurs et les comédiens.

4. *Dans le domaine de la photographie*, la circulation numérique des images quasi « libre » et « gratuite » soulève des interrogations quant à la valeur créée mais pose également des questions liées aux atteintes de droit de propriété intellectuelle. Concernant l'utilisation des photographies dans la presse, une mission de médiation entre agences, éditeurs et photographes de presse a été confiée par la ministre de la culture et de la communication en juin 2013 à M. Francis Brun-Buisson, conseiller-maître à la Cour des comptes. Cette médiation a pour objectif de parvenir à la signature d'un code de bonnes pratiques professionnelles en matière d'utilisation de photographies de presse afin, notamment, de sensibiliser au respect des droits moraux et patrimoniaux des photographes sur l'Internet et de limiter l'utilisation de la mention dite « droits réservés », qui, utilisée abusivement, peut conduire à l'exploitation de photographies sans autorisation et sans rémunération de leurs auteurs.

En améliorant l'identification des photographies présentes sur les services de presse en ligne, le code de bonnes pratiques vise également à faire bénéficier les photographes et les agences d'une meilleure rémunération pour l'exploitation de leurs œuvres sur l'Internet. La signature dudit code de bonnes pratiques devrait intervenir prochainement.

Source : direction générale des médias et des industries culturelles (DGMIC) du ministère de la culture et de la communication.

La DGMIC pointe aussi le risque que certains contenus culturels, notamment des œuvres audiovisuelles et cinématographiques européennes ou d'expression française, même s'ils sont effectivement présents dans l'immensité de l'Internet, soient de moins en moins accessibles, et donc atteignent de moins en moins leur public en pratique.

Une réflexion sur l'évolution du cadre législatif européen et national doit donc être menée afin de s'assurer que l'ensemble des distributeurs, y compris les moteurs de recherche ou les magasins d'applications par exemple, **prennent leur part à l'objectif de politique publique de diversité culturelle**. C'est le sens des propositions relatives à un conventionnement des services de médias audiovisuels à la demande qui ont été articulées par le rapport Lescure en mai 2013, sur le fondement desquelles, notamment, le Gouvernement poursuit ses travaux d'élaboration d'un projet de loi relatif à la création artistique. C'est le sens également des démarches menées par la France sur la scène européenne, le Gouvernement étant conscient que ces problématiques ne sauraient être appréhendées au seul échelon national, en vue d'une révision de la directive « Services de médias audiovisuels » (SMA) qui permettent d'en élargir le champ d'application tout en traitant le problème de la territorialité du droit.

Une piste envisagée consisterait à substituer au principe du pays d'origine celui du pays de destination des services. Ainsi, à l'instar du dispositif retenu pour la directive TVA , quel que soit le lieu d'établissement des services en Europe, la réglementation française serait appliquée à la partie du service qui est principalement destinée au public français. Néanmoins, cela irait à l'encontre de l'objectif européen d'établissement d'un marché unique, même en matière audiovisuelle.

Afin de garantir la diversité culturelle européenne, un autre champ de réflexion pourrait être lancé autour d'obligations de « mise en avant » des services assurant la promotion d'œuvres européennes par tous les distributeurs de services quels qu'ils soient (plateformes de vidéo en ligne, fournisseurs d'accès à Internet, constructeurs de matériels...).

L'Union européenne a entrepris plusieurs chantiers dans la perspective d'une évolution du cadre législatif. En matière de chronologie des médias, la Commission européenne a initié le projet MEDIA pour expérimenter la diffusion simultanée des œuvres cinématographique en salle et en vidéo à la demande.

Le projet « des licences pour l'Europe », achevé en novembre 2013 et destiné à développer l'offre légale de contenus en ligne, nécessite d'être relancé : il reste à approfondir les modalités de la portabilité transfrontalière des services et à réfléchir sur les contenus créés par les utilisateurs, sur le patrimoine audiovisuel et sur la « fouille » de textes et de données (*data mining*).

Enfin, la rémunération pour copie privée a reçu le soutien du Parlement européen qui a adopté le 27 février 2014 le rapport de Mme Françoise Castex, députée européenne, faisant suite à un rapport de M. Antonio Vitorino remis en janvier 2013. Mais la Commission a décidé de poursuivre ses travaux en vue

d'une harmonisation européenne dans le cadre de sa réflexion d'ensemble sur le droit d'auteur.

b) Des initiatives nationales non coordonnées à l'échelle de l'Union européenne

La question du partage équitable de la valeur a tout particulièrement cristallisé l'action de plusieurs États membres dans le différend opposant les éditeurs de presse et Google ; les données du problème étant l'utilisation faites des articles de presse ou d'extraits par ses algorithmes de recherche en vue de leur publication sur la page *Google news*, sans rémunération des auteurs et des éditeurs de presse.

La réponse en ordre dispersé à cette problématique est symptomatique de la difficulté des auteurs de contenus comme des États à appréhender les bouleversements introduits par l'Internet dans le monde de l'édition et du marché publicitaire. Le constat demeure pour l'heure celui de l'impuissance :

– s'agissant en premier lieu de **l'Allemagne**, sur le volet de la protection des droits d'auteurs, une loi dite « *Lex Google* » a été adoptée en août 2013, obligeant les agrégateurs ou moteurs de recherche commerciaux à reverser une commission aux éditeurs de presse pour l'utilisation d'articles d'actualité, les éditeurs devant à leur tour rémunérer les auteurs de ces articles. En fait, Google a mis en place volontairement avant l'entrée en vigueur de la loi un système d'option (*opt-in*) pour les éditeurs de presse qui veulent figurer gratuitement sur Google News, ce qui a privé la loi d'effet utile ;

– de son côté, **la France** a préféré négocier directement avec Google, dans le cadre d'un accord conclu et entré en application le 13 juin 2013 entre le moteur de recherche et l'association de la presse d'information politique et générale, l'alimentation d'un fonds de 60 millions d'euros sur trois ans pour soutenir la numérisation du marché de la presse. L'État n'est pas partie prenante à l'accord mais veille à son application dans l'intérêt du pluralisme de la presse ;

– enfin, **le gouvernement espagnol** s'est focalisé sur la question de la captation de valeur publicitaire des moteurs de recherche sur les contenus éditoriaux offerts par les sites de presse en proposant un dispositif s'inspirant de l'exemple allemand et instaurant un mécanisme de négociation de compensations entre les agrégateurs de contenus et les organismes de gestion collective de droits, sous l'égide d'une agence administrative.

Cette différence d'approches, qu'elles soient conventionnelle ou législative, justifierait qu'une réflexion spécifique soit lancée au niveau européen pour définir une position commune et donner plus de poids au marché européen face aux grandes plateformes de services.

Proposition n° 16 : inciter les fédérations professionnelles du secteur culturel à se rapprocher entre États membres pour faire valoir leurs droits en étant unies face aux plateformes « *over the top* »

c) La nécessité d'aligner les taux de TVA des produits culturels numériques et physiques

La directive 2006/112/CE, qui encadre la TVA au niveau européen, prohibe l'application de taux réduits aux services fournis par voie électronique. La Commission européenne considère que l'application en France du taux réduit de TVA au livre numérique homothétique et du taux super-réduit à la presse en ligne contreviennent au droit de l'Union européenne.

À cet égard, la Commission a saisi la Cour de justice de l'Union européenne (CJUE) contre la France s'agissant du taux réduit de TVA sur le livre numérique le 6 septembre 2013. Elle a par ailleurs lancé le 27 janvier 2014 une procédure d'alerte précontentieuse s'agissant du taux super-réduit de TVA sur la presse en ligne, procédure qu'elle vient de clore négativement. Elle s'apprête désormais à adresser une mise en demeure à la France.

Votre mission soutient l'objectif du gouvernement, qui est d'obtenir une évolution du cadre réglementaire de l'Union européenne permettant explicitement l'application de taux réduits non seulement pour le livre numérique homothétique, mais également pour la presse en ligne et, de manière générale, pour les biens et services culturels en ligne. Il s'agit d'obtenir une modification de la directive 2006/112/CE pour avoir la possibilité explicite d'appliquer des taux de TVA réduits aux biens et services culturels (livre, presse, vidéo, musique), y compris ceux prestés en ligne.

Pour M. Jacques Toubon, « *il est manifeste que la presse écrite est en train de mourir de la distribution numérique gratuite ! Il est donc impossible que la Commission refuse d'établir la neutralité fiscale entre ces deux activités* ».

Proposition n° 17 : aligner les taux de TVA des biens et services culturels numériques et physiques

d) Le besoin d'un cadre européen unique pour promouvoir les acteurs culturels européens sur l'Internet

Votre mission regrette que la question culturelle soit absente de la stratégie numérique pour l'Europe adoptée par la Commission européenne en 2010. Celle-ci s'est focalisée sur les questions relatives au marché unique numérique en matière de télécommunication, au déploiement du haut débit, à la confiance dans les transactions numériques ou à l'accessibilité des sites web du secteur public.

Pourtant, l'Europe possède des atouts puisqu'elle demeure un grand pourvoyeur de contenus culturels en ligne. C'est à un rééquilibrage qu'appelle M. Jacques Toubon :« *Nous devons faire en sorte que s'institue, d'une manière ou d'une autre, par la régulation, un équilibre entre ceux qui détiennent les savoirs, les logiciels, les produits, les terminaux et la puissance financière, et ceux qui, comme les Européens, n'ont pas encore réussi à faire émerger une industrie compétitive, mais apportent à l'écosystème des milliards de données et de contenus culturels numériques* ».

Ce constat appelle la création d'« *une politique européenne de la culture profitant de l'environnement numérique* ». Pour mettre en œuvre une telle politique, il **propose de conduire, notamment sous forme de coopération renforcée, des actions auxquelles seraient associés neuf, dix, ou douze États membres**.

Par ailleurs, votre mission d'information propose également que la Commission européenne intègre dans sa réflexion des propositions novatrices favorisant la créativité et la diversité culturelle, caractéristiques de la mise en réseau des savoirs, et donnant de la valeur à sa « *capacité contributive distribuée* », selon les termes employés par Mme Valérie Peugeot :

– en poursuivant la réflexion sur la réforme des droits d'auteurs dans le sens d'une reconnaissance et d'une protection des productions et création des auteurs dits « proams ». Mme Peugeot souligne que « *le web est le produit de ce que l'on a appelé des « proams » ; il participe à faire tomber la séparation historique entre producteur et consommateur, entre le créateur et son public, entre professionnel et amateur. Cette capacité contributive distribuée est un facteur clé de la créativité et de la diversité culturelle de nos sociétés*. » Il importe donc de trouver les moyens de la promouvoir ;

– en protégeant le développement des « Communs », ressources qui ne sont gérées ni par le marché et les droits de propriété classiques ni par la puissance publique, mais par des communautés auto-organisées autour de logiques de partage non marchands qui nourrissent la diversité culturelle et l'innovation sociale.

Pour préserver ces échanges non marchands, il faudrait donc inventer d'autres formes de rétribution des auteurs et laisser place à un espace où les ressources sont gérées sur le mode du partage. Mme Peugeot avance ainsi l'idée d'un « *bundle of rights* », un faisceau de droits dans lequel on pourrait imaginer un découplage du droit d'usage.

Proposition n° 18 : intégrer une nouvelle dimension à la politique européenne de la culture, valorisant la créativité des internautes et le partage non marchand de contenus.

B. UN RÉGIME EXIGEANT ET RÉALISTE DE PROTECTION DES DONNÉES À L'ÈRE DU CLOUD *ET DU* BIG DATA

À en croire certains, et notamment nos partenaires américains, le régime européen de protection des données personnelles serait devenu totalement obsolète car fondé sur les principes de finalité et de proportionnalité, incompatibles avec le *big data*. Ce dernier défierait en effet le principe de proportionnalité dans la mesure où il consiste en une « *accumulation sans cesse croissante de données afin d'augmenter toujours les potentialités d'exploitation et de faciliter l'apparition d'usages imprévus lors de la collecte* », ainsi que l'expliquait à

votre mission d'information M. Laurent Cytermann, rapporteur général adjoint du Conseil d'État. Aussi mettrait-il à mal le principe de finalité « *dès lors que la valorisation des données passe par leur réutilisation à des fins autres que celles pour lesquelles elles ont été collectées mais qu'on ne connaît pas à l'avance* », rendant « *absurde* » un dispositif reposant sur le principe du consentement préalable, pour reprendre les mots de M. Viktor Mayer-Schönberger, professeur à l'*Oxford Internet Institute*.

Par ailleurs, le *cloud computing* et l'hébergement de nos données sur des serveurs distants détenus par des sociétés le plus souvent de droit américain, feraient échapper nos propres données, y compris personnelles, à la législation européenne ou, plus précisément, les soumettraient à un droit américain moins protecteur et devenu extraterritorial avec l'adoption du *Patriot Act*[1].

1. Soutenir la validité de l'approche européenne fondée sur l'affirmation d'un droit fondamental à la protection des données personnelles

Bien qu'en partie fondée, la critique consistant à dénoncer l'obsolescence du cadre juridique européen à l'heure du *big data* repose en fait sur la prétendue opposition voire incompatibilité entre le droit et l'innovation. **Les détracteurs du droit préconisent ainsi de renoncer à la régulation au profit de l'autorégulation, la technique étant seule capable de répondre à la technique**.

Tel est notamment le cas des voix qui s'élèvent, en particulier outre-Rhin, depuis les révélations de l'affaire Snowden pour appeler à un renforcement de nos capacités de chiffrement et à une diffusion de cette pratique. Toutefois, comme on l'a vu précédemment, le programme *Bullrun* de la NSA démontre précisément l'inutilité des efforts en la matière puisque l'agence de renseignement américaine avait tout mis en œuvre pour affaiblir les logiciels et même les normes de chiffrement pour se ménager des « portes dérobées ». Au surplus, **répondre par la technique à un problème posé par la technique ne résout pas de manière définitive les difficultés car une nouvelle technique permettra toujours de contourner les sécurités instaurées par la précédente technique**. Si le passage des clés de chiffrement de 1 024 bits à 2 048 bits rend *a priori* le chiffrement plus difficile à casser, ce n'est probablement qu'une question de temps avant le développement de l'ordinateur quantique auquel la NSA travaillerait activement selon Edward Snowden. Le chiffrement ne fait que renchérir la surveillance en ligne sans l'empêcher.

Dans le même ordre d'idées, les procédés d'anonymisation connaissent eux aussi des limites. Comme le rappelaient certaines des personnes entendues par votre mission d'information, dans le *big data*, peu de données personnelles sont en jeu et, lorsque de telles données sont collectées et utilisées, leur intérêt ne réside pas tant en ce qu'elles dévoilent d'un individu mais en ce qu'agrégées, elles

[1] Cf. supra

« disent » de populations entières (*cf. supra* les méthodes probabilistes mises en œuvre pour exploiter le *big data*). C'est pourquoi, les techniques d'anonymisation sont souvent présentées comme la solution pour protéger les personnes physiques à l'égard du traitement de leurs données personnelles. Cependant, les facultés de réidentification vont s'accroissant[1], ce qui a conduit le groupe de protection des personnes à l'égard du traitement des données à caractère personnel, dit « Groupe de l'article 29 » ou « G 29 », qui rassemble les autorités de protection des États membres de l'Union européenne, à émettre une recommandation le 10 avril dernier invitant les responsables de traitement ayant anonymisé des données à effectuer une veille régulière afin de s'assurer du maintien dans le temps du caractère anonyme de celles-ci.

Pour autant, **tourner le dos à la technique reviendrait à se priver d'outils à même de contribuer à l'efficience du droit**. C'est tout l'intérêt de l'approche en termes de « ***privacy by design*** » ou « confidentialité des données dès la conception », c'est-à-dire la technique intégrant les contraintes juridiques dès l'origine. Lors de son audition, M. Bernard Benhamou citait l'exemple des puces RFID[2] : « *de nouvelles actions sont possibles et doivent faire l'objet de négociations internationales, pour une régulation des technologies de l'Internet. Je pense, par exemple, au « droit au silence des puces», c'est-à-dire au fait que les objets connectés qui seront présents dans notre environnement puissent être désactivés : il faut le prévoir en amont, dès la conception des matériels, et non en aval lorsque ces objets seront massivement présents dans l'environnement des citoyens*. »

De même, faire de la protection des données le critère par défaut dans le réglage des paramètres d'un appareil ou d'une application permet de s'assurer du consentement de la personne pour activer des fonctionnalités potentiellement attentatoires à sa vie privée comme la géolocalisation. Cette « ***privacy by default*** » ou « confidentialité des données par défaut » devrait ainsi être la norme par exemple sur les réseaux sociaux.

Depuis la loi du 6 août 2004 qui a modifié la loi « Informatique et libertés », la Commission nationale de l'informatique et des libertés (CNIL) peut délivrer des **labels** « *à des produits ou à des procédures tendant à la protection des personnes à l'égard du traitement des données à caractère personnel, après qu'elle les a reconnus conformes aux dispositions de la […] loi [Informatique et libertés]* »[3]. D'autres pays européens, en particulier l'Allemagne, se sont engagés dans semblables démarches de labellisation ou de certification, si bien que la Commission

---

[1] Cf. *les développements consacrés à ce sujet dans* La protection des données personnelles dans l'open data : une exigence et une opportunité, *rapport d'information de MM. Gaëtan Gorce et François Pillet, fait au nom de la commission des lois (n° 469, 2013-2014) (disponible à l'adresse suivante : http://www.senat.fr/notice-rapport/2013/r13-469-notice.html).*

[2] *Pour* Radio Frequency Identification, *permettant d'identifier et de localiser sans contact des objets ou des personnes grâce à une puce (également dénommée étiquette ou tag) qui dialogue par ondes radio avec un lecteur, sur des distances pouvant aller de quelques centimètres à une dizaine de mètres.*

[3] Cf. *le c du 3° de l'article 11 de la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*.

européenne a décidé d'expérimenter la mise en place d'un label européen. Conduite avec succès de 2007 à 2009 sous l'égide de l'autorité de protection des données du Land de Schleswig-Holstein, cette expérimentation a été pérennisée. Le projet « EuroPriSe » (pour *European Privacy Seal*, « Label européen de protection de la vie privée ») est actuellement géré par un consortium réunissant les autorités de protection des données ou organismes privés de certification de huit États membres : l'Allemagne, l'Autriche, l'Espagne, la France, les Pays-Bas, le Royaume-Uni, la Slovaquie et la Suède. La proposition de règlement européen sur la protection des données personnelles en cours de discussion intègre d'ailleurs cette dimension puisque son considérant 77 encourage « *la création de mécanismes de certification, ainsi que de labels et de marques normalisées en matière de protection des données* ». Il appelle également à la création au niveau européen d'un « label européen de protection des données » « *afin de générer un climat de confiance chez les personnes concernées et une sécurité juridique pour les responsables du traitement et, dans le même temps, exporter les normes européennes de protection des données en permettant aux entreprises non européennes d'entrer sur les marchés européens en obtenant cette certification* ».

L'étape suivante serait donc de parvenir à l'élaboration de labels au niveau international.

Proposition n° 19 : promouvoir le *privacy by design* et le *privacy by default* par des labels européens et internationaux.

Si les labels sont tellement plébiscités, au premier chef par les acteurs économiques, c'est qu'ils sont perçus comme susceptibles de procurer un avantage concurrentiel dès lors qu'ils permettent d'attester aux yeux des consommateurs de la qualité d'un produit ou d'un service, tout en participant de la diffusion de la « culture Informatique et libertés ».

Ainsi, **loin de constituer un frein à l'innovation, le droit peut inciter l'industrie à être plus innovante**. Lors de l'examen au Sénat d'une proposition de loi visant à encadrer l'usage des techniques biométriques, ce point a été souligné à de multiples reprises[1]. Bien que la France soit l'un des seuls pays au monde, si ce n'est le seul, à encadrer l'usage de la biométrie par un contrôle préalable de la CNIL, l'industrie française dans ce secteur a développé une expertise mondialement reconnue. De l'avis de tous, le travail mené entre les acteurs économiques et la CNIL a de fait permis une émulation de l'industrie française qui a dû développer des solutions pour sécuriser au mieux la mise en œuvre de traitements biométriques, afin de répondre aux exigences de la législation sur la

[1] *Proposition de loi visant à limiter l'usage des techniques biométriques, présentée par M. Gaëtan Gorce et les membres du groupe socialiste (n° 361, 2013-2014). Lors de l'examen en séance publique, Mme Axelle Lemaire, secrétaire d'État chargée du numérique, a ainsi indiqué :* « Notre pays compte des sociétés innovantes qui ont développé des technologies en lien avec la confiance numérique. Ce secteur, en plein essor, est une source d'attractivité économique pour la France, qui dispose d'une législation protectrice en matière d'utilisation des données : nos sociétés ont dû s'adapter au cadre législatif et réglementaire et développer des technologies qui sont aujourd'hui recherchées à l'étranger. » *(http://www.senat.fr/seances/s201405/s20140527/s20140527010.html)*

protection des données personnelles. Cet exemple de la biométrie illustre donc l'affirmation de Mme Isabelle Falque-Pierrotin devant votre mission d'information, selon laquelle « *le domaine de la protection des données personnelles est un facteur de l'identité européenne suffisamment consensuel pour constituer un atout pour son industrie* ».

Inversement, comme l'indiquait M. Viktor Mayer-Schönberger, « *il y a là une opportunité pour nous autres Européens de développer de nouveaux services et à travers notre puissance économique, démontrer notre volonté d'une meilleure protection de notre vie privée.* » S'appuyant sur l'exemple de Microsoft qui annonçait il y a peu qu'il envisageait la possibilité de ne stocker les données des internautes européens que sur le sol européen, ce professeur invitait les Européens à une « approche pragmatique » : « *quel rôle pour l'Union européenne face à la prédominance des États-Unis ? La réponse est somme toute assez simple : les entreprises de l'Internet américaines font de 30 à 40 % de leurs bénéfices en Europe, où elles doivent se conformer au droit européen.* » **Parce que l'Europe représente un marché si important pour les entreprises du monde entier, elle est en mesure d'imposer sur son territoire ses propres règles du jeu**.

Dès lors, quelles règles mettre en place ?

Les tenants d'un droit à la propriété de ses données personnelles mettent en avant la faculté qu'auraient les individus à tirer profit eux-mêmes de leurs données tout en gardant la maîtrise de leur identité numérique. Ainsi, la richesse produite par l'exploitation des données personnelles reviendrait au véritable propriétaire, non aux entreprises qui prospèrent grâce aux données d'autrui. M. Pierre Bellanger, fondateur et PDG de la radio Skyrock, déclarait devant votre mission d'information : « *première action à entreprendre : établir la propriété des données. Aujourd'hui, elles sont* res nullius *: leur usage est réglementé, mais elles ne sont la propriété de personne. Nous avons le droit d'auteur, mais pas celui de nos données, qui sont pourtant la trace de ce que nous sommes les auteurs de notre vie ! […] Ce statut de propriété privée des données changerait d'un coup toute l'économie numérique aujourd'hui fondé sur le pillage des données personnelles.* »

Cependant, ainsi que le remarquaient nos collègues Mme Anne-Marie Escoffier et M. Yves Détraigne dans leur rapport de 2009 sur la vie privée à l'heure des mémoires numériques[1], la patrimonialisation des données personnelles soulève de nouvelles difficultés car la propriété implique la cessibilité. En cas de cession, l'individu perdrait tout droit sur ses données personnelles. Accorder un droit de propriété de chacun sur ses données personnelles emporterait par ailleurs un risque de marchandisation de celles-ci. Cela reviendrait à renvoyer la responsabilité de la protection de ses données à l'individu alors même que l'on connaît la forte inégalité du rapport de force qui

[1] La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information, *rapport d'information de M. Yves Détraigne et Mme Anne-Marie Escoffier, fait au nom de la commission des lois (n° 441, 2008-2009) (disponible à l'adresse suivante : http://www.senat.fr/notice-rapport/2008/r08-441-notice.html).*

oppose le consommateur aux entreprises. Au demeurant, comme l'expliquait Mme Valérie Peugeot, un tel droit de propriété ne pourrait qu'aboutir au « *renforcement des inégalités entre citoyens numériques, entre ceux en capacité de gérer leurs données, de les protéger, les monétiser, et ceux qui par manque de littératie, de temps, ou toute autre raison, laisseraient faire par défaut le marché* »[1].

Une solution pourrait dès lors être de créer un droit de propriété spécifique prévoyant l'incessibilité des données personnelles mais autorisant seulement un droit d'usage des données, une forme de location. Cependant les données pouvant être facilement dupliquées, cela reviendrait *in fine* à faire échapper les données à leur propriétaire. D'où l'idée développée par certains, par analogie avec le droit d'auteur, de soumettre les données personnelles à un régime de propriété intellectuelle instaurant un droit exclusif d'usage pour les individus. Cependant, il est constant que de simples informations ne constituent pas en tant que telles des œuvres de l'esprit, de sorte qu'elles ne peuvent bénéficier de la protection d'un droit de propriété intellectuelle impliquant création et originalité. L'une ou l'autre solution nécessiterait au surplus l'élaboration d'un nouveau régime dérogatoire alors même que les données personnelles bénéficient déjà, dans le droit en vigueur, d'un statut spécifique.

Par ailleurs, **ces propositions et l'idée de monétisation des données personnelles qui les sous-tend vont à l'encontre de la conception européenne de la vie privée qui place sa protection sur le terrain des droits et libertés fondamentaux**. Ainsi, l'article 8 de la Charte des droits fondamentaux de l'Union européenne proclame le droit de toute personne à la protection des données à caractère personnel la concernant. Conformément à ce même article, il découle de ce droit celui de consentir au traitement loyal des données à des fins déterminées, à moins qu'une loi n'autorise à passer outre ce consentement, ainsi que le droit de toute personne « *d'accéder aux données collectées la concernant et d'en obtenir la rectification* ».

Comme le rappelait Mme Isabelle Falque-Pierrotin lors de son audition par votre mission d'information, **la protection ainsi assurée aux données personnelles est plus forte que celle qu'un droit de propriété sur ses données personnelles garantirait à l'individu**. Cette approche en termes de droit fondamental permet à l'individu de conserver des droits sur ses données personnelles même lorsque quelqu'un d'autre en fait usage. Cette affirmation est confortée par l'arrêt *Google Spain* rendu par la Cour de justice de l'Union européenne le 13 mai dernier, par lequel la juridiction a jugé que les droits fondamentaux énoncés aux articles 7[2] et 8 de la Charte « *prévalent, en principe, non seulement sur l'intérêt économique de l'exploitant du moteur de recherche, mais également sur l'intérêt [du] public à accéder à [une] information lors d'une recherche*

---

[1] *Cf. Mme Valérie Peugeot,* Données personnelles, sortir des injonctions contradictoires *(disponible à l'adresse suivante : http://vecam.org/article1289.html.)*

[2] *L'article 7 de la Charte dispose que* « toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications. »

portant sur le nom [d'une] personne. » Le juge a également souligné que le demandeur n'avait pas à faire la démonstration d'un quelconque préjudice.[1]

2. Conforter en le modernisant le cadre juridique européen de protection des données

S'adossant à l'article 8 de la Charte des droits fondamentaux de l'Union européenne, le régime juridique européen de protection des données personnelles repose sur **quatre principes cardinaux** :

– le **principe de finalité** qui précise que les données personnelles ne peuvent être collectées que pour des finalités déterminées, explicites et légitimes et ne peuvent être traitées ultérieurement de manière incompatible avec ces finalités ;

– le **principe de proportionnalité**, connexe au précédent, qui dispose non seulement que les données personnelles collectées doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées, mais encore qu'elles ne peuvent être conservées que pendant une durée n'excédant pas la durée nécessaire aux finalités ;

– le **principe de sécurité** des données personnelles, un responsable de traitement devant prendre toutes les précautions utiles pour préserver les données de toute déformation, endommagement ou fuite ;

– les **droits de l'individu relativement à ses données personnelles,** de consentir ou de s'opposer à leur collecte, d'y accéder et d'en obtenir rectification.

Ces principes, posés en France dès la loi « Informatique et libertés » du 6 janvier 1978 et repris dans la directive européenne de 1995[2], ont permis jusqu'à aujourd'hui de protéger les citoyens européens à l'égard du traitement de leurs données personnelles malgré les évolutions technologiques. Mme Isabelle Falque-Pierrotin déclarait devant votre mission d'information que « *l'espace juridique européen a donc apporté la preuve qu'il était suffisamment robuste pour intégrer l'innovation, même lorsque sont remises en cause les approches traditionnelles comme c'est par exemple le cas avec le* big data. » Et de renchérir en indiquant que « *l'idée du projet de règlement est donc de convaincre les Américains, mais aussi et surtout les Européens, que le cadre juridique de l'Union européenne est suffisamment souple pour*

---

[1] Cf. *le considérant 99 de l'arrêt CJUE, gr. ch., 13 mai 2014, aff. C-131/12 :* « dans le cadre de l'appréciation des conditions d'application de ces dispositions [les articles 12, sous b), et 14, premier alinéa, sous a), de la directive 95/46], il convient notamment d'examiner si la personne concernée a un droit à ce que l'information en question relative à sa personne ne soit plus, au stade actuel, liée à son nom par une liste de résultats affichée à la suite d'une recherche effectuée à partir de son nom, sans pour autant que la constatation d'un tel droit présuppose que l'inclusion de l'information en question dans cette liste cause un préjudice à cette personne. »

[2] *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données*.

intégrer l'innovation tout en offrant des garanties pour les consommateurs. Au regard de la gouvernance juridique des données, l'Union européenne peut donc se prévaloir d'outils robustes à la fois offensifs et défensifs. »

Présentée par la Commission européenne le 25 février 2012[1], cette proposition de règlement vise à remplacer la directive de 1995 pour harmoniser les règles de protection des données personnelles sur le territoire de l'Union européenne. Elle ne représente pas tant une remise à plat de ces règles qu'un changement de valeur juridique dans la mesure où un règlement est d'application directe et immédiate, contrairement à une directive. Cette transformation est cependant l'occasion d'actualiser ce régime juridique en y apportant des améliorations, dont certaines sont susceptibles de fournir des solutions aux difficultés évoquées précédemment. Après deux ans de négociation, leur finalisation n'est toujours pas parvenue à son terme.

a) Redéfinir le principe de proportionnalité

En réponse au défi lancé par le *big data* aux principes de finalité et de proportionnalité, il est envisagé de procéder à **l'examen de l'adéquation entre les moyens mis en œuvre et les objectifs poursuivis non au stade de l'utilisation des données mais dès leur collecte**. Tel est le sens du principe de « minimisation » retenu par le Parlement européen à l'initiative de la commission LIBE. L'article 5 de la résolution législative du 12 mars 2014 impose ainsi que les données à caractère personnel collectées sont « *adéquates, pertinentes et limitées au minimum nécessaire au regard des finalités pour lesquelles elles sont traitées ; elles ne sont traitées que si, et pour autant que, les finalités du traitement ne peuvent pas être atteintes par le traitement d'informations ne contenant pas de données à caractère personnel* ».

La même solution semble être privilégiée par la Cour de justice de l'Union européenne dans son arrêt *Digital Rights Ireland Ltd/Kärntner Landesregierung* du 8 avril 2014. Par cette décision, la Cour a invalidé la directive dite « *data retention* »[2] pour défaut d'adéquation stricte entre l'objectif de lutte contre les infractions graves et une conservation indifférenciée des données de connexion, sans limitation ni temporelle, ni géographique, ni circonscrite à des personnes susceptibles d'être associées à une infraction grave.

---

[1] Cf. *la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) (COM(2012)11) et la résolution législative du Parlement européen du 12 mars 2014 sur la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) (COM(2012)11 – C7-0025/2012 – 2012/0011(COD))*.

[2] *Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE*.

L'invalidation de la directive « *data retention* » pour défaut de proportionnalité

Par un arrêt de grande chambre en date du 8 avril 2014[1], la Cour de justice de l'Union européenne a invalidé la directive sur la conservation des données de connexion, dite directive « *data retention* ».

Cette décision est intervenue sur renvois préjudiciels de la Cour suprême irlandaise et de la Cour constitutionnelle autrichienne. Celles-ci s'interrogeaient sur la compatibilité de la directive, en ce qu'elle permettait le stockage en masse de données relatives à la quasi-totalité de la population de l'Union, sans ciblage spécifique, pour une durée allant jusqu'à deux ans, avec le droit au respect de la vie privée et familiale, et le droit à la protection des données à caractère personnel, garantis par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne.

La Cour a considéré que l'obligation de conservation et de traitement des données ainsi que l'accès des autorités nationales compétentes à celles-ci, prévues par la directive, constituaient une ingérence dans les droits précités d'autant plus grande que les utilisateurs n'en étaient pas informés. Si cette ingérence répondait à un objectif d'intérêt général de l'Union européenne – « *la lutte contre la criminalité grave afin de garantir la sécurité publique* » –, elle n'en était pas moins disproportionnée dans la mesure où :

– l'obligation de conservation des données couvrait « *de manière généralisée toute personne et tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic sans qu'aucune différenciation, limitation ni exception soient opérées en fonction de l'objectif de lutte contre les infractions graves* » ;

– l'accès aux données collectées était trop large, insuffisamment encadré et ne faisait l'objet d'aucun contrôle préalable par une juridiction ou une autorité indépendante ;

– la durée de conservation oscillait entre 6 mois et 2 ans sans distinction entre les données en fonction des personnes ni des infractions concernées. Et de conclure « *que la directive 2006/24 ne prévoit pas de règles claires et précises régissant la portée de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte* », ingérence qualifiée « *d'une vaste ampleur et d'une gravité particulière dans l'ordre juridique de l'Union* ».

b) Réaffirmer l'applicabilité des normes européennes sur le territoire européen

La prédominance des acteurs américains du numérique sur le marché européen pose de manière récurrente la question de l'applicabilité des normes européennes sur le territoire même de l'Union européenne.

L'arrêt *Google Spain* de la Cour de justice de l'Union européenne précité en est une illustration. La Cour était interrogée par la justice espagnole sur l'interprétation de l'article 4 de la directive de 1995 qui prévoit notamment que celle-ci s'applique dès lors que le traitement de données personnelles est effectué « dans le cadre des activités » d'un établissement sur ce territoire, non « par » un établissement situé sur ce territoire. La Cour a d'abord rappelé que l'objectif de la directive est d'assurer une garantie efficace et complète des droits fondamentaux des personnes, du droit à la vie privée et de la protection des données à caractère personnel. Puis, elle a noté que « *les activités de l'exploitant du moteur de recherche et*

[1] *CJUE, gr. ch., 8 avril 2014, aff. C-293/12.*

celles de son établissement situé dans l'État membre concerné sont indissociablement liées dès lors que les activités relatives aux espaces publicitaires constituent le moyen pour rendre le moteur de recherche en cause économiquement rentable et que ce moteur est, en même temps, le moyen permettant l'accomplissement de ces activités. ». En conséquence, la Cour conclut qu'« *un traitement de données à caractère personnel est effectué dans le cadre des activités d'un établissement du responsable de ce traitement sur le territoire d'un État membre […], lorsque l'exploitant d'un moteur de recherche crée dans un État membre une succursale ou une filiale destinée à assurer la promotion et la vente des espaces publicitaires proposés par ce moteur et dont l'activité vise les habitants de cet État membre.* »

Cet arrêt témoigne de la nécessité de réaffirmer de manière forte l'applicabilité du droit européen sur le territoire de l'Union européenne. C'est pourquoi la proposition de règlement intègre en son article 3 le critère de l'activité dirigée afin de **rendre de manière indiscutable le règlement applicable aux responsables de traitement établis hors de l'Union européenne s'ils traitent de données de résidents de l'Union européenne dans le cadre de l'offre de biens ou de services à ces résidents, ou dans le cadre de l'observation de leur comportement**[1].

Compétence juridictionnelle, loi applicable et activité dirigée

Issu des règlements européens Bruxelles I[2] et Rome I[3] relatifs à la détermination de la juridiction compétente et à la loi applicable en matière de litiges transfrontaliers intra-européens, **ce critère de l'activité dirigée a été forgé pour protéger le consommateur dans ses relations contractuelles avec des professionnels**.

En cas de litiges nés de tels contrats, le règlement Bruxelles I attribue la compétence au juge de l'État membre sur le territoire duquel est domicilié le consommateur lorsque le contrat a été conclu avec un prestataire « *qui, par tout moyen, dirige ses activités vers cet État membre ou vers plusieurs États, dont cet État membre* », à moins que le consommateur, à l'origine de l'action, n'en décide autrement, ou qu'une clause n'ait attribué la compétence au juge de l'État membre où résidaient les deux parties au moment de la conclusion du contrat. Le règlement Bruxelles I *bis* étendra cette règle aux prestataires établis hors de l'Union européenne à partir de 2015.

[1] *Art. 3, paragraphe 2, de la résolution législative du Parlement européen du 12 mars 2014 :*
« 2. Le présent règlement s'applique au traitement des données à caractère personnel appartenant à des personnes concernées dans l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées :
« a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes concernées ; ou
« b) à l'observation de ces personnes concernées. »

[2] *Règlement (CE) n° 44/2001 du Conseil du 22 décembre 2000 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale, dit « Bruxelles I ». Ce règlement a fait l'objet d'une refonte qui étend aux États tiers l'application du critère de l'activité dirigée (règlement (UE) n° 1215/2012 du Parlement européen et du Conseil du 12 décembre 2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale (refonte)).*

[3] *Règlement (CE) n° 593/2008 du Parlement européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations contractuelles, dit « Rome I ».*

Le règlement Rome I précise quant à lui que la loi applicable à ces litiges est celle du pays de résidence du consommateur, à condition que le professionnel exerce ses activités ou dirige ses activités dans ce pays. Il précise en outre que les parties peuvent également, au titre de la liberté de choix, appliquer une autre loi, à condition que cette loi apporte le même niveau de protection au consommateur que celle de son État de résidence.

Dans un arrêt du 7 décembre 2010, la Cour de justice de l'Union européenne a précisé cette notion d'activité dirigée en considérant qu'il appartenait au juge de rechercher les indices démontrant que le professionnel a manifesté sa volonté d'établir des relations commerciales avec les consommateurs d'un ou plusieurs autres États. Si « *la simple accessibilité du site Internet du commerçant ou de celui de l'intermédiaire dans l'État membre sur le territoire duquel le consommateur est domicilié* » de même que « *la mention d'une adresse électronique ainsi que d'autres coordonnées ou de l'emploi d'une langue ou d'une monnaie qui sont la langue et/ou la monnaie habituellement utilisées dans l'État membre dans lequel le commerçant est établi* » sont insuffisantes pour établir la compétence du juge du pays de résidence du consommateur, la Cour a en revanche énuméré certains des indices permettant au juge d'établir cette activité dirigée :

« *Les éléments suivants, dont la liste n'est pas exhaustive, sont susceptibles de constituer des indices permettant de considérer que l'activité du commerçant est dirigée vers l'État membre du domicile du consommateur, à savoir la nature internationale de l'activité, la mention d'itinéraires à partir d'autres États membres pour se rendre au lieu où le commerçant est établi, l'utilisation d'une langue ou d'une monnaie autres que la langue ou la monnaie habituellement utilisées dans l'État membre dans lequel est établi le commerçant avec la possibilité de réserver et de confirmer la réservation dans cette autre langue, la mention de coordonnées téléphoniques avec l'indication d'un préfixe international, l'engagement de dépenses dans un service de référencement sur Internet afin de faciliter aux consommateurs domiciliés dans d'autres États membres l'accès au site du commerçant ou à celui de son intermédiaire, l'utilisation d'un nom de domaine de premier niveau autre que celui de l'État membre où le commerçant est établi et la mention d'une clientèle internationale composée de clients domiciliés dans différents États membres.* »[1]

À l'initiative du Parlement européen, ce même article 3, en son paragraphe 1, prévoit également que le règlement « *s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement de données ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou pas dans l'Union* », afin d'inclure l'hypothèse du *cloud computing*.

c) Renforcer les droits des internautes : recours collectif et alternative au « guichet unique »

Participe par ailleurs du renforcement des droits des internautes européens la création, par la proposition de règlement européen, d'une **action de groupe en matière de protection des données personnelles**. Le paragraphe 2 de son article 73 dispose ainsi que « *tout organisme, organisation ou association qui agit dans l'intérêt public et qui a été valablement constitué conformément au droit d'un État membre a le droit d'introduire une réclamation auprès d'une autorité de contrôle dans*

[1] *CJUE, 7 déc. 2010, aff. C-585/08, P. Pammer c/ Reederei Karl Schlüter GmbH & Co KG et aff. C-144/09, Hotel Alpenhof GesmbH c/ O. Heller, considérant n° 93.*

tout État membre au nom d'une ou de plusieurs personnes concernées, s'il considère que les droits dont jouit une personne concernée en vertu du présent règlement ont été violés à la suite du traitement de données à caractère personnel ».

En revanche, un point de la proposition de règlement a fortement cristallisé les débats : le « **guichet unique** ». Afin de simplifier les formalités pour les entreprises, la Commission européenne avait proposé que dans le cas où un responsable de traitement est établi dans plusieurs États membres, l'autorité de contrôle de l'État membre où se situe l'établissement principal du responsable de traitement soit désignée comme chef de file. Comme le soulignait notre collègue Simon Sutour, si le critère de l'établissement principal ne pose pas de difficulté pour les contrôles préventifs et formalités préalables, il n'en va pas de même en cas de litige, « *l'application de ce critère [pouvant] conduire à ce qu'un citoyen voit sa réclamation traitée par une autre autorité que son autorité de contrôle nationale, parce que l'entreprise responsable du traitement est sise dans un autre État membre que celui où il réside. Ainsi, un Français formant une requête contre Facebook devrait l'adresser à l'autorité de contrôle irlandaise.* »[1] Cette analyse a d'ailleurs été confirmée par le service juridique du Conseil qui a fait connaître, lors de la réunion du Conseil Justice et affaires intérieures (JAI) des 5 et 6 décembre 2013, que le « guichet unique » était non conforme avec la Charte des droits fondamentaux de l'Union européenne du fait de l'éloignement de l'autorité chef de file par rapport aux personnes concernées. C'est pourquoi, une proposition alternative a été formulée, notamment par la France, consistant en la mise en place d'un mécanisme de codécision entre autorités de contrôle concernées, sous l'égide du Comité européen de protection des données.

La proposition de règlement a été adoptée à la quasi-unanimité par le Parlement européen lors de sa séance du 12 mars 2014. Cependant, certains désaccords persistent entre les États membres. À l'issue du Conseil Justice et Affaires intérieures des 5 et 6 juin, des progrès ont certes été enregistrés, les États membres s'accordant notamment sur le champ territorial d'application du nouveau règlement ; d'autres points, en particulier le « guichet unique », restent cependant problématiques. Enfin, le Royaume-Uni demeure opposé au choix d'un règlement, en substitution de l'actuelle directive.

Votre mission estime quant à elle que cette proposition de règlement comporte des éléments de réponse aux difficultés constatées dans l'application de la directive de 1995. Elle appelle donc à une adoption rapide de ce texte.

Proposition n° 20 : adopter le plus rapidement possible la proposition de règlement européen sur la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

[1] Cf. *le rapport de M. Simon Sutour, fait au nom de la commission des lois, sur la proposition de résolution sur la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (E 7055) (n° 446, 2011-2012) (disponible à l'adresse suivante : http://www.senat.fr/dossier-legislatif/ppr11-406.html)*

Si cette proposition de règlement européen contient des avancées importantes, les auditions menées par votre mission d'information ont fait apparaître que d'autres améliorations pourraient être apportées au régime européen de protection des données personnelles.

d) Mieux protéger certaines données

Abondant dans le sens du président Gorce, Mme Isabelle Falque-Pierrotin a, lors de son audition par votre mission d'information, acquiescé à l'idée que « *certaines données doivent faire l'objet d'une attention particulière : les données biométriques, les données de santé…* ».

Pour reprendre ce premier exemple, les données biométriques font effectivement l'objet d'une vigilance croissante, comme en témoigne la proposition de loi précitée visant à limiter l'usage des techniques biométriques. Ainsi que le notait M. François Pillet, rapporteur pour la commission des lois du Sénat de cette proposition de loi, cet intérêt du Parlement français coïncide avec les préoccupations exprimées au niveau européen[1]. En effet, à l'occasion de la révision de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe, dite « Convention 108 », il a été proposé, en décembre 2012, d'intégrer au sein des données sensibles les données biométriques. L'article 6 de la convention, dans le projet final, stipule donc que « *le traitement de données biométriques identifiant un individu de façon unique […] n'est autorisé qu'à la condition que la loi applicable prévoit des garanties appropriées, venant compléter celles de la présente convention* ». Ce même article précise en outre que « *les garanties appropriées doivent être de nature à prévenir les risques que le traitement de données sensibles peut présenter pour les intérêts, droits et libertés fondamentales de la personne concernée, notamment un risque de discrimination* ».

De la même façon, à l'issue de l'examen par le Parlement européen en première lecture, de la proposition de règlement sur les données personnelles, les données biométriques ont été intégrées parmi les catégories particulières de données. L'article 9 de la résolution législative du Parlement européen du 12 mars 2014 pose le principe de l'interdiction du traitement de données biométriques[2], principe néanmoins tempéré par une série d'exceptions parmi lesquelles le consentement de la personne concernée, à moins qu'une disposition nationale y fasse obstacle.

---

[1] Cf. *le rapport n° 465 (2013-2014) disponible à l'adresse suivante : http://www.senat.fr/dossier-legislatif/ppl13-361.html.*

[2] *« 1. Le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les croyances philosophiques, l'orientation sexuelle ou l'identité de genre, l'appartenance et les activités syndicales, ainsi que le traitement des données génétiques ou biométriques ou des données concernant la santé ou relatives à la vie sexuelle, aux sanctions administratives, aux jugements, à des infractions pénales ou à des suspicions, à des condamnations, ou encore à des mesures de sûreté connexes sont interdits. »*

Ces données particulièrement sensibles doivent faire l'objet d'une protection renforcée, protection qui devrait passer, comme l'indiquait Mme Isabelle Falque-Pierrotin, « *par des garanties procédurales spécifiques : exigence d'étude d'impact, d'un consentement renforcé…* »

À l'inverse, aussi bien la CNIL que son homologue belge, selon les informations recueillies par votre mission auprès de notre ambassade dans ce pays, appellent l'attention sur la notion de « données pseudonymes », introduite au Parlement européen, craignant qu'une distinction opérée au sein des données personnelles ne conduise à un affaiblissement du régime de protection de ces dernières.

Proposition n° 21 : renforcer les garanties procédurales entourant le traitement des données particulièrement sensibles par l'obligation de fournir des études d'impact sur la vie privée.

e) Instaurer un régime de responsabilité du responsable de traitement de données

Au-delà de ces données sensibles, **l'évolution des technologies invite à repenser la définition des données personnelles afin d'en assurer une meilleure protection**.

À l'heure du *big data* et du profilage des individus par *online tracking*, le régime juridique conçu pour les « informations nominatives » des années 1970 ne paraît plus tout à fait adapté. Tel est le constat opéré par Mme Jessica Eynard, docteur en droit[1], qui rappelle que le régime de protection actuel est centré sur la personne, considérée comme la meilleure « gardienne » de ses propres données. Ainsi, le droit premier garanti est celui de l'information préalable, condition de mise en œuvre des autres droits que sont les droits *a priori*, à savoir le droit à consentir à un traitement ou, à l'inverse, le droit de s'y opposer, ainsi que les droits *a posteriori* – droit d'accès, droit de rectification, « droit à l'oubli » sous la forme d'un droit à la désindexation ou à l'effacement des données à l'issue d'un certain délai ou à la demande, et droit à la portabilité des données, comme la proposition de règlement européen se propose d'en créer un. La mise en œuvre de tous ces droits implique donc la connaissance par la personne concernée d'un traitement de ses données personnelles.

Désormais cependant, les données personnelles peuvent être recueillies et utilisées à l'insu de la personne ou sans que celle-ci soit capable d'apprécier la violation de sa vie privée que cela emporte. Dès lors, faire reposer le régime de protection sur la personne concernée ne permet plus de garantir effectivement cette protection. C'est pourquoi, Mme Jessica Eynard propose d'instituer pour ce nouveau type de données personnelles, définies comme « *toute information saisissant l'essence physique ou psychique de la personne physique identifiée ou identifiable qu'elle concerne et échappant intellectuellement et juridiquement à cette dernière* », un nouveau régime de protection sur le modèle de ce qui existe en droit

[1] *Mme Jessica Eynard est l'auteur de :* Les Données personnelles – quelle définition pour un régime de protection efficace ?, *Michalon, Paris, 2013.*

de la consommation. Concrètement, cela passerait par l'instauration d'un régime de responsabilité du responsable de traitement qui se verrait imposer une **obligation d'information de la personne concernée en cas d'irrégularité dans le traitement de ses données**, obligation à laquelle l'autorité de protection des données pourrait contraindre le responsable de traitement dans la mesure où en cas de refus de celui-ci, elle pourrait se substituer à lui à ses frais.

Un régime de responsabilité du responsable de traitement est également préconisé par M. Viktor Mayer-Schönberger qui constatait que dans le contexte du *big data*, « *on ne peut plus laisser les particuliers seuls face aux fournisseurs d'accès. C'est David contre Goliath sauf qu'à la différence de David, les individus n'ont pas les moyens pour exercer leurs droits.* » Lors de son audition par votre mission d'information, il a ainsi formulé la proposition suivante : « *rendre les entreprises directement responsables en les contraignant à réaliser des évaluations préalables à toute réutilisation de données, afin de prendre les mesures nécessaires pour réduire les risques et effets néfastes identifiés pour les usagers. Il faudrait qu'en cas d'infraction, la responsabilité tant civile que pénale des entreprises soit engagée. Cela permettrait aux enjeux de protection des données personnelles d'être ramenés au premier plan et de ne plus être considérés uniquement à l'aune de sanctions de quelques centaines de milliers d'euros. En retour, les entreprises pourraient réutiliser les données sans avoir à revenir auprès de l'internaute pour recueillir son consentement à chaque nouvelle réutilisation. Cela faciliterait d'ailleurs leur tâche.* » Selon lui, « *un tel système pourrait permettre de recueillir tout le bénéfice du* big data *tout en préservant les libertés individuelles* ».

Proposition n° 22 : instaurer un régime de responsabilité des responsables de traitement de données à deux versants :

– en amont de la collecte, créer une obligation d'étude d'impact sur la vie privée afin de réduire les risques pour les usagers,

– en aval, créer une obligation de signalement des irrégularités dans le traitement des données.

f) Explorer de nouvelles pistes pour réaffirmer la maîtrise par les individus de leurs données personnelles

Lors de son audition par votre mission d'information, M. Vinton Cerf, vice-président de Google, est revenu sur son affirmation souvent critiquée selon laquelle la vie privée serait une anomalie. Il a ainsi expliqué : « *lorsque j'ai employé ce terme, j'avais en tête l'absence de vie privée que j'ai connue il y a cinquante ans dans mon petit village. Aucun des 3 000 habitants n'ayant le téléphone, le chef du bureau de poste, qui composait les numéros avant de vous passer la communication savait qui téléphonait à qui, comme il savait qui écrivait à qui. Chacun savait ce que les autres faisaient : je n'avais pas le sentiment d'avoir vraiment une vie privée. Dans une grande ville, l'environnement plus anonyme rend possible la notion de vie privée. Or cet anonymat est mis à mal par l'Internet et ses multiples interconnexions. La notion de vie privée, à laquelle j'espère que nous ne renoncerons pas, est sans doute à redéfinir au regard de ce nouveau contexte.* »

De fait, nombre de personnes entendues ont mis en avant le fait que la notion de vie privée tendait à disparaître sur l'Internet, soit pour contester le principe même d'un régime juridique de protection des données personnelles, soit au contraire pour inviter le législateur à défendre les personnes contre elles-mêmes. Le dévoilement de leur intimité par les individus sur les réseaux sociaux serait le signe de ce désintérêt pour la notion même de vie privée. Lors de son audition, M. Laurent Cytermann a fortement nuancé cette affirmation et renvoyé votre mission d'information aux travaux du sociologue Antonio Casilli.

Analysant les comportements sur les réseaux sociaux, tout particulièrement Facebook, M. Antonio Casilli conclut que « *trop souvent les analystes et les commentateurs ont pris pour une renonciation intégrale à la* privacy *ce qui en réalité n'est que* l'actuation de formes de dévoilement stratégique d'informations personnelles à des fins de gestion du capital social en ligne ». Il démontre ainsi au fil de son étude que « *le dévoilement de soi apparaît de plus en plus lié à la création de lien social en ligne, s'intégrant dans de véritables stratégies d'usage finalisées à la capacitation personnelle, professionnelle, culturelle ou politique* ». S'inscrivant en faux avec la dichotomie tranchée opposant intime et « extime », il constate au contraire que « *les acteurs optimisent le dévoilement d'informations personnelles en se positionnant le long d'un continuum dont « ouverture » et « fermeture » sont les extrêmes* », opérant en quelques sortes des allers retours le long de ce continuum en fonction des réactions : « *dans la mesure où les données ne sont pas sensibles* par leur nature*, mais selon leur pertinence par rapport à un milieu social de choix, le respect de la vie privée revient principalement à vérifier l'adaptation entre l'information dévoilée, l'intention stratégique de son locuteur et le contexte de son dévoilement* ». Constatant donc que « *le dévoilement va de pair avec l'adaptation progressive aux signaux venant de l'environnement social* », M. Casilli en déduit le concept de « *privacy* négociée ». [1]

Ce n'est donc pas à la « fin de la vie privée » à laquelle on assiste, mais à une évolution de celle-ci, passée du « droit à être laissé en paix » selon l'expression du juge à la Cour suprême américaine Louis Brandeis, au droit pour l'individu de « *décider en principe lui-même quand et dans quelles limites les éléments de sa vie privée sont dévoilés* », conformément à la jurisprudence de la Cour constitutionnelle de Karlsruhe qui élaborait de la sorte un **« droit à l'autodétermination informationnelle »**. **Il en découle une évolution non tant des principes du droit que de sa mise en œuvre afin que chacun retrouve la maîtrise de ses données personnelles**. Selon quelles modalités ?

On a vu précédemment que la propriété de ses données personnelles ne répondait pas véritablement aux enjeux à l'œuvre ici. Mme Valérie Peugeot propose quant à elle de décourager l'usage des données pratiqué par les grandes plateformes de l'Internet sous couvert d'une fausse gratuité, au profit du rétablissement d'une économie « servicielle », dans laquelle **l'utilisateur conserve le contrôle sur les données qu'il a coproduites**. Elle a ainsi exposé à votre

[1] *Antonio A. Casilli,* Contre l'hypothèse de la « fin de la vie privée », La négociation de la *privacy* dans les médias sociaux*, Revue française des sciences de l'information et de la communication, 2013.*

mission d'information le projet *vendor relationship management* sur lequel elle travaille avec la Fondation Internet nouvelle génération (Fing) et un ensemble d'entreprises : « *les données de 300 clients volontaires sont stockées sur un* cloud *personnel, chacun d'entre eux en ayant la maîtrise. Chaque individu peut ainsi renseigner son profil beaucoup plus précisément, et c'est lui qui choisit les entreprises qui y auront accès. Le jour où il recherche une machine à laver, au lieu que sa requête lui renvoie des myriades de publicités, il ne reçoit que des offres adaptées*. »

M. Viktor Mayer-Schönberger nous invitait également à « *changer notre approche de la vie privée, passer d'une logique de protection à une logique de participation. La question n'est pas tant de participer ou non à Internet, mais comment y participer. Certains utilisateurs savent exercer leur droit à la vie privée eux-mêmes, mais pour la plupart d'entre eux, c'est trop compliqué. Regardez donc les paramètres de protection de la vie privée sur Facebook ! Comme dans d'autres domaines comme la sécurité alimentaire ou routière, le rôle des pouvoirs publics est de prendre des mesures pour obliger à simplifier ces paramétrages.* »

L'une comme l'autre de ces propositions mettent ainsi en avant l'importance de l'éducation au numérique des utilisateurs de l'Internet (*cf. infra*).

Ces propositions qui visent à rendre à l'internaute la maîtrise de ses données ramènent également au premier plan **la question récurrente du « droit à l'oubli »**. Selon M. Viktor Mayer-Schönberger, le « droit à l'oubli » n'a rien de nouveau, la proposition de règlement européen ne faisant que rebaptiser ce droit ; toutefois **son effectivité passerait probablement davantage par sa mise en œuvre par les juges que par de nouvelles normes**. L'arrêt de la Cour de justice de l'Union européenne *Google Spain* du 13 mai 2014 lui donne raison. Par cet arrêt, la Cour a en effet jugé que « *même un traitement initialement licite de données exactes peut devenir, avec le temps, incompatible avec cette directive lorsque ces données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées* ». Il s'ensuit que toute personne a le droit d'obtenir rectification, effacement ou verrouillage des données dont le traitement n'est pas conforme à la directive. Cette affaire a par ailleurs fait la démonstration que davantage qu'un droit à la suppression d'informations même exactes et licites, le « droit à l'oubli » prend la forme d'un droit à la désindexation ou au déréférencement de l'information par les moteurs de recherche : si la Cour européenne, répondant à une question préjudicielle, a jugé que le moteur de recherche avait une obligation de déréférencement, l'autorité de protection des données personnelles espagnole, l'AEPD, avait au préalable écarté les griefs du requérant à l'encontre du journal La Vanguardia, estimant que « *la publication par cette dernière des informations en cause était légalement justifiée étant donné qu'elle avait eu lieu sur ordre du ministère du Travail et des Affaires sociales et avait eu pour but de conférer une publicité maximale à la vente publique afin de réunir le plus grand nombre d'enchérisseurs* » Cela confirme **le nécessaire arbitrage, sous le contrôle du juge, entre droit à la vie privée d'une part, et droit à la mémoire et liberté d'expression et de communication d'autre part**.

Si à l'issue de ces développements, tant la nécessité d'une protection des données personnelles que la validité de l'approche juridique européenne en la matière ne sont plus à démontrer, reste à évoquer les conditions d'efficacité et d'effectivité de la norme de droit.

Comme la Cour de justice de l'Union européenne l'a rappelé dans sa décision du 8 avril 2014 invalidant la directive « *data retention* », **l'exigence de précision de la norme est d'autant plus impérative quand la norme touche aux données personnelles**.

Par ailleurs, le temps du politique et du droit n'étant pas celui de la technologie et de l'innovation, **il importe que le droit s'en tienne à l'énonciation de principes sans entrer dans le détail technique au risque de l'obsolescence de la norme juridique**. Tel est le sens de la mise en garde formulée par Mme Céline Castets-Renard, professeur à l'université Toulouse I Capitole, co-directrice du master 2 « droit et informatique », à votre mission d'information : *« oui, apporter une réponse juridique est essentiel, mais il faudra veiller à ne pas trop l'ancrer dans la technique, qui évolue très vite. Ne reproduisons pas l'erreur de la loi Hadopi, qui s'est trop focalisée, en matière de contrefaçon, sur un type de technologie. »*

Si la proposition de règlement européen n'apporte pas toutes les réponses au défi lancé au régime juridique européen par les derniers développements de l'Internet, certaines de ses dispositions constituent assurément des avancées. C'est pourquoi votre mission d'information appelle à une adoption rapide de ce texte, condition *sine qua non* d'une promotion de l'approche européenne de la protection des données personnelles à l'international.

3. Promouvoir cette approche à l'international

« *Sur le plan juridique, le temps est aux grandes manœuvres. On assiste à une concurrence entre les grandes régions juridiques ; la question se pose de savoir laquelle offrira l'espace le plus adapté à l'économie de demain, fondée sur le numérique et les données.* »

C'est ainsi que Mme Isabelle Falque-Pierrotin brossait devant votre mission d'information le tableau de la guerre juridique que se livrent actuellement les différentes puissances au niveau international. Pour elle, « *sous l'angle de l'innovation technologique et industrielle, l'Europe dispose, à travers la proposition de règlement, d'une arme juridique utile vis-à-vis des grands acteurs internationaux, ouvrant ainsi la faculté d'orienter la gouvernance juridique de la donnée selon notre propre schéma, sans avoir à subir celui des autres puissances* ».

Ces enjeux sont d'autant plus perceptibles que l'on se penche sur la question des transferts de données personnelles en dehors de l'Union européenne. En effet, si, on l'a vu, le respect du droit européen en la matière sur le territoire même de l'Europe est bravé, les données personnelles des Européens sont d'autant plus exposées et les risques d'atteinte à leur vie privée d'autant plus grands lorsque ces données quittent le territoire de l'Union. C'est pourquoi la

directive de 1995 et, à l'avenir, le règlement posent le **principe de la soumission de tout transfert de données à caractère personnel vers un pays tiers à la condition que ce dernier offre un niveau de protection des données personnelles adéquat**. La reconnaissance d'un « niveau de protection adéquat » relève de la Commission européenne. À ce jour, elle a reconnu comme assurant un niveau de protection adéquat l'Andorre, l'Argentine, l'Australie, le Canada, les Îles Féroé, Guernesey, Israël, Jersey, l'Île de Man, la Nouvelle-Zélande, la Suisse, l'Uruguay. Toutefois, étant donné l'importance des échanges commerciaux avec les États-Unis, et bien que ceux-ci ne puissent offrir un niveau de protection adéquat du fait de l'absence de législation nationale de protection des données personnelles, la Commission européenne a également reconnu comme adéquate la protection assurée par les États-Unis dans le cadre du *Safe Harbor*, également appelé « Sphère de sécurité », par une décision sectorielle.

a) La protection des données personnelles des citoyens de l'Union européenne dans les relations transatlantiques

La question de la protection des données personnelles est en effet l'un des points les plus épineux des relations entre l'Union européenne et son partenaire américain. Bien que, contrairement aux idées reçues, la notion de vie privée ne soit pas étrangère au monde anglo-saxon, il demeure que la manière de concevoir la protection de celle-ci diffère de part et d'autre de l'Atlantique. À ces considérations s'ajoute la défiance des Européens envers leurs alliés à la suite des révélations de l'affaire *Prism* et des doutes émis par les institutions européennes sur le sérieux avec lequel le partenaire américain a rempli ses engagements dans le cadre du *Safe Harbor*.

Le *Safe Harbor*

Après l'entrée en vigueur de la directive 95/46/CE le 25 octobre 1998, la Commission européenne et le Ministère du commerce américain ont entamé des discussions pour convenir de **sept** principes **de protection de la vie privée**. Cet ensemble de principes, **les « *Safe Harbor Privacy Principles* », publiés par le Ministère du commerce** le 21 juillet 2000, reprend pour l'essentiel ceux énoncés dans la directive :

– information des personnes dont les données sont collectées,

– faculté pour la personne concernée de s'opposer à un transfert ou à un usage de ses données pour des finalités différentes de celles pour laquelle elle a initialement consenti, son consentement exprès étant requis dans le cas de données sensibles,

– soumission du transfert à une tierce partie à la condition que celle-ci offre un niveau de protection adéquat,

– droit d'accès et de rectification des données,

– sécurité des données,

– intégrité des données,

– contrôle de l'effectivité de la mise en œuvre de ces principes notamment par l'instauration de mécanismes de recours pour les personnes concernées.

La Commission européenne a jugé que le *Safe Harbor* offrait un niveau de protection adéquat par la décision 2000/520/CE du 26 juillet 2000, en dépit des critiques soulevées par le « G 29 » et le Parlement européen.

Pour adhérer au *Safe Harbor* et être en mesure de recevoir des flux de données personnelles en provenance des États membres de l'Union européenne, une entreprise américaine doit, d'une part, stipuler dans sa politique de protection de la vie privée rendue publique qu'elle adhère aux principes du *Safe Harbor* et s'y conformer effectivement, et, d'autre part, certifier annuellement au Ministère du commerce qu'elle est en conformité avec ces principes. Le dispositif du *Safe Harbor* repose donc essentiellement sur un **mécanisme d'auto-certification**.

Le contrôle du respect par les entreprises des principes du *Safe Harbor* réside principalement en la mise en place de voies de recours. À cet effet, le *Safe Harbor* a instauré un **système de règlement extrajudiciaire des litiges** par un tiers indépendant, dont les modalités de mise en œuvre sont laissées au libre choix des entreprises. Celles-ci peuvent en effet opter :

– soit pour l'adhésion à des instances ou organismes de recours indépendants ayant déclaré publiquement leur compétence pour connaître des plaintes déposées par des particuliers pour manquement aux principes du *Safe Harbor* tels *TRUSTe* ou l'*International Centre for Dispute Resolution/American Arbitration Association*,

– soit s'engager à coopérer avec le panel de l'Union européenne sur la protection des données, entité composée de représentant de différentes autorités de protection des données personnelles européennes. Cette seconde option est obligatoire lorsque l'entreprise traite de données personnelles dans le cadre d'une relation de travail à des fins de gestion de ressources humaines. 53 % des entreprises ont désigné ce panel pour le règlement de leurs litiges[1].

Dans toutes les hypothèses, **en cas de manquement à leurs obligations, les entreprises tombent sous le coup du droit commercial américain**. À cet égard, elles sont placées sous la

[1] Cf. *la communication de la Commission au Parlement européen et au Conseil relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire, COM(2013)847 final, du 27 novembre 2013.*

juridiction de la Commission fédérale du commerce (*Federal Trade Commission*) **ou du Ministère des transports** pour les entreprises du secteur aérien. Les pouvoirs que détient la Commission fédérale du commerce en matière de protection de la vie privée résultent de la section 5 du *Federal Trade Commission Act* qui déclare illégales les « *manœuvres et pratiques déloyales ou frauduleuses dans le domaine du commerce* ». Le *Safe Harbor* fonctionne donc sur le principe suivant : dès lors qu'une entreprise aura certifié adhérer au *Safe Harbor* et mettre en œuvre ses principes de protection de la vie privée, elle ne pourra manquer à cet engagement sous peine d'être reconnue coupable de fausse déclaration, donc de « pratique frauduleuse ». Toutefois **la compétence de la Commission fédérale du commerce ne couvre que les manœuvres et pratiques déloyales et frauduleuses dans le domaine du commerce**, elle ne s'étend donc pas à la collecte et l'utilisation d'informations personnelles à des fins non commerciales. En outre, certains secteurs d'activités échappent à la compétence de la Commission tels les sociétés de télécommunications.

Cependant, en application de l'article 3 de la décision 2000/520/CE, **les autorités de protection peuvent suspendre les flux de données vers une organisation adhérant au *Safe Harbor*** dans deux hypothèses :

– si la Commission fédérale du commerce, le Ministère des transports ou une instance indépendante de recours a constaté que cette organisation viole les principes du *Safe Harbor*,

– ou dans le cas « *où il est fort probable que les principes sont violés ; où il y a tout lieu de croire que l'instance d'application concernée ne prend pas ou ne prendra pas en temps voulu les mesures qui s'imposent en vue de régler l'affaire en question ; où la poursuite du transfert ferait courir aux personnes concernées un risque imminent de subir des dommages graves ; et où les autorités compétentes des États membres se sont raisonnablement efforcées, compte tenu des circonstances, d'avertir l'organisation et de lui donner la possibilité de répondre.* »

Le *Safe Harbor* a fait l'objet de deux rapports d'évaluation par la Commission européenne en date des 13 février 2002 et 20 octobre 2004. Cependant, à la suite de la révélation de l'ampleur de la surveillance opérée par les services de renseignement américains, la pertinence de la décision de la Commission de 2000 a été fortement remise en question. Ce questionnement est d'autant plus important que les citoyens de l'Union européenne ne bénéficient pas des mêmes droits ni des mêmes garanties procédurales que les Américains dans le cadre des programmes de surveillance américains *(cf. supra)*.

Par deux communications du 27 novembre 2013[1], la Commission européenne a pris acte des lacunes constatées du *Safe Harbor* et du fait que certaines autorités de protection des données nationales, à l'instar d'autorités allemandes, considéraient d'ores et déjà l'opportunité de suspendre certains flux de transferts de données. Écartant les options de maintien du *statu quo* et de suspension/abrogation de sa décision, la Commission européenne a proposé de renforcer le *Safe Harbor* selon trois axes :

[1] Cf. *la communication de la Commission au Parlement européen et au Conseil :* « Rétablir la confiance dans les flux de données entre l'union européenne et les États-Unis d'Amérique » *(COM(2013)846 final) et la communication de la Commission au Parlement européen et au Conseil relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire (COM(2013)847 final), du 27 novembre 2013.*

– en améliorant la transparence des politiques de ces entreprises en matière de protection de la vie privée ;

– en invitant les autorités américaines à mieux contrôler et surveiller le respect par les entreprises des principes auxquels elles ont déclaré adhérer ;

– en garantissant aux citoyens de l'Union européenne l'accès à des mécanismes de règlement des litiges.

Sur ce dernier point, la Commission a en effet pu constater le faible nombre de recours. À titre d'illustration, le panel de l'Union européenne sur la protection des données n'a été jusqu'à présent saisi que de quatre plaintes. La Commission fédérale du commerce n'a poursuivi que dix entreprises pour violation du *Safe Harbor* ; elle n'a en outre jamais été saisie par un organisme de règlement extrajudiciaire de litiges.

Pour sa part, le Parlement européen a réagi par l'adoption, le 12 mars 2014, d'une résolution[1] par laquelle il invite la Commission à présenter des mesures prévoyant la suspension immédiate de sa décision de 2000 et les États-Unis à présenter une proposition de nouveau cadre juridique. Il y invite également les autorités nationales de protection des données à faire usage de leur faculté de suspendre tout flux de données vers des organisations ayant adhéré au *Safe Harbor* et n'offrant d'autres garanties. Il convient de se souvenir qu'au moment de l'adoption de la décision de 2000, le Parlement européen déplorait déjà que le *Safe Harbor* ne reconnaisse pas le « *droit de tout individu à introduire une plainte devant un organisme public indépendant chargé d'examiner les recours relatifs à toute violation présumée des principes* »[2].

Lors de sa dernière réunion plénière des 9 et 10 avril 2014, le « G 29 » a quant à lui estimé que, « *si le processus de révision en cours entre la Commission et les autorités américaines ne conna[issai]t pas une issue positive, l'accord* Safe Harbor *devra[it] être suspendu* »[3]. Cela rejoint la position indiquée par Mme Isabelle Falque-Pierrotin, par ailleurs présidente du « G 29 », lors de son audition par votre mission d'information : « *la menace de suspendre le* Safe Harbor *serait une arme de dissuasion extrêmement puissante si elle était brandie par l'Europe* ».

Certaines des treize recommandations faites par la Commission européenne ne semblent pas poser de difficultés aux États-Unis, telles celle préconisant que les entreprises certifiées offrent aux consommateurs un lien Internet vers leur politique de confidentialité ou celle demandant au gouvernement américain de consacrer davantage de ressources à l'évaluation des

---

[1] *Résolution sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures (2013/2188(INI)).*

[2] Cf. *la résolution A5-0177/2000 du Parlement européen sur le projet de décision de la Commission relative à la pertinence des niveaux de protection fournis par les principes de la sphère de sécurité et les questions souvent posées y afférentes, publiées par le ministère du commerce des États-Unis, C5-0280/2000 / 2000/2144(COS).*

[3] Cf. *le site Internet de la Commission nationale de l'informatique et des libertés.*

demandes de mises en conformité. D'autres paraissent en revanche plus délicats, en particulier l'obligation de publier les conditions de protection de la vie privée figurant dans tout contrat conclu entre les entreprises auto-certifiées et leurs sous-traitants, par exemple pour les services d'informatique en nuage, dont les États-Unis estiment qu'il s'agit d'une exigence lourde qui ne bénéficierait pas aux consommateurs.[1] Surtout, les autorités américaines ne semblent pas disposées à donner satisfaction aux Européens quant aux possibilités pour ces derniers de déposer un recours et d'obtenir réparation en cas de mauvaise utilisation de leurs données, selon la commissaire Viviane Reding.

Le 18 juin 2014, la Cour suprême irlandaise a renvoyé à la Cour de justice de l'Union européenne la question de la légalité du transfert de données personnelles opéré dans le cadre du *Safe Harbor* au regard du droit européen. Cette question préjudicielle s'inscrit dans le cadre d'un litige opposant un citoyen autrichien à Facebook : après avoir demandé l'accès à ses données personnelles auprès de la société américaine et obtenu communication d'un DVD contenant plus de 1 200 pages d'informations sur son compte, M. Max Schrems a saisi l'autorité de protection des données personnelles irlandaise d'une vingtaine de plaintes. C'est la première fois que la question de la conformité du *Safe Harbor* au droit de l'Union est ainsi posée.

Dans l'attente de la décision de la Cour de justice de l'Union européenne, votre mission d'information estime pour sa part indispensable de renégocier le *Safe Harbor* et se rallie à l'opinion du « G 29 » selon laquelle il serait nécessaire de le suspendre dans l'hypothèse où les autorités européennes ne seraient pas entendues. Peut-être une suspension des flux de données personnelles vers certaines entreprises dont il est avéré qu'elles n'ont pas respecté leurs engagements pourrait-elle renforcer la position européenne dans les négociations. Une piste de réflexion pourrait être de s'assurer de la mise en œuvre effective du *Safe Harbor* en en confiant le contrôle aux autorités européennes plutôt qu'aux autorités américaines, en une sorte de *Safe Harbor* « inversé ». En tout état de cause, votre mission d'information considère que la question des données personnelles doit être traitée indépendamment des négociations sur le Partenariat transatlantique de commerce et d'investissement, communément désigné « TTIP » (pour *Transatlantic Trade and Investment Partnership*) : touchant à la garantie de droits fondamentaux, elle ne saurait être regardée comme simple monnaie d'échange dans une négociation commerciale[2].

Proposition n° 23 : renégocier le *Safe Harbor* en se gardant la possibilité de le suspendre si les exigences des autorités européennes n'étaient pas entendues et tenir cette négociation distincte de celle du traité transatlantique.

En outre, votre mission d'information note avec satisfaction que, si la proposition de règlement entérine la faculté de la Commission européenne

[1] Cf. *Brian Beary, « UE/États-Unis : l'accord « Safe Harbour » remis à plat »*, Europolitics, *14 mai 2004.*
[2] Cf. infra.

d'apprécier le niveau de protection assuré par un territoire ou un secteur de traitement des données à l'intérieur d'un pays tiers – validant ainsi *a posteriori* le principe des décisions sectorielles adoptées par la Commission à l'instar de la décision portant sur le *Safe Harbor* –, **cette compétence est encadrée et les critères à prendre en compte par la Commission, précisés**. Y figure en particulier « *l'existence de droits effectifs et opposables, y compris un* ***droit de recours administratif et judiciaire effectif*** *des personnes concernées, notamment celles ayant leur résidence sur le territoire de l'Union et dont les données à caractère personnel sont transférées* ». À l'initiative de la Commission LIBE du Parlement européen, les décisions de la Commission européenne prendraient la forme d'actes délégués – non d'actes d'exécution – afin de ménager un droit d'opposition et de révocation au Parlement européen et au Conseil ; ces décisions seraient en outre prises après avis du Comité européen de la protection des données sur le caractère suffisant du niveau de protection.

Votre mission d'information soutient également l'introduction, à l'initiative de la Commission LIBE, de l'article 43 *bis* qui encadre le transfert ou la divulgation de données à caractère personnel à la demande des autorités administratives ou juridictionnelles de pays tiers en les soumettant à l'accord de l'autorité de protection européenne compétente. Cette « clause anti-FISA » participe de l'instauration du « *bouclier juridique* » appelé de ses vœux par Mme Isabelle Falque-Pierrotin, qui expliquait lors de son audition l'importance qu'une telle disposition aurait dans la conduite des négociations transatlantiques : « *dans notre cadre juridique européen, l'article additionnel introduit par le Parlement européen permettant de résister à la demande d'accès aux données de citoyens européens par des États étrangers permet de faire avancer l'idée d'accords intergouvernementaux sur la coopération en matière de renseignements et donnerait une architecture juridique donnant un cadre aux échanges d'informations. Ensuite, la question de savoir si ce cadre sera respecté est de nature politique. Mais nous aurions au moins établi une architecture symbolique pour sécuriser les échanges de nos grandes entreprises européennes face aux pressions de la législation américaine. Il faut rehausser l'exigence juridique européenne pour rétablir l'équilibre. À partir du moment où nous aurons provoqué un conflit de loi, nous pourrons alors entamer une discussion plus équilibrée avec les Américains*. »

L'adoption de cet article 43 *bis* renforcerait donc la position de l'Union européenne dans ses négociations avec les États-Unis, lui permettant de revenir sur l'absence de droit au recours des citoyens de l'Union européenne devant les juridictions américaines. À cet égard, votre mission d'information a pris connaissance avec intérêt de certaines des recommandations faites au Président Obama par le groupe de travail sur le renseignement et les technologies de communication[1]. La mise en œuvre en particulier de la recommandation n° 14, qui préconise d'appliquer sans distinction le *Privacy Act* de 1974, donnant accès à tous les individus aux informations les concernant avec droit de rectification, serait un signal attendu et positif du gouvernement des États-Unis à l'adresse de ses alliés européens.

[1] Cf. Liberty and Security in a Changing World, Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies, *12 décembre 2013.*

Proposition n° 24 : adopter la disposition introduite par le Parlement européen dans la proposition de règlement encadrant le transfert ou la divulgation de données personnelles à la demande des autorités administratives ou juridictionnelles de pays tiers.

b) La Convention 108, outil le plus efficace de promotion de l'approche européenne en matière de protection des données personnelles

Si la négociation d'accords bilatéraux avec nos partenaires américains peut fortement contribuer à sécuriser les données personnelles des citoyens européens lors de leurs transferts vers les États-Unis, une approche plus globale de promotion du modèle européen de protection des données personnelles serait probablement plus profitable à long terme. Cela permettrait en effet non seulement de faire l'économie de tels accords bilatéraux, mais également de **diffuser la « culture Informatique et libertés » de manière à en faire bénéficier davantage de populations**.

Pour ce faire, ainsi que l'indiquait Mme Céline Castets-Renard, la **Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, dite « Convention 108 », pourrait s'avérer l'outil le plus pertinent**. Cette convention est en effet à ce jour le **seul instrument international juridiquement contraignant adopté dans le domaine de la protection des données personnelles**. Par son article 4, elle impose en effet à chaque État partie à la convention de prendre, « *dans son droit interne, les mesures nécessaires pour donner effet aux principes de base pour la protection des données énoncés [par la convention]* ».

En outre, **la convention couvre un champ d'application territorial plus large que le seul continent européen dans la mesure où son adhésion est ouverte à des États non membres du Conseil de l'Europe** par son article 23. Ainsi, l'Uruguay a ratifié la convention, portant le nombre des parties à quarante-six États, dont tous les États membres du Conseil de l'Europe à l'exception de Saint-Marin et de la Turquie, qui l'a signée mais non encore ratifiée. Le Maroc a par ailleurs demandé son adhésion. En revanche, seuls trente États ont ratifié le protocole additionnel de 2001 concernant les autorités de contrôle et les flux transfrontaliers de données, qui impose aux parties contractantes la mise en place d'autorités de contrôle indépendantes.

Ouverte à la signature le 28 janvier 1981 et entrée en vigueur le 1er octobre 1985, **la convention puise à la même source d'inspiration que le droit de l'Union européenne et repose sur les mêmes principes** de finalité, de proportionnalité, de sécurité et de droit d'accès et de rectification ; elle s'applique au secteur privé comme au secteur public. Depuis 2010, le Conseil de l'Europe a engagé un processus de révision de la convention afin de l'adapter aux changements technologiques et de renforcer le dispositif de suivi. Les travaux de révision ont été conduits en partenariat avec l'Union européenne, représentée par la Commission, puisque celle-ci commençait à la même période les travaux préparatoires à la révision du cadre juridique de l'Union européenne en matière

de protection des données. Cela explique la très grande proximité entre le texte de la convention révisée, adopté par le Conseil de l'Europe lors de sa séance plénière des 27 et 29 novembre 2013, et la proposition de règlement européen.

Si tous les États membres de l'Union européenne sont parties à la Convention 108, tel n'est pas le cas de l'Union européenne elle-même qui ne bénéficie que d'un statut d'observateur. L'adhésion de l'Union européenne à la convention est en effet en discussion depuis la fin des années 1990, mais celle-ci achoppe sur le refus de certains États parties d'accepter les amendements permettant l'adhésion de l'Union, en raison en particulier des exigences européennes relatives aux transferts de données internationaux. À ce jour, seuls trente-trois États parties ont accepté lesdits amendements.

Cette situation n'a cependant pas empêché l'Union européenne, à la suite des révélations d'Edward Snowden, de demander aux États-Unis d'adhérer à la convention. Cela permettrait en effet d'envisager la reconnaissance des États-Unis comme pays offrant un niveau de protection adéquat, rendant en particulier inutile la renégociation du *Safe Harbor*. Il va de soi toutefois que la promotion par l'Union européenne de la Convention 108 aurait d'autant plus de poids que celle-ci serait elle-même partie à la convention.

Proposition n° 25 : poursuivre les négociations en vue de l'adhésion de l'Union européenne à la Convention 108 afin d'asseoir la légitimité de l'Union à demander aux États-Unis d'y adhérer également.

c) Le droit privé en soutien à la promotion des valeurs européennes en matière de protection des données personnelles

À côté de ces outils de droit international public, l'Union européenne a développé d'autres instruments pour permettre d'assouplir le principe de l'interdiction de transfert de données à caractère personnel vers des pays tiers n'assurant pas un « niveau de protection adéquat », en s'appuyant sur le droit international privé.

La directive de 1995 prévoit ainsi que peut être autorisé un transfert ou un ensemble de transferts vers un pays tiers n'assurant pas un niveau de protection adéquat « *lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants ; ces garanties peuvent notamment résulter de clauses contractuelles appropriées* ». Les « **clauses contractuelles types** » sont des **modèles de contrat de transfert de données personnelles** entre deux responsables de traitement ou entre un responsable de traitement et un sous-traitant. Elles précisent en particulier la responsabilité de chacun des cocontractants (solidarité ou responsabilité renforcée de l'exportateur des données), les modalités de règlement des litiges, celles d'exercice de leurs droits d'accès par les personnes concernées et la coopération avec les autorités de protection des données. Si le règlement conserve le principe des clauses contractuelles types, le Parlement européen a supprimé la possibilité pour la

Commission européenne d'adopter ces clauses types, réservant cette faculté aux autorités de contrôle.

Face à la demande des entreprises multinationales de simplification des démarches pour procéder à des transferts internationaux de données personnelles entre leurs différentes entités, les autorités de protection des données ont avalisé l'élaboration de codes de conduite internes, désignés sous l'appellation « **règles d'entreprise contraignantes** » ou « ***Binding Corporate Rules*** » (**BCR**). Ces règles portant sur les transferts internationaux de données sont adoptées par la maison mère et doivent être obligatoirement appliquées par toutes les filiales et tous les employés du groupe. Cela implique non seulement l'insertion de clauses dans les contrats de travail et conventions collectives, et de sanctions disciplinaires en cas d'infraction, mais également la mise en place de formations internes et de mécanismes de contrôle pour s'assurer du respect du code de conduite – audit interne, cellule de gestion des plaintes.

Concrètement, l'élaboration de ces BCR s'établit sous le contrôle d'une autorité européenne de protection des données personnelles « chef de file » qui s'assure de la conformité à la directive des règles mises en place et prend en charge la procédure de coopération avec les autres autorités européennes auprès desquelles seront déposées les demandes d'autorisation de transfert. Afin d'accélérer ce processus, certaines autorités de protection des données de l'Espace économique européen (EEE) se sont engagées à mettre en œuvre une procédure de « reconnaissance mutuelle » : lorsqu'une autorité en reconnaissance mutuelle considère que des BCR apportent un niveau de protection suffisant, les autres autorités en reconnaissance mutuelle approuvent les BCR automatiquement. Au 9 août 2012, vingt et une autorités de protection avaient accepté cette procédure de « reconnaissance mutuelle »[1]. La proposition de règlement intègre dans le droit positif la pratique des « règles d'entreprise contraignantes » en les encadrant. Les ministres des États membres ont validé cette disposition lors du dernier Conseil JAI.

Par ailleurs, **la proposition de règlement confie à la Commission européenne et aux autorités de contrôle mandat pour élaborer des mécanismes de coopération internationaux** destinés à faciliter l'application de la législation relative à la protection des données à caractère personnel, et à améliorer l'assistance mutuelle avec les autorités des pays tiers. Cette nouvelle disposition vient légitimer les actions entreprises jusqu'à présent par les autorités européennes pour ouvrir des « chemins d'interopérabilité » entre les différents systèmes juridiques et promouvoir ainsi l'approche européenne en matière de protection des données personnelles.

[1] *Selon le site Internet de la CNIL, ces autorités sont celles des pays suivants : Allemagne, Autriche, Belgique, Bulgarie, Chypre, Espagne, Estonie, France, Grande-Bretagne, Irlande, Islande, Italie, Lettonie, Liechtenstein, Luxembourg, Malte, Norvège, Pays-Bas, République tchèque, Slovaquie, Slovénie.*

Un exemple d'interopérabilité :
le rapprochement des règles de l'Union européenne avec celles de l'APEC

Le Forum de coopération économique de la région Asie-Pacifique (APEC) regroupe vingt et un États, notamment les États-Unis, le Canada, le Japon, la Chine, la Russie et la Corée du Sud.

Dès 2004, l'APEC s'est doté de principes directeurs en matière de protection de la vie privée et des données personnelles, certains de ses membres ayant adopté des législations en la matière. À partir de 2011 cependant, l'APEC s'est attelé à l'élaboration de règles communes permettant d'encadrer les flux de données personnelles en son sein, proches des BCR : les *Cross-Border Privacy Rules* (CBPR).

Depuis 2013, le « G 29 » et l'APEC travaillent à un interfaçage entre leurs deux systèmes afin de permettre aux groupes internationaux d'adopter des règles internes conformes aux deux standards. Un référentiel listant les principes communs aux deux systèmes ainsi que ceux spécifiques à chacun a ainsi été mis au point et approuvé par chacune des parties les 27 et 28 février 2014.

Tant les « clauses contractuelles types » que les BCR peuvent ainsi permettre de remédier aux insuffisances du *Safe Harbor* dans la mesure où le contrôle des mesures mises en place par les entreprises est assuré par les autorités européennes, non par les autorités américaines. C'est pourquoi, dans l'hypothèse où la renégociation du *Safe Harbor* n'aboutirait pas, les autorités européennes pourraient proposer aux entreprises américaines qui le souhaitent de les aider à se doter de tels instruments.

C. CONSTRUIRE UNE STRATÉGIE INDUSTRIELLE EUROPÉENNE POUR MAÎTRISER NOS DONNÉES ET PORTER NOS VALEURS

« *Régulation appropriée […], mais aussi recherche de la masse critique : tels sont les deux enjeux en matière industrielle*. » Ce propos tenu par M. Vincent Champain, directeur des opérations de General Electric France, devant votre mission résume à lui seul les impératifs majeurs d'une stratégie industrielle européenne en matière de numérique.

Par **régulation appropriée**, il faut entendre un dispositif de protection des données qui **intègre pleinement la dimension économique du secteur du numérique**, et qui adapte donc sa méthodologie aux évolutions qu'impose le *big data*.

Votre mission recommande de **traiter les flux de données de façon réaliste et équilibrée**, à la fois comme un **enjeu fondamental en termes de protection des droits et libertés personnels**, mais aussi comme une **ressource dont l'accès est indispensable pour permettre à nos entreprises d'innover** en proposant des services adaptés et personnalisés, susceptibles de dégager de la valeur ajoutée.

Le deuxième impératif en matière industrielle consiste donc à **rechercher une échelle de développement plus vaste**, qui permette à nos entreprises de

dépasser leur « pré-carré » national et de bénéficier de l'ensemble du marché européen. Ainsi que l'a fait remarquer M. Vincent Champlain, « *l'Europe est performante en matière d'innovation […] mais elle n'a pas su rechercher la masse critique* ». Un tropisme européen nous porterait « *trop souvent à rechercher des solutions nationales […]. Ainsi, les pôles de compétitivité sont beaucoup plus petits en Europe qu'aux États-Unis ou au Japon, parce qu'ils sont disséminés dans de nombreux États membres. Nous manquons, de ce point de vue, d'une véritable stratégie industrielle à l'échelle européenne. Des pôles d'échelle européenne seraient, au reste, les interlocuteurs adéquats dans la recherche de l'équilibre entre protection des libertés publiques et capacité de développement de nos industries.* »

Cette recherche de la masse critique pourrait passer par différents vecteurs. Le premier d'entre eux serait la **mise au point de normes industrielles communes**, qui puissent éventuellement devenir des références mondiales dans un second temps, comme cela a été le cas pour la norme GSM en matière de téléphonie mobile.

Le second instrument qui permettrait de fédérer les compétences nationales dans l'Internet et, plus largement, le numérique, serait le **lancement de véritables initiatives industrielles communes**. Les réussites qu'ont constitué, dans les secteurs de l'aviation et de l'espace, Airbus et Arianespace, doivent servir d'**exemples** à cet égard, même si la comparaison du numérique avec Airbus est délicate, l'Internet ne présentant pas du tout les mêmes barrières à l'entrée que l'aéronautique. Ces deux succès industriels, où « *l'ambition a précédé l'organisation et l'a structurée* », montrent l'importance d'une **impulsion forte au niveau européen**. Ils révèlent également la nécessité d'une **réflexion se plaçant dès le départ au niveau mondial**, ce qui est le cas dans la communauté scientifique et chez certains industriels, mais « *ce qui n'est pas le cas des régulateurs, de l'administration, voire des parlementaires, qui en restent à une logique plus nationale* », poursuit M. Vincent Champain.

Par ailleurs, l'Europe dispose d'un atout sur lequel elle peut fonder et promouvoir des solutions industrielles communes : le respect de principes juridiques protecteurs pour les libertés individuelles, et la confiance que cela peut susciter chez les clients et acheteurs potentiels. Le **haut standard européen de protection des données doit servir de base à notre politique industrielle**. Ainsi que l'a rappelé M. Philippe Lemoine devant votre mission, l'affaire Snowden a suscité des inquiétudes réelles dans les milieux d'affaires, auxquelles les entreprises européennes sont en mesure de répondre. « *Les grands patrons soulignent combien il est important de créer la confiance – la loi informatique et libertés peut être, pour nous, un atout* », a-t-il souligné.

1. Catalyser l'industrie européenne du numérique autour d'une ambition affichée

La politique européenne en matière d'industrie du net a consisté, jusqu'à aujourd'hui, à créer et mettre en place un écosystème qui soit acceptable pour

l'ensemble de ses acteurs. À cette démarche, qui doit être poursuivie, doit s'en ajouter une nouvelle, consistant à soutenir nos entreprises sur les marchés extérieurs, comme le font nos principaux compétiteurs internationaux (États-Unis, Japon et Chine, notamment).

a) Définir une véritable politique industrielle transversale au service du numérique

La première priorité pour l'Europe et pour la France doit être de capitaliser sur les domaines dans lesquels elles occupent une place de *leader*. Ces champs d'activité sont bien plus nombreux et importants, dans le secteur du numérique, que ce que l'on peut croire.

- **À l'échelle nationale**

Le rapport de la commission « innovation 2030 » présidée par Mme Anne Lauvergeon[1] pointe les **forces de notre pays en matière d'innovation**. Cinquième puissance mondiale, la France se classe onzième en matière d'innovation. Elle bénéficie d'une population au niveau de formation élevé, d'une recherche publique de qualité, d'un tissu productif important et diversifié, d'un réseau d'infrastructures développé, d'incitations fiscales favorables à travers le crédit d'impôt recherche (CIR)…

De façon plus sectorielle, notre pays peut compter sur des **domaines d'excellence reconnus à l'échelle mondiale**. Ainsi que le mentionne très explicitement le rapport, la France abrite « *plusieurs sociétés de niveau international, notamment dans le domaine de l'Internet des objets (Withings, Sigfox, Parrot…) qui n'ont rien à envier à leurs concurrents, ou encore des sociétés comme Critéo dans le domaine du ciblage publicitaire, qui est l'un des champions mondiaux, avec une taille déjà très significative. Plusieurs grands groupes sont* leaders *de sous-segments (Dassault Systèmes, Gemalto, Ingenico, Morphosytèmes…)* ».

Ces succès interviennent dans une **économie qui a radicalement changé d'aspect**, étant passée d'un modèle planifié et centralisé à un **modèle réticulaire et décentré où l'initiative « part du bas »**. Ainsi que l'a expliqué M. Roberto di Cosmo, professeur d'informatique à l'Université Paris-VII, directeur de l'initiative pour la recherche et l'innovation sur le logiciel libre (IRILL), « *dans les industries plus anciennes […], le besoin d'investissement initial et de temps sont très importants, ce qui convient à une stratégie jacobine où l'on décide de concentrer les moyens sur une technologie donnée. Dans le domaine d'Internet, la barrière à l'entrée est très faible, et cette stratégie ne peut plus fonctionner.* » C'est donc la fluidité dans l'accès au réseau qui est la condition d'une innovation abondante et fructueuse.

Les pouvoirs publics doivent donc assurer le respect de cette liberté d'accès au réseau, en garantissant sa neutralité[2], mais aussi aller au-delà, en **adoptant une véritable politique industrielle**. « *Alors que l'État s'est engagé dans*

[1] Un principe et sept ambitions pour l'innovation, *rapport de la commission « innovation 2030 » présidée par Mme Anne Lauvergeon, octobre 2013.*

[2] Cf. supra.

un partenariat stratégique avec les industriels en matière de défense ou d'aéronautique, rien de tel dans le domaine du numérique », regrette à cet égard M. Loïc Rivière, vice-président du comité stratégique de la filière numérique (CSFN).

À cet égard, il nous faudra **rompre avec une tendance nationale à protéger d'anciens modèles économiques au détriment de nouveaux, plus innovants**, tendance qui nous place aujourd'hui en situation de dépendance numérique envers les États-Unis. Plusieurs exemples illustrent ce travers : notre réticence à adopter l'Internet, pourtant initié par des chercheurs français mais perçu comme un produit américain, par opposition au Minitel, dont le modèle économique centralisé était stable et bien maîtrisé ; la stigmatisation, par ailleurs, du téléchargement en pair-à-pair au profit de modes plus classiques de diffusion des contenus audiovisuels, alors que nous possédions des sociétés précurseurs en ce domaine, comme Azureus/Vuze, Wizzgo, Dailymotion et Deezer.

Bien que de nature différente, ces deux cas soulignent la reproduction d'une même erreur consistant à assurer la survie artificielle de technologies dépassées et à refuser de nouveaux modèles économiques en rupture. Dans le contexte globalisé que présente l'Internet aujourd'hui, **un tel repli sur notre « pré-carré » industriel n'est plus adapté**, tout service étant accessible depuis n'importe quel pays. Une attitude défensive se traduit, dans ce cas, par des pertes d'emploi et de recettes sur notre territoire, une grande difficulté à appréhender par la loi des services alors émis de l'étranger, une absence de garanties pour des données hébergées dans des pays tiers ou encore un risque de dépendance envers un quasi-monopole lorsque le marché est absorbé par une seule société basée à l'étranger.

Pour autant, notre pays n'a pas déserté le secteur de l'industrie, ni celui du numérique, et reste capable d'un certain volontarisme et d'une approche ouverte en la matière. L'annonce, au mois de septembre 2013, par le Président de la République, de la définition de **34 grands plans industriels** illustre ainsi la **détermination du Gouvernement** à soutenir les innovations françaises dans les secteurs d'avenir. Associant acteurs publics et entreprises, pilotés par un industriel ou, à défaut, par un pôle de compétitivité, ils doivent permettre de développer d'ici cinq à dix ans une offre de produits nationaux adaptée aux marchés les plus porteurs.

Le **numérique occupe une place de choix** dans ce « chantier industriel » mis en place par le Gouvernement, puisque **16 des 34 plans** – soit quasiment la moitié – sont en rapport direct avec ce secteur : *big data*, *cloud*, objets connectés, « réalité augmentée », logiciels et systèmes embarqués, services sans contact, e-éducation, hôpital numérique, cybersécurité, nanoélectronique, robotique, supercalculateurs, véhicule à pilotage automatique, réseaux électriques intelligents et souveraineté des télécoms.

Mais au-delà de cette logique relativement sectorielle, il importe de **poursuivre des politiques transversales en faveur de l'économie numérique**. En effet, comme le note M. Loïc Rivière, « *tout inviterait à considérer qu'une stratégie de*

filière, qu'une politique industrielle dédiée au numérique n'aurait pas de sens ». La notion même de « filière numérique » ne lui paraît d'ailleurs « *pas très opératoire dans le contexte de transformation numérique globale, insuffisant, en tout cas, pour définir des politiques publiques de ré-industrialisation* ».

Ces politiques transversales passent nécessairement par le **soutien à la R&D et à l'innovation**. La commission « innovation 2030 » propose à cet égard de « *reconnaître, au plus haut niveau, l'existence d'un principe d'innovation, équilibrant le principe de précaution, yin et yang du progrès des sociétés* ». Il se traduirait notamment par « *l'acceptation du risque dans les décisions pour aboutir à des choix pondérés mais aussi par une évaluation régulière* » qu'elle préconise de confier à l'Office parlementaire d'évaluation des choix scientifiques et technologiques (OPECST).

On notera à ce sujet que le Sénat a adopté, le 27 mai dernier, une proposition de loi de notre collègue Jean Bizet visant à modifier la Charte de l'environnement pour exprimer plus clairement que le principe de précaution est aussi un principe d'innovation, sa bonne application reposant en effet sur le développement des connaissances scientifiques, la diffusion des résultats de la recherche, la transparence et le débat[1].

Il conviendrait également de **conforter le dispositif français d'appui à l'export**. Selon le rapport de la commission « innovation 2030 » précité, « *le marché intérieur français, souvent mature et d'une croissance modeste, est de taille insuffisante pour amortir des investissements importants* », même à l'échelle des PME et ETI. Face à ces limites, « *les entreprises doivent donc impérativement « jouer mondial » pour grossir vite et avoir une chance de devenir des* leaders ». Mme Gabrielle Gauthey, vice-présidente d'Alcatel-Lucent, présidente de la commission innovation du Mouvement des entreprises de France (Medef), a ainsi dit prôner « *depuis des années une réforme du système français de soutien à l'exportation, […] bien trop centré sur l'industrie, et pas assez sur la recherche et le développement* ». Les Allemands, les Belges ou les Suédois, a-t-elle indiqué, prennent mieux en compte la contribution à la balance commerciale, à l'emploi, ou encore la R&D. L'Inspection des finances conduit toutefois une mission sur le sujet, dont des améliorations sont attendues.

Proposition n° 26 : réorienter le dispositif national de soutien à l'export sur le soutien à la R&D et à l'innovation pour les PME et ETI du secteur numérique.

- **À l'échelle européenne**

Le retard de l'Europe dans les secteurs de la *high tech*, exposé par ailleurs[2], plonge ses racines dans « ***l'absence, depuis quinze ans, de politique industrielle*** », ainsi qu'a pu l'exposer à la mission M. Hervé Collignon, co-auteur d'un rapport d'A.T. Kearney sur la place des industries européennes dans les TIC[3] : « *Les Chinois, les Coréens et les Américains bâtissent des plans stratégiques à 10*

[1] *Proposition de loi n° 183 (2013-2014) de M. Jean Bizet visant à modifier la Charte de l'environnement pour préciser la portée du principe de précaution.*

[2] *Voir* supra.

[3] *Voir* supra.

ou 15 ans, avec une stratégie industrielle nationale assumée. Ce n'est pas forcément le cas en Europe. »

L'analyse du CNNum, livrée à votre mission par son secrétaire général, M. Jean-Baptiste Soufron, a été identique : « *On distingue mal ce que sont les priorités de l'Europe. Les grands acteurs européens du numérique ont eu du mal à survivre ces cinq dernières années, même s'il en reste quelques-uns comme Deezer ou Spotify, qui va vers une entrée en bourse, Criteo, cotée au Nasdaq. […]* ***Ce qui manque cependant, c'est une vision stratégique à moyen et long terme****, pour définir quelles entreprises européennes pourraient travailler ensemble.* »

Dans son rapport intitulé *L'Union européenne, colonie du monde numérique*, votre rapporteure avait longuement souligné ce « **défaut de stratégie politique » de l'Europe en matière d'industrie numérique**. Elle avait certes relevé certains éléments positifs, comme la création en 2004 d'un poste de commissaire européen en charge du numérique ; la communication sur la politique industrielle publiée en octobre 2012 à l'initiative du commissaire Tajani, en charge de l'industrie, évoquant publiquement la nécessité d'un projet industriel en matière numérique ; ou encore les inflexions positives de la commissaire Mme Neelie Kroes, illustrées par la communication de la Commission européenne du 18 décembre 2012 qui actualise la stratégie numérique de l'Union.

Malgré cela, votre rapporteure déplorait que « *l'impulsion reste en fait difficile à donner pour concrétiser les ambitions affichées par l'Union européenne dans sa stratégie numérique* », pointant notamment **certaines limites institutionnelles**, telles qu'un mauvais fonctionnement du mécanisme de coordination interne à la Commission, ou encore la persistance de cloisonnements en son sein, « *empêchant d'appréhender les enjeux numériques de manière transversale* ».

La définition d'une politique industrielle européenne apparaît effectivement indispensable pour « remonter la pente » et reconquérir les places perdues. À cet effet, selon M. Hervé Collignon, « ***un plan d'ensemble à l'échelle européenne devrait définir les domaines d'investissement prioritaires****, en concertation avec les associations et les industriels, pour tenir compte à la fois des demandes des citoyens en matière de santé, de transports, d'éducation, et des exigences de développement de secteurs économiques où l'Europe est déjà forte, comme l'automobile, les industries de process, les télécoms, les institutions financières, afin d'orienter les investissements vers la transformation à venir de ces secteurs* ».

La France et l'Allemagne, qui jouent un rôle moteur dans la dynamique européenne et sont dotées chacune d'une solide industrie du numérique et des technologies innovantes, **sont appelées à occuper les premières places et à montrer l'exemple**. Et ceci même si l'expérience de certains projets industriels franco-allemands a pu laisser une impression d'inachevé, tels que Quaero, un programme d'analyse automatique et d'enrichissement de contenus numériques, ou encore Galileo, le projet de système de positionnement par satellites alternatif au GPS.

Nos deux pays seraient voués naturellement à se rapprocher dans ce domaine, en prenant l'initiative d'une **politique plus intégrée de développement du secteur numérique**. Le Conseil national du numérique (CNNum) a ainsi plaidé, par la voix de son secrétaire général, M. Jean-Baptiste Soufron, pour la mise en place d'une « *CECA du numérique* », par analogie avec la première politique commune qui, dès le début des années 50, avait soutenu massivement les industries européennes du charbon et de l'acier. Ce « noyau dur » permettrait de travailler « *main dans la main avec quelques pays, pour pousser ensuite les feux au niveau de l'Europe toute entière* ».

Proposition n° 27 : faire émerger, à l'initiative de la France et de l'Allemagne, une véritable politique européenne de l'industrie numérique définissant les champs d'investissement à moyen et long terme, et mobilisant les instruments permettant de les atteindre.

Les élections européennes du mois de mai ont été une excellente occasion pour mettre en lumière le « besoin d'Europe » dans ce secteur du numérique. Le Forum numérique européen, groupe de réflexion mis sur pied au début de l'année, a publié en ce sens une lettre ouverte aux candidats à la présidence de la Commission européenne. Il y encourage les candidats à **inclure dans leur campagne électorale un agenda clair et ambitieux en faveur de l'économie numérique**. Cela doit passer par une stratégie transversale, précisent-ils, « *car c'est l'économie dans son ensemble qui est devenue numérique* ».

Par ailleurs et toujours dans cette perspective d'accroître le poids de l'industrie européenne du numérique, il conviendrait de « *créer des conditions de concurrence équitables pour les entreprises européennes sur le marché mondial* ». Cela requerrait la **définition d'un véritable « *level playing field* »**, c'est-à-dire d'un environnement dans lequel toutes les entreprises d'un marché donné sont traitées de façon identique - s'agissant des règles de subventions, d'aides d'État et de normes *anti-dumping*. Mme Gabrielle Gauthey, voyant là une condition *sine qua non* à la revitalisation des équipementiers européens, a insisté devant votre mission sur ce point. Il vaut d'ailleurs pour nombre d'autres secteurs industriels où nos entreprises souffrent d'une asymétrie des conditions concurrentielles par rapport à des acteurs tiers.

Cette recherche d'un « terrain de jeu » équitable avec les pays tiers les plus concurrentiels doit s'entendre également d'une **possibilité pour les acteurs européens de se rapprocher sans se voir entraver par des règles plus sévères que celles qui existent par ailleurs**. Début mai, la chancelière allemande, Angela Merkel, a ainsi appelé à ce qu'« *un équilibre [soit] trouvé entre puissance sur le marché et concurrence* », et ce pour que les entreprises européennes « *puissent marquer des points au niveau international* »[1]. Soulignant que la Chine avait trois grands fournisseurs de télécommunications alors que l'Union en a 28, elle a expliqué que, lorsque l'un d'eux cherchait à s'agrandir, la législation européenne en matière de

[1] *« Concurrence : Berlin pour plus de marge de manœuvre pour les télécoms »,* Agence Europe, *9 mai 2014.*

concurrence menaçait de le bloquer. Durant sa campagne pour l'accession à la présidence de la Commission européenne, le candidat du Parti populaire européen (PPE) M. Jean-Claude Juncker, s'est engagé en ce sens à « *repenser l'application de nos règles de concurrence dans le marché du numérique* ».

Plus récemment encore, l'approche de la Commission européenne tendant à imposer aux opérateurs mobiles souhaitant fusionner des cessions d'infrastructures à titre compensatoire a été contestée par les autorités nationales de la concurrence et certains opérateurs, voire par la chancelière allemande[1]. Pour les autorités de la concurrence allemande, irlandaise, autrichienne, italienne et britannique, cela remettrait en cause l'investissement dans la 4G et contraindrait *de facto* les opérateurs à augmenter leurs prix. Et en tout état de cause, les régulateurs nationaux conservent le pouvoir d'imposer des corrections *ex post*, si des ententes concurrentielles voyaient le jour.

Votre rapporteure, dans son rapport intitulé *L'Union européenne, colonie du monde numérique*, appelait également à « ***instaurer un tel débat proprement politique autour de la mise en œuvre de la politique de concurrence*** ». Elle y relevait l'approche globale mise en œuvre par les États-Unis, où « *la politique antitrust n'est pas déconnectée de la politique industrielle* ». Intégrant en outre les enjeux culturels, elle y proposait ainsi d'« *encadrer la politique de la concurrence par des objectifs politiques (sécurité des réseaux, maîtrise de ses données par l'Union européenne, diversité culturelle, neutralité du* net, *promotion de l'industrie européenne du numérique…)* ».

Proposition n° 28 : inciter la Commission européenne à concilier les règles de concurrence européennes dans le secteur numérique avec une ambition de puissance industrielle favorisant l'émergence de « champions européens ».

b) Favoriser la constitution d'un tissu industriel de PME et d'ETI du numérique et faciliter leur financement

Le secteur du numérique a été fortement marqué par le **développement, à la fin des années 90, des « jeunes pousses » ou « *start-up* »**, jeunes entreprises à fort potentiel de croissance faisant l'objet de levées de fonds. Proliférant dans les technologies de l'information et de la communication (TIC) – alors qualifiées de « nouvelles » –, ces entreprises « *dot com* » (c'est-à-dire en « .com ») recherchaient une entrée rapide en bourse et promettaient des profits substantiels.

Issu des États-Unis, ce modèle y a donné lieu aux **plus belles réussites du secteur du numérique**, et ce en des **délais extrêmement courts**. Les « GAFA » (à l'exception d'Apple), mais aussi Yahoo, eBay, Twitter, qui toutes ont commencé comme des « *start up* », n'existaient pas il y a vingt ans. Si l'on remonte un peu en arrière, des entreprises comme Intel, Microsoft ou Apple ont également connu une telle évolution.

[1] *À l'occasion des fusions entre Hutchinson et Orange en Autriche, et entre Hutchinson et Telefonica en Irlande.*

En France, de **beaux succès** ont également été enregistrés, avec des entreprises comme Free, PriceMinister, Pixmania, Meetic, Dailymotion ou Deezer, qui datent d'une quinzaine d'années pour les plus anciennes et ont revêtu à l'origine la forme de « *start up* ».

La **tentation** serait donc grande de vouloir **favoriser l'émergence de nouvelles « *start up* » nationales dans le numérique**, qui viendraient concurrencer les *leaders* mondiaux du secteur. Il n'est pas évident, cependant, que cette stratégie soit aujourd'hui la plus opportune. En effet, le risque d'échec de ce type d'entreprises est élevé, du fait de leur petite taille et de leur manque de visibilité sur des marchés ayant déjà atteint une forme de maturité.

Comme l'a souligné devant votre mission M. Nicolas Colin : « *Quand tout, hier, était ouvert, le paysage est aujourd'hui dominé par de grands géants qui ont franchi la barre, souvent grâce à la bulle spéculative des années 1990, et se trouvent en position dominante sur des marchés globaux. Nos dirigeants politiques, nos industriels doivent prendre cette nouvelle donne au sérieux. On n'a plus affaire à de jeunes gens qui bricolent dans leur garage, mais bien à des capitaines d'industrie qui jouent en calculant plusieurs coups à l'avance sur le grand échiquier de l'économie mondiale*. »

Mais l'obstacle le plus important réside sans doute dans le **risque de prédation des « *start up* » par des acteurs étrangers**, comme l'ont montré devant votre mission MM. Pierre Bellanger et Loïc Rivière. Les grands acteurs américains du secteur ont en effet tendance à voir dans ces structures légères, qu'ils peuvent facilement racheter, un **moyen d'externaliser leur R&D sur le territoire européen**, en y profitant d'un environnement fiscal favorable, à travers le crédit impôt recherche, mais aussi une main d'œuvre extrêmement qualifiée et créative.

Ainsi que le constate M. Loïc Rivière en effet, « *il semble que nos PME qui réussissent n'aient d'autre avenir que d'être absorbées par des grands groupes américains : la France serait-elle devenue une « terre d'externalisation de la R&D » pour ces grands groupes ? Ce serait inquiétant, car cela sanctionnerait notre incapacité collective à créer des champions industriels de classe mondiale ; c'est vrai dans les logiciels, où il n'y a plus qu'un seul acteur français – et quatre ou cinq européens – dans le Top 20 mondial du numérique, et où notre Top 10 a été décimé, ces dernières années, par des rachats.* »

Plus que la multiplication de petites initiatives souvent promises à l'échec ou au rachat par des acteurs étrangers, il faudrait donc **préférer la constitution d'un véritable réseau de très petites (TPE), petites et moyennes entreprises (PME), voire d'entreprises de taille intermédiaire (ETI)**, qui soit à même de se fédérer, de mutualiser certaines compétences, d'établir des synergies et de faire preuve d'une plus grande résistance vis-à-vis d'acteurs tiers.

Le rapport de notre collègue Bruno Retailleau sur les entreprises de taille intermédiaire (ETI)[1], dont nombre d'analyses et de préconisations valent

[1] Les entreprises de taille intermédiaire au cœur d'une nouvelle dynamique de croissance, *rapport au Premier ministre, février 2010.*

également pour les PME, a bien mis l'accent sur la **nécessité de « faire bloc » pour ces entreprises**. « *Trop longtemps ignorées des pouvoirs publics comme des économistes* » et constituant « *le maillon fragile du tissu économique français* », elles souffrent « *d'un manque de coopération entre [elles]* ». Et ce alors qu'« *une PME ou une ETI isolée est une entreprise potentiellement en danger* ». Aussi le rapport propose-t-il « *l'organisation [d']écosystèmes de coopération* » entre entreprises de ce type.

Au-delà de ces coopérations entre entreprises, il semble que la **facilitation de l'accès aux financements** soit une condition indispensable au développement des PME et ETI du secteur numérique. À défaut, comme l'a observé M. Loïc Rivière, le « *manque de capitaux laisse la place aux fonds d'investissement américains* » et les « *petites structures tombent rapidement dans le giron des grands groupes américains* ». Le secrétaire général de Dailymotion, M. Giuseppe de Martino, a ainsi pointé les carences dans l'accompagnement de la croissance de ce type d'entreprises. Il a cité l'exemple de sa propre société, de 200 salariés, qui manque de moyens pour poursuivre son développement.

Votre rapporteure avait déjà, dans son rapport évoqué plus haut, mis en lumière « *une **faiblesse concernant le financement de la croissance des jeunes pousses**, d'une part au stade de l'amorçage et du décollage […], et d'autre part, au stade de leur développement […]* ». Le rapport citait le rapport de l'Inspection générale des finances (IGF) sur le soutien à l'innovation numérique en France[1] et le rapport de MM. Colin et Collin sur la fiscalité numérique précité.

Relevant « *le lien étroit que l'économie numérique entretient avec le capital-risque* », mais aussi le caractère limité des possibilités d'introduction en bourse en matière numérique au vu de la faible liquidité des places financières, il formulait notamment comme proposition d'« ***encourager le capital-risque européen**, socle de souverai*neté*, et **faciliter l'introduction en bourse** des jeunes entreprises européennes du numérique pour leur permettre de financer leur développement au lieu d'être rachetées* ».

Il apparaît que, dans le secteur numérique, le **soutien requis pour les entreprises en croissance doive excéder le court terme et se poursuivre jusqu'au dégagement des premiers bénéfices**, lequel peut arriver plus ou moins tardivement. Les entreprises innovantes du numérique sont en effet basées sur un modèle économique précaire dans lequel les profits ne couvrent pas nécessairement les investissements. **Amazon**, devenu le *leader* mondial de la distribution en ligne, **a ainsi été financé pendant huit ans à fonds perdus**, avant les premiers retours sur investissement.

Pointant l'urgence de « *prendre de **nouvelles décisions pour assurer l'accès des entreprises aux liquidités** dont elles ont besoin* », le rapport Retailleau précité

http://www.caissedesdepots.fr/fileadmin/PDF/06._solutionsdurables_tv/EM01-synthese_du_rapport_retailleau_sur_les_eti_original.pdf

[1] Le soutien à l'économie numérique et à l'innovation, *rapport de l'IGF, janvier 2012. http://www.igf.finances.gouv.fr/webdav/site/igf/shared/Nos_Rapports/documents/2012/2011-M-060-02.pdf*

énumérait plusieurs mesures qui permettraient de « dénouer » ce problème. Elles consistent en l'instauration d'une fiscalité favorable à l'autofinancement, en la mise en place de plateformes régionales d'orientation financière pour mieux informer les entreprises, en la facilitation de la transmission familiale de ces entreprises ou encore en l'engagement de la Caisse des Dépôts et Consignations sur un programme d'abondement ou de co-investissement dans des fonds de capital développement adaptés.

Proposition n° 29 : mieux accompagner les TPE, PME et ETI françaises et européennes du secteur numérique en favorisant, à l'échelle nationale comme européenne, la coopération entre elles et en confortant leur accès à des solutions de financement adaptées (renforcement du capital-risque, facilitation de leur introduction en bourse…).

c) Former des « clusters » *de dimension européenne*

Les **pôles de compétitivité**, ou *clusters*, ont été **définis par la loi** comme des regroupements « *sur un même territoire d'entreprises, d'établissements d'enseignement supérieur et d'organismes de recherche publics ou privés qui ont vocation à travailler en synergie pour mettre en œuvre des projets de développement économique pour l'innovation* ». Ce type de structures, qui bénéficient de subventions publiques et d'un régime fiscal particulier, ont par nature vocation à intervenir dans les technologies d'avenir.

La **troisième phase de développement** des pôles de compétitivité a été lancée par le Gouvernement début 2013, et s'inscrit dans le cadre du Pacte national pour la croissance, la compétitivité et l'emploi. Particulièrement en phase avec la nouvelle économie, elle cherche à accroître les retombées des projets de R&D en termes de croissance et à amplifier l'accompagnement de la croissance des PME et ETI dans les territoires.

C'est ainsi que de **nombreux secteurs de l'économie numérique** ont fait l'objet de tels pôles. Comme l'indique le rapport de la commission « innovation 2030 » précité, « *un écosystème dynamique de start-up existe ainsi en France autour de ce sujet. Des pôles de compétitivité du domaine des TIC, qui favorisent les coopérations publiques privées, tels que Systematic, Cap Digital, Images & réseaux ou Solutions communicantes sécurisées, sont un outil de concentration de cet écosystème*. »

Mais beaucoup de ces pôles sont aujourd'hui, de par leur dimension nationale, d'une **taille trop étroite pour conquérir les marchés extérieurs**, et cela tout particulièrement dans le secteur numérique, très largement mondialisé. Il conviendrait donc de fédérer les pôles de même type existants chez nos partenaires européens, afin là encore d'atteindre cette « masse critique » indispensable pour contester la domination des grands acteurs mondiaux du numérique.

L'orientation des politiques communes vers le soutien à l'émergence de *clusters* européens de classe mondiale s'est faite, en ce sens, à la fin des années 2000. Elle a été définie par des communications de la Commission européenne de

2008 et 2010[1] et dans les conclusions du Conseil compétitivité, adoptées sous la présidence française en novembre 2008. Tardant à se concrétiser, elle a été relancée par la *smart specialization*, ou « spécialisation intelligente », qui représente l'élément clé de l'initiative européenne pour 2014-2020, « l'Union pour l'innovation ».

Poursuivant un objectif de « croissance intelligente », ou *smart growth*, basée sur la connaissance et l'innovation, l'Union européenne estime le niveau pertinent pour appréhender la spécialisation économique comme étant le pôle de développement économique ou le *cluster*, et recommande de s'inspirer de l'exemple français en la matière.

Plusieurs directions générales de la Commission européenne sont impliquées. La DG Politique régionale et urbaine mobilise les fonds structurels, notamment le Fonds européen de développement régional (FEDER). La DG Entreprises et industrie, avec son programme Compétitivité et innovation (CIP), aide au développement de coopérations entre *clusters* au niveau européen. Enfin, la DG Recherche facilite les projets de recherche communs à plusieurs *clusters*.

Malgré ces instruments et initiatives, le **bilan des *clusters* européens reste mitigé**, le dépassement de leur territorialisation au niveau régional vers une intégration proprement européenne restant difficile. Leur concentration dans les secteurs innovants à forte valeur ajoutée en ferait pourtant des catalyseurs de développement naturels pour des initiatives transeuropéennes dans les domaines de l'Internet et du numérique. Il conviendrait donc de mieux utiliser les opportunités offertes par le cadre communautaire en la matière.

Selon M. Hervé Collignon, co-auteur du rapport d'AT Kearney sur l'Europe numérique, « *des* clusters *paneuropéens devraient être créés* ». Quant au choix des lieux où ils doivent être créées, indique-t-il, « *mieux vaut [le] déterminer […] en tenant compte de l'implantation des grands donneurs d'ordre qu'en se guidant sur un seul souci d'aménagement du territoire. On pourrait imaginer de confier le* cluster *automobile à l'Allemagne, les télécoms à Stockholm, la défense, la sécurité et l'aéronautique à la France, la banque à Londres. […] Il s'agit de confier un* leadership *aux pays les plus avancés, en fléchant les investissements selon un plan concerté à l'échelle de l'Europe.* »

Proposition n° 30 : utiliser davantage les instruments facilitant la mise en place de *clusters* européens dans les secteurs de l'Internet et du numérique.

[1] « *Vers des* clusters *de classe mondiale dans l'Union européenne : mise en œuvre d'une stratégie d'innovation élargie* », *communication de la Commission européenne du 17 octobre 2008 ;* « *Une politique industrielle intégrée à l'ère de la mondialisation* », *communication de la Commission européenne du 28 octobre 2010.*

d) S'assurer que notre politique commerciale intègre le secteur numérique sans remettre en cause la protection de nos valeurs

La négociation actuellement en cours d'un partenariat transatlantique de commerce et d'investissement (TTIP)[1] entre l'Union européenne et les États-Unis cristallise la différence d'approche distinguant l'Europe de certains États tiers en matière de politique commerciale. Dotée d'un marché unique ouvert et attractif, celle-ci doit en effet veiller à ce que ses partenaires commerciaux traitent d'une façon réciproque ses entreprises et respectent les valeurs qu'elle place au-dessus d'aspects purement consuméristes.

(1) Un volet numérique insuffisamment pris en compte par l'Union européenne

L'objectif du TTIP est d'aboutir, par l'élimination des obstacles non tarifaires entre les deux continents, à réduire les barrières aux échanges de biens et de services dans la quasi-totalité des secteurs, et ainsi à créer entre les deux ensembles une **zone de libre-échange transatlantique à l'horizon 2015**. Avec 30 % des échanges commerciaux internationaux et 46 % du PIB mondial, celle-ci serait la plus importante au monde. La cinquième série de négociations sur ce traité de libre-échange s'est ouverte en ce sens le 19 mai dernier à Arlington[2].

La politique commerciale relevant de la **compétence exclusive de l'Union européenne**, selon l'article 3 du traité sur le fonctionnement de l'Union européenne, ces négociations sont conduites par la Commission européenne, autorisée en ce sens par le Conseil de l'Union européenne. Le Parlement européen y est associé, tout accord commercial étant, *in fine*, soumis à son approbation. Les parlements nationaux seront aussi sollicités pour approuver l'accord dans la mesure où il est mixte, c'est-à-dire qu'il affecte aussi les compétences nationales.

Mener à bien une telle négociation est dans l'intérêt réciproque des deux parties, à commencer par l'Union européenne. Le Conseil et la Commission européenne s'étaient prononcés en faveur de l'ouverture de ces négociations en se basant sur des études d'impact indiquant qu'un tel accord de libre-échange permettrait d'**accroître de 0,5 % la production économique annuelle de l'Union**.

La négociation sur ce projet de traité comprend un **important volet numérique**. Ainsi que le souligne le CNNum dans son avis d'avril dernier au ministre du commerce extérieur sur ledit volet[3], ce projet de partenariat bilatéral « *est le premier à être aussi ambitieux en matière de numérique* ». Le Conseil pointe notamment « *l'envergure qu['y] prennent les multiples dispositions tendant à faciliter les échanges et les investissements transfrontaliers dans le domaine du numérique* ».

Or, ces aspects numériques, pourtant fondamentaux dans la perspective d'une économie mondiale ouverte et dématérialisée, ne sont **pas suffisamment**

[1] *Ou* Trans-Atlantic Free Trade Agreement *(TAFTA).*

[2] *La première série s'est ouverte en juillet 2013 à Washington, la deuxième en novembre 2013 à Bruxelles, la troisième en décembre 2013 à Washington et la quatrième en mars 2014 à Bruxelles.*

[3] Partenariat transatlantique de commerce et d'investissement : faire du volet numérique un atout pour la négociation, *avis du CNNum pour le ministre du commerce extérieur, avril 2014.*

investis et pris en compte par les mandataires européens. Jugeant « *parfois insuffisante la mobilisation des négociateurs officiels* », le CNNum déplore ainsi que « *le volet numérique du projet de partenariat de commerce et d'investissement soit sous-estimé* », ce qui entraîne un « *rapport de force […] défavorable à l'Union européenne* ».

Pour Mme Valérie Peugeot, le déficit de politique européenne en matière industrielle, et plus précisément dans le secteur du numérique, « *constitue un lourd handicap […] dans les négociations internationales, comme celles qui sont en cours sur le traité transatlantique, le TTIP, où l'Europe entre mal préparée, où ses industriels n'ont guère conscience des enjeux commerciaux qui s'y jouent* ».

Mme Peugeot a attiré l'attention, à cet égard, sur le risque lié à l'inclusion dans les négociations d'un tel volet numérique qui « *pourrait bien, dans des domaines comme l'éducation ou la santé, se révéler un cheval de Troie* ». Derrière les négociations du TTIP, les **États-Unis souhaiteraient en effet contourner les initiatives de la Commission européenne** et le projet de règlement sur la protection des données personnelles pour instaurer une dérégulation sur des secteurs protégés par l'Union européenne, tels que l'éducation, la santé et la culture.

D'une façon générale, la critique couramment émise, et relayée par nombre d'associations et d'acteurs de la société civile, porte sur l'**insuffisante capacité de l'Union européenne à faire valoir et protéger la spécificité de ses valeurs dans le secteur du numérique**. En effet, aux termes de l'article 1 *bis* du traité la constituant, l'Union européenne s'est construite sur les valeurs de respect de la dignité humaine, de liberté, de démocratie et d'État de droit, et les transactions de biens et services doivent s'opérer dans un cadre s'y conformant.

Or, **l'approche des États-Unis**, qui recherchent avant tout l'ouverture de nos marchés, **est toute autre** en la matière. « *Les ambitions affichées sont claires* », observe le CNNum, nos partenaires américains souhaitant en effet « *faciliter le commerce et les échanges de produits et de services délivrés* via *l'utilisation du commerce électronique* » d'une part, et « *inclure dans le TTIP des dispositions permettant le mouvement transfrontalier de données* » d'autre part. Et pour atteindre ces objectifs, les Américains disposent de moyens d'action et d'influence bien plus importants que ceux de l'Union européenne.

« *L'**asymétrie entre les États-Unis et l'Union européenne en matière de numérique** ne peut être ignorée* », insiste le CNNum. En effet, les premiers « *disposent d'une avance commerciale et intellectuelle fondée sur une vision à long terme. Elle a été élaborée de longue date et appuyée sur des crédits notamment militaires, tandis que l'attitude suiviste de l'Union européenne lui a été gravement préjudiciable. Les États-Unis bénéficient d'une très forte synergie avec leurs institutions politiques et administratives. L'industrialisation du numérique y est plus aboutie qu'en Europe. Les capacités d'investissement y sont mieux mobilisées. L'ambition d'en faire un facteur de puissance est affichée. Les acteurs du marché américain disposent de moyens de développement commercial et d'investissement plus importants que leurs équivalents européens.* »

Si le rapport de force peut paraître inégal, l'**Union européenne a cependant de solides avantages à faire valoir** dans la négociation pour ne pas se plier à la volonté des États-Unis. Fort d'un marché de 500 millions d'utilisateurs potentiels, globalement bien formés et dotés d'un pouvoir d'achat conséquent, notre continent est présent dans de nombreuses industries de pointe du secteur numérique. Surtout, il a su garantir le respect de valeurs pouvant constituer autant d'atouts pour des entreprises et des consommateurs de plus en plus sensibles à la préservation de leurs données et de leurs libertés.

(2) Des valeurs propres à l'Europe devant être réaffirmées dans les négociations

L'Europe ne doit pas faire preuve de timidité dans la protection de ses valeurs lors des négociations commerciales internationales, bien au contraire. Elle doit **mettre en avant la spécificité de son approche**, consistant à trouver un équilibre entre considérations économiques et préservation des libertés fondamentales.

Mme Catherine Trautmann, lors de son audition devant votre mission, a insisté sur l'importance pour l'Union européenne de **« tenir » cette ligne avec fermeté**. « *Dès lors que, dans les négociations commerciales, nous défendons non seulement des clauses de sauvegarde environnementale et sociale mais aussi de protection des droits et libertés fondamentaux, nous tenons une position forte* », a-t-elle observé. « *La France s'est montrée allante sur le TTIP, sur des questions comme l'origine géographique, mais les conditions que nous avons posées quant à l'exception culturelle ont été vues d'emblée comme une attitude offensive sur la protection des données*. »

C'est dans cette optique d'affirmation résolue de la spécificité du modèle européen comme un élément non négociable dans les accords commerciaux qu'est intervenue la résolution présentée par M. Claude Moraes, député européen. Elle pose en effet comme **condition de l'approbation du TTIP le règlement des questions relatives à la protection des données personnelles et au respect des droits et libertés** fondamentales des citoyens européens.

C'est également en ce sens que le CNNum recommande, de façon générale et comme première proposition, de « *s'appuyer sur les valeurs de l'Union européenne pour faire levier dans la stratégie de négociation* », mais également de « *conserve[r] sa capacité à réglementer et structurer le marché numérique dans le futur, et s'attache[r] à obtenir dans la négociation du traité toutes les garanties nécessaires à cet effet* ».

Cette posture générale, qui tend à « ne pas marchander » le maintien de nos valeurs européennes d'ouverture et de protection, se décline dans chacun des sous-enjeux ayant trait aux problématiques numériques abordées dans le cadre du TTIP.

- **Le système de protection des indications géographiques**

Les indications géographiques, en tant qu'elles sont porteuses d'une valeur économique pour les producteurs et d'informations au profit du consommateur, méritent d'être protégées par le droit. Très fortement présentes dans le secteur alimentaire, et plus précisément dans celui du vin et des spiritueux, elles constituent un **vecteur essentiel du développement économique** de l'Europe et de valorisation de la diversité de ses territoires.

Or, l'**ouverture en cours par l'ICANN des extensions de noms de domaine au « .vin » et « .wine » menace directement ce système de protection**, en risquant d'entraîner des confusions chez les consommateurs et de remettre en cause la notoriété de nos produits à l'export[1]. Le danger est d'autant plus grand que le projet de l'ICANN pourrait, à terme, s'étendre à d'autres indications géographiques européennes protégées. Ce dossier a pris une importance majeure et mobilise aujourd'hui l'ensemble des acteurs, économiques et politiques, concernés à l'échelle européenne.

Faute d'accord entre le secteur et les sociétés candidates à l'exploitation des sites en « .vin » et « .wine », les négociations semblent aujourd'hui dans une impasse risquant d'aboutir à une délégation par l'ICANN des noms de domaine en « .vin » et « .wine ». À cet égard, le **manque de détermination de la Commission européenne dans les négociations commerciales**, en particulier avec les États-Unis, a été soulignée par la Confédération nationale des producteurs de vin et eaux de vie de vin à Appellation d'Origine Contrôlée (CNAOC), qui voit dans l'évolution de ce dossier *« un très mauvais signal pour les discussions en cours entre l'Union européenne et les États-Unis en vue de conclure un accord transatlantique »*[2].

La problématique dépasse en fait le secteur du vin pour concerner celui des indications géographiques, auxquelles les États-Unis préfèrent la notion de marque. Pour Mme Vanessa Gouret, conseillère chargée de la politique commerciale et des règles du commerce international, « *les indications géographiques sont un sujet important et particulièrement complexe avec les Américains – parce qu'ils y voient une barrière commerciale, dans un environnement juridique largement dominé par le droit des marques, là où, en particulier en Europe du Sud, nous y trouvons un outil pour valoriser et protéger des territoires* ». Elle a signalé que 55 sénateurs américains avaient demandé que les États-Unis s'opposent à ce qu'elles figurent dans l'accord transatlantique.

Face à ces risques, **l'Union doit « parler d'une seule voix »** et **ne rien céder dans le maintien du système de protection** existant. Dans cette optique, le renforcement dans la législation européenne d'une part, et leur reconnaissance par les États-Unis d'autre part, sont attendus comme des préalables à une

---

[1] *Voir* supra *l'encadré sur le « .vin » et « .wine ».*

[2] *« « .vin » et « .wine » ou la première étape d'un racket mondial organisé », communiqué de presse de la CNAOC et de la Fédération européenne des vins d'origine (European Federation of Wine Origine – EFOW).*

discussion sur leur articulation avec les noms de domaine, comme dans le secteur du vin[1].

Proposition n° 31 : obtenir la reconnaissance explicite par les États-Unis du système des indications géographiques avant la mise en place des noms de domaine se référant à de telles indications.

- **Le traitement des données personnelles**

Pour ce qui est des données, dont les Américains poussent à un renforcement de la libre-circulation entre les deux rives de l'Atlantique, toute libéralisation devrait être complétée par des dispositions permettant des **restrictions fondées sur des objectifs de protection de la vie privée des personnes et de sécurité publique**, qui permettraient à l'Union européenne d'adopter des actes destinés à les mettre en œuvre.

Constatant que **les services numériques intensifs en exploitation de données pénètrent durablement des domaines où il ne peut être dérogé au respect de la souveraineté et des libertés fondamentales** (comme dans les secteurs de la santé, de la sécurité, des services financiers ou de l'énergie) et font naître des risques réels quant à leur préservation, le Conseil estime en effet qu'une « *vigilance particulière doit être portée à l'encadrement de ces pratiques* ».

Les **révélations sur la surveillance massive de citoyens européens ont eu des répercussions sur la stratégie de l'Union**. Peu encline désormais à s'engager dans un processus de libéralisation de la circulation des données, cette dernière a pris conscience de la nécessité, au contraire, de renforcer leur sécurisation.

Cette problématique, qui dépasse la seule question de la protection des données personnelles et constitue un véritable enjeu de politique industrielle, inclut le régime de stockage, de transfert et d'utilisation de tout type de données. L'Union serait particulièrement bienvenue, à cet égard, de s'entendre sur une **stratégie commune passant notamment par la signature d'un accord sur la règlementation de ces données**.

La libéralisation intégrale des flux de données doit donc être repoussée tant qu'un socle normatif protecteur n'a pas été validé au niveau européen, afin d'accompagner la transition des industries traditionnelles vers l'intermédiation numérique, et surtout de s'assurer du respect des libertés fondamentales et d'objectifs d'intérêt général (vie privée, sécurité publique, santé publique…). Il convient, dans cette perspective, de **mener à bien la procédure législative d'adoption du paquet « données personnelles »**, dont le vote définitif est attendu avant la fin de l'année[2].

Enfin, en cas d'adoption du principe de libre circulation des données, le CNNum recommande, à juste titre, de **prévoir des exceptions à la libre circulation des données** équivalentes aux dispositions des articles XIV et XIV *bis*

[1] *Voir* supra.
[2] *Voir* supra.

de l'Accord général sur le commerce des services (AGCS)[1] et **d'exclure du champ d'application les données relatives aux domaines sensibles** de la santé, de la cybersécurité et de la finance.

Proposition n° 32 : veiller à assortir toute libéralisation transatlantique de la circulation de ces données, d'exceptions justifiées par des objectifs de protection de la vie privée des personnes et de sécurité publique.

- **La politique de concurrence européenne**

La politique européenne de la concurrence a permis à l'Union d'établir un **marché unique fluide et homogène**, qui constitue un atout dans les négociations qu'elle mène avec ses partenaires commerciaux. Un tel marché ouvert peut cependant **se retourner contre elle** dès lors que les restrictions impliquées par cette règlementation, particulièrement strictes pour les entreprises européennes, ne se retrouvent pas dans les marchés tiers, et font donc peser sur elles un handicap concurrentiel.

Cette analyse avait été déjà clairement faite par votre rapporteure dans son rapport *L'Union européenne, colonie du monde numérique ?* Elle y observait ainsi que « *les restrictions en matière d'aides d'État auxquelles sont soumises les entreprises européennes leur font subir un* ***handicap concurrentiel face à des concurrents mondiaux assujettis à moins de contraintes****, recevant des subventions d'une manière moins transparente qu'en Europe ou privilégiés dans les marchés publics domestiques* ».

L'application d'une politique de concurrence forte au sein de l'Union doit permettre à de « nouveaux entrants » de disputer aux acteurs en place des parts de marché, et favorise en tant que tels les efforts de compétitivité et d'innovation de nos entreprises. Mais elle doit être prolongée, à l'extérieur de l'Union, par une **démarche offensive tendant à l'uniformisation des règles du jeu au niveau mondial**.

Comme l'a souligné le CNNum dans son rapport sur le volet numérique du TTIP, « *il est essentiel que le* ***principe d'égalité de traitement*** *soit respecté entre les différents acteurs du numérique et que les règles de concurrence s'appliquent sur tous les segments de la chaîne de valeur du numérique* ». La priorité doit donc être portée, dans les négociations commerciales internationales, à garantir un tel principe, dit « *level playing field* ».

Si tous les États membres de l'Union ne partagent pas forcément cette analyse, la France, qui la promeut, a été rejointe progressivement par un nombre croissant d'entre eux. Après que M. Mario Monti eut, dans son rapport *Une nouvelle stratégie pour le marché unique*, présenté en 2010 au président Barroso, souhaité faire de l'Union « *un marché ouvert mais non désarmé* », le Conseil compétitivité d'octobre 2012 a ouvert la porte à l'**inclusion d'une clause d'alignement** dans les accords commerciaux.

---

[1] *Les articles XIV et XIV* bis *de l'AGCS, annexé à l'accord instituant l'OMC, autorisent d'apporter à un accord de libéralisation des échanges des restrictions fondées sur des objectifs de protection de la vie privée des personnes et de sécurité publique.*

Une telle évolution assurerait une concurrence plus loyale entre l'Union européenne et les pays tiers sur les aides d'État au profit de ces technologies clefs génériques, que la Commission a identifiées comme essentielles pour la capacité industrielle et innovatrice de l'Union. Il faut aujourd'hui pousser cette inflexion jusqu'à son terme, et **obtenir de la Commission européenne un véritable rééquilibrage des conditions de concurrence** entre nos opérateurs et ceux des pays tiers.

Proposition n° 33 : inciter la Commission européenne à assurer une convergence règlementaire garantissant des règles de jeu équitables *(level playing field)* pour les entreprises européennes du numérique, notamment eu égard à l'encadrement des aides d'État.

- **L'ouverture des marchés publics**

Les marchés publics, qui représenteraient jusqu'à 20 % du PIB de la plupart des pays selon l'OMC, constituent un **débouché très important pour les entreprises du secteur numérique**. L'accès non-discriminatoire et transparent à ces marchés, garanti dans l'Union européenne, doit être également assuré dans les États tiers, afin que nos entreprises aient autant de chance d'y remporter des succès commerciaux que l'inverse.

En l'état actuel des choses, il existe une **grande différence dans l'accès à ces marchés publics entre notre continent et les États-Unis**, pour ne citer qu'eux. 85 % de nos marchés sont ainsi ouverts, en fait ou en droit, aux entreprises américaines, tandis que nos entreprises ne peuvent répondre qu'à 32 % des appels d'offre publics outre-Atlantique[1]. Ce taux, qui n'est que de 28 % pour le Japon, tombe à zéro pour la Chine, totalement fermée de ce point de vue.

Tout comme la grande ouverture du marché européen, la **faible ouverture du marché américain relève d'une véritable volonté politique**, et se manifeste à travers plusieurs grandes lois. Le *Small Business Act*, pour la plus connue, réserve l'accès à certains marchés publics aux PME américaines, ne donnant à nos PME que la possibilité de s'allier avec des partenaires locaux. Le *Buy American Act*, quant à lui, constitue un mécanisme de « préférence nationale » imposant à l'administration fédérale un traitement prioritaire pour les biens américains, sanctionnant ainsi les entreprises offrant des produits étrangers, et notamment européens.

Les accords de l'OMC proprement dit ne couvrent pas les marchés publics. Ceux-ci font en effet l'objet d'un **accord spécifique de l'OMC, dit accord AMP**, qui inclue les pays industrialisés (dont l'Union européenne) et quatorze autres (dont les États-Unis, le Canada, le Japon …), mais n'est **pas respecté**, comme le montre la faiblesse des taux d'ouverture précités. Il en découle que les entreprises de ces pays, qui peuvent venir nous concurrencer sur notre propre marché à des prix particulièrement bas, ne sont pas inquiétées sur leur marché domestique par nos propres entreprises.

[1] Cf. *rapport du CNNum sur le volet numérique du TTIP.*

Prenant conscience des risques d'une telle concurrence déloyale sur notre potentiel de croissance externe, **l'Union a fait de l'ouverture réciproque des marchés l'une de ses priorités**. Le Parlement européen a notamment adopté, à la mi-janvier, une proposition de règlement[1] allant en ce sens. Il permettrait, en cas d'adoption par le Conseil, de restreindre l'accès à nos marchés à des entreprises implantées dans des pays dont les marchés publics nous sont fermés, en application d'un principe de réciprocité.

Le Sénat a explicitement appuyé cette initiative européenne en votant une résolution européenne du 26 novembre 2012[2] favorable à la réciprocité dans l'ouverture des marchés publics. Le texte est cependant loin d'être définitivement adopté dans la mesure où un certain nombre d'États membres s'y opposent, sous prétexte d'un risque de renchérissement de l'achat public. Il convient donc, pour notre pays, de **continuer à se mobiliser pour qu'aboutisse la procédure d'adoption de ce texte** protecteur de nos entreprises du secteur numérique.

Proposition n° 34 : promouvoir une plus grande réciprocité dans l'accès aux marchés publics, pour ouvrir aux entreprises européennes des marchés dans les pays tiers.

2. Exploiter les données européennes au service du « bien commun »

a) Investir l'industrie du big data

Comme l'a mis en avant la commission « innovation 2030 », « *la multiplication des données créées par les particuliers, les entreprises et les pouvoirs publics sera porteuse de nouveaux usages et de gains de productivité. La mise à disposition par l'État et par ses opérateurs des données publiques constituera une opportunité pour favoriser l'essor de nouvelles* start-up. »

Or, **notre pays possède d'indéniables atouts pour occuper les premières places dans le traitement industriel du *big data*** : son école de mathématiques et de statistiques, parmi les meilleures au monde ; la présence sur le territoire d'entreprises déjà *leaders* de sous-segments de ce marché ; ou encore l'importance des investissements consacrés à la sécurité des données et des communications sur l'Internet.

Le *big data* : caractéristiques et champs d'application

Le *big data* désigne la collecte, l'exploration et l'analyse de grandes masses de données, en vue d'expliquer ou de prédire des évolutions ou des comportements à grande échelle.

[1] *Proposition de règlement concernant l'accès des produits et services des pays tiers au marché intérieur des marchés publics de l'Union et établissant des procédures visant à faciliter les négociations relatives à l'accès des produits et services originaires de l'Union aux marchés publics des pays tiers, COM(2012)124 du 26 mars 2012.*

[2] *Résolution n° 38 (2012-2013) sur la réciprocité dans l'ouverture des marchés publics.*

À l'origine opéré par les « géants » de l'informatique, tels qu'IBM dans les années 60, qui a créé les bases de données dites relationnelles, le *big data* est désormais opéré essentiellement par ceux du web, Google, Amazon, Facebook ou Twitter, qui ont développé leurs propres systèmes simplifiés, désignés génériquement par le terme Nosql.

On le présente traditionnellement comme caractérisé par la **règle des trois, voire des cinq « v »** :

– volume de données : de plusieurs millions de gigaoctets (Go) pour les géants du web à quelques milliers pour des fichiers de géolocalisation, il n'y a pas de limite clairement fixée ;

– vitesse d'actualisation et d'analyse des données : ces dernières sont aujourd'hui traitées en temps réel ou quasi-réel ;

– variété des données : texte, images, multimédia … ;

– véracité des données : la précision du résultat final (ou « *data mining* ») dépend du degré de précision des données ;

– valeur des données : le traitement des données peut être source d'immenses plus-values.

Les **champs d'application** du *big data* sont infinis : amélioration des diagnostics et du ciblage thérapeutique pour l'industrie pharmaceutique, efficacité accrue des campagnes de publicité sur le web, estimations des primes d'assurance, recommandations accompagnées d'achats pour les marchands en ligne, anticipation de la délinquance pour la police …[1]

En 2013, le *big data* a donné lieu à plus de 425 milliards de dollars d'investissement par les entreprises américaines, 200 millions de dollars par l'administration américaine et 3 millions d'euros par la Commission européenne. En France, où la commission « innovation 2030 » en a fait l'un des sept défis d'avenir, 11,5 millions d'euros de subventions sont dédiées par l'État à son développement[2].

Or, la **collecte des données personnelles et l'utilisation des données publiques**, auxquelles recourent les expériences de *big data*, sont **affectées d'un *a priori* négatif sur le Vieux continent**, par opposition à des pays plus jeunes et ouverts aux possibilités de développement et de croissance qu'elles recèlent pour l'ensemble de la société. Ainsi que l'a fait observer M. Stéphane Grumbach, « *il y a en France, comme plus généralement en Europe, un biais dans notre perception des questions de l'Internet* », biais provenant « *en partie d'une très forte sensibilité aux questions de liberté individuelle, et de la perception de l'individu menacé tant par la machine étatique,* via *la surveillance et la censure, que par la machine industrielle,* via *l'exploitation de la vie privée* ».

« *Si ces questions sont évidemment importantes* », poursuit-il, « *la trop forte focalisation sur ces sujets occulte […] des enjeux essentiels de la révolution numérique pour nos sociétés, [soit les] enjeux économiques, politiques, ainsi que géopolitiques.* ***L'équilibre primordial entre les intérêts particuliers et le bien commun est insuffisamment discuté.*** » Ainsi, excessivement « *focalisée sur la peur obsessionnelle*

[1] *Exemples cités dans l'article* « Big data *: trois défis pour les maths* », Le Monde science et techno, *27 janvier 2014.*

[2] *Chiffres cités dans l'article* « Big data *: perspectives de business et valeur déjà démontrée* », Les Échos, ADP - *Guillaume Chenu, 19 mai 2014.*

du mauvais usage qu'une société peut faire des données personnelles et des atteintes à l'individu, l'Europe n'a pas anticipé ni même compris les changements en cours dans le monde, non seulement aux États-Unis, mais également dans les autres pays, acteurs de la révolution numérique ».

Pourtant, l'industrie du *big data* représente un **poids économique potentiellement considérable**. McKinsey Global Institute évalue la création de valeur potentielle par le *big data* à 200 milliards d'euros dans les administrations publiques européennes[1] ; le Boston Consulting Group estime à 315 milliards d'euros en 2011 la valeur des données personnelles des consommateurs européens et considère que leur exploitation permettrait une création de valeur représentant 8 % de l'ensemble du PIB européen à l'horizon 2020[2].

Les **données personnelles constituent aujourd'hui une ressource activement recherchée** par tous les acteurs du net, **car elles déterminent la valeur**. Si les industries de l'Internet les exploitent pour cibler avec une plus grande précision les annonceurs, les données permettent aussi d'en apprendre davantage, « *non pas sur l'individu, mais sur une population* » ; en ce sens, leur croisement à une très grande échelle, rendu possible grâce aux puissants algorithmes mis au point par les grands acteurs du net et aux capacités de calcul exponentielles des ordinateurs, peut revêtir une **réelle utilité sociale**. C'est ainsi que Google a mis en place un service de suivi statistique des épidémies de grippe en avance d'une dizaine de jours sur les instituts de veille sanitaire.

Les **données sont certes le « *carburant des plateformes d'intermédiation* »** – moteurs de recherche et réseaux sociaux – qui dégagent des connaissances exclusives sur l'activité qu'elles observent et permettent ainsi d'autres services. Mais l'intérêt des plateformes, en réalité, « ***dépasse largement le numérique***. *Les plateformes d'intermédiation ont un potentiel de révolution de nos organisations considérable* », juge M. Stéphane Grumbach.

« *Une telle intermédiation entre des usagers qui offrent des services et d'autres qui sont à la recherche de tels services peut conduire à une efficacité extrêmement importante, ainsi qu'à des économies de très grande ampleur.* » Et cela sans compter la mise en réseau des objets connectés, qui vont augmenter les volumes de données et les services que leur traitement pourra rendre.

Ainsi, au vu de l'infinité de services que permettra l'utilisation des données, mais également de leur apport potentiel en termes de croissance et d'emploi, il est impératif que les pouvoirs publics, à l'échelle nationale comme européenne, fassent preuve de **vision prospective et d'anticipation dans l'accompagnement du *big data***, et s'attellent à définir des méthodes rendant l'exploitation du *big data* compatible avec le respect de la vie privée. Comme l'indique M. Stéphane Grumbach, « *il faudrait remettre en avant l'objectif du bien commun, alors que la vie privée est centrée sur l'individu* ».

---

[1] La force du nombre, Réaliser le potentiel socio-économique des entrepreneurs au XXIe siècle, *rapport McKinsey Global Institute, octobre 2011.*

[2] *Idem.*

Les pouvoirs publics prennent peu à peu la mesure de l'importance du *big data* pour notre économie. La précédente ministre en charge de l'économie numérique, Mme Fleur Pellerin, avait annoncé en juillet 2013 un **plan d'investissement de 300 millions d'euros dans le *big data***. Avec au cœur des mesures attendues, la création d'un incubateur dédié. L'objectif affiché est de pouvoir atteindre, en cinq ans, 2,8 milliards d'euros de création de valeur et de permettre la création de 10 000 emplois.

Il convient aujourd'hui de prolonger cet effort, d'évaluer son impact économique et surtout de **« changer de culture » vis-à-vis du *big data***, en y voyant au moins autant une ressource indispensable à la création de valeur dans une économie dématérialisée et au progrès social dans son ensemble, qu'un instrument potentiellement attentatoire aux libertés individuelles et sujet à encadrement normatif.

Finalement, c'est la loi qui doit tracer la frontière entre respect des libertés et possibilités d'usage commercial. Comme l'a fait observer M. Jacky Richard, rapporteur général du Conseil d'État, « *il faut définir avec attention la notion de données. […]* ***Le législateur devra réaliser des choix. […] Il [lui] revient […] de fixer la frontière entre les données privées dont la confidentialité doit être préservée et celles qui peuvent servir de base, grâce à des mécanismes d'agrégation sous réserve de précautions, à une économie fondée sur la valeur liée à l'exploitation de ces données.*** »

Proposition n° 35 : promouvoir le *big data* comme un véritable enjeu industriel, source d'amélioration du bien commun, en définissant précisément des mécanismes raisonnables pour l'agrégation de données susceptibles de faire l'objet d'une valorisation économique.

*b) Miser sur l'*open data *comme source de valeur pour toute la société*

Le Gouvernement et les administrations ne sont pas épargnés par l'évolution des flux de données en *big data*. La publication des données ouvertes prend, pour ces personnes publiques, le nom d'*open data*. Les systèmes d'intermédiation qu'il permettra de développer apporteront au citoyen de nouveaux services, sur la base d'informations indexées et organisées. Sur ce sujet, votre mission renvoie au rapport d'information récemment produit par son président et l'un de nos collègues, M. François Pillet[1].

L'*open data*

L'*open data* est une méthode de gouvernance favorisant l'accès aux documents et aux données publiques *via* l'Internet, afin de renforcer la transparence, de donner aux citoyens des moyens de contrôle de l'action publique, et de générer des activités porteuses d'une plus-value pour les utilisateurs ou pour la société toute entière.

[1] *Rapport n° 469 (2013-2014) réalisé au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur l'*open data *et la protection de la vie privée par MM. Gaëtan Gorce et François Pillet.*

En tant que tel, l'*open data* utilise les ressources de **l'« e-gouvernement »**, soit le recours aux TIC par les administrations publiques afin de rendre les services publics plus accessibles à leurs usagers et d'améliorer leur fonctionnement interne.

L'*open data* est **source de croissance**. Selon le rapport de Graham Vickery pour l'Union européenne[1], une plus grande ouverture des données publiques, telle que la permet l'*open data*, serait de nature à faire croître les marchés liés à l'exploitation de ces données de 32 à 40 milliards d'euros.

L'*open data* concerne au premier chef **l'État**. La plateforme « data.gouv.fr » permet ainsi « *aux services publics de publier des données publiques et à la société civile de les enrichir, modifier, interpréter en vue de coproduire des informations d'intérêt général* ».

Le Président de la République, M. François Hollande, a annoncé récemment l'adhésion française au Partenariat pour un gouvernement ouvert *(Open Government Partnership - OGP)*. Il réunit actuellement 63 États qui s'engagent à suivre les principes de la gouvernance ouverte et transparente, définis dans la déclaration de principes du 20 septembre 2011 : transparence de l'action publique, participation citoyenne à l'élaboration des politiques publiques, intégrité, innovation et utilisation des nouvelles technologies pour moderniser l'action publique, notamment à travers l'ouverture des données.

L'État devra ainsi établir, en concertation avec la société civile, un « plan d'action national » avant le 31 mars 2015, comportant des engagements en vue d'une gouvernance plus transparente, plus efficace et plus responsable. L'action de l'État en ce domaine est pilotée, sous l'autorité du Premier ministre, par la mission « Etalab », qui fait partie du Secrétariat général pour la modernisation de l'action publique (SGMAP).

Mais l'*open data* concerne également **les collectivités**, qui ont d'ailleurs ouvert la voie en étant parmi les premières personnes publiques à mettre en ligne leurs bases de données, l'association Open Data France et la 27ème Région œuvrant notamment en ce sens.

L'*open data*, en ce qu'il met à disposition des données placées sous la responsabilité et l'autorité des pouvoirs publics, est un **instrument qu'il convient donc de développer** au nom du bien commun en apportant toutes garanties d'une collecte et d'un traitement des données respectant les principes d'anonymat et de non-discrimination qui doivent guider l'action collective en la matière. Ainsi, comme l'a souligné M. Bertrand de la Chapelle, « *la collecte de données publiques ou sur objets connectés, pour leur exploitation en* open data *et* via *des mécanismes de croisement, va devenir source de valeur économique et sociale : c'est cela qu'il faut faciliter* ».

Il conviendrait, à cet égard, de **lever certains freins limitant l'apport potentiel de l'*open data* à la sphère économique** et à la croissance. Ces obstacles tiennent en majeure partie à des considérations d'ordre technique : manque de précision des données empêchant de générer une information à valeur ajoutée ; hétérogénéité des données proposées entre les territoires ; hétérogénéité des

[1] Review of recent PSI re-use studies and related market developments, *Graham Vickery, septembre 2011.*

formats dans lesquels sont proposées ces données…[1] Votre rapporteure fait siennes les recommandations formulées à cet égard par la mission commune d'information du Sénat sur l'accès aux documents administratifs et aux données publiques, en particulier la recommandation n° 15 visant à l'établissement d'un « *référentiel général de réutilisabilité des données, portant à la fois sur leur format, leur structuration, leur granularité, leur contextualisation, ainsi que sur la documentation des algorithmes permettant de procéder à des extractions et des agrégations* »[2].

Se pose par ailleurs une interrogation quant au modèle économique, le coût d'acquisition des données – qui sont parfois proposées contre le paiement d'une licence – pouvant être supérieur aux recettes générées, ce qui peut entraver la mise en œuvre de l'objectif de gratuité des données de l'*open data*.

Proposition n° 36 : poursuivre le développement de l'*open data* dans l'ensemble des collectivités publiques en standardisant les données délivrées et en tendant vers la gratuité de leur mise à disposition, tout en respectant les principes d'anonymat et de non-discrimination.

3. Lancer deux projets industriels concrets : *cloud* européen sécurisé mais ouvert pour les données les plus sensibles, et système d'exploitation pour mobile

Pour donner corps à l'ambition industrielle de l'Union européenne en matière numérique, il convient de lancer des projets industriels concrets.

Le premier serait de nature à redonner la main à l'Union européenne sur l'Internet mobile, le second sur la maîtrise de ses données qui transitent dans le *cloud*.

Le système d'exploitation Androïd, qui s'est diffusé rapidement sur les téléphones mobiles, a été développé par Google, et a démontré qu'**aucune position dominante** – celle de Microsoft ou d'Apple, en l'occurrence – **n'est incontestable sur un marché innovant**. Malheureusement, aucun équivalent n'a été mis au point sur notre continent, nous contraignant aujourd'hui à utiliser les systèmes étrangers sans pouvoir recourir à un substitut européen. Ainsi, selon M. Vincent Champain, « *l'Europe aurait pu décider de lancer son système d'exploitation, comme l'a fait [également] la Chine pour le téléphone mobile* ».

S'il eût été souhaitable de ne pas prendre de retard en ce domaine, le principe de « contestabilité » continuelle des positions dominantes, surtout sur des marchés entièrement basés sur l'innovation, comme l'est le secteur des TIC,

---

[1] *Voir, à ce sujet, les propositions faites par l'AFDEL, le syndicat des éditeurs de logiciels et solutions Internet, dans son document :* « Open data, *bilan d'étape de la stratégie française & propositions pour en faire un axe majeur de création de valeur pour l'industrie numérique », avril 2014.*

[2] *Refonder le droit à l'information publique à l'heure du numérique : un enjeu citoyen, une opportunité stratégique, rapport d'information de Mme Corinne Bouchoux, fait au nom de la mission commune d'information sur l'accès aux documents administratifs et aux données publiques (n° 589, 2013-2014) (disponible à l'adresse suivante : http://www.senat.fr/notice-rapport/2013/r13-589-1-notice.html)*

permet d'être optimiste. **Développer un *operating system* (OS) mobile propre à l'Europe** et de nature à concurrence Androïd et iOS semble pouvoir constituer un objectif parfaitement pertinent d'un point de vue économique, et qui, de surcroît, nous aiderait à restaurer notre souveraineté numérique.

Proposition n° 37 : favoriser le développement d'un système d'exploitation sur mobile européen constituant une alternative crédible aux principaux systèmes d'exploitation actuellement existants.

Un second projet, de plus grande envergure et viable seulement à l'échelle européenne, consisterait à faire émerger des services de *cloud* respectueux des exigences européennes en matière de protection des droits et libertés fondamentaux.

a) Le cloud*, au cœur de l'informatique de demain*

Si ses prémices sont apparues dès les années 50, avec l'accès depuis des terminaux à des applications fonctionnant sur des systèmes centraux, le *cloud* ne s'est vraiment développé, dans sa version contemporaine, que **dans les années 2000**, avec l'apparition des hébergeurs *web*, pouvant accueillir et conserver sur leurs serveurs des applications et des données.

Qu'est-ce que le *cloud computing* ?

Le *cloud computing*, ou « informatique en nuages », désigne, selon la définition qu'en donne le MIT, un ensemble de processus utilisant la puissance de calcul et de stockage de serveurs informatiques distants à travers un réseau, généralement l'Internet.

Il correspond à un important **changement d'approche des systèmes informatiques** : longtemps constitués de serveurs ou de terminaux situés au sein même des entreprises ou chez les particuliers, ils se trouvent désormais externalisés dans des centres de données, ou *data centers*, dont les services et les capacités de stockage sont loués à l'activité ou au forfait.

Trois types de services peuvent être offerts par le *cloud* :

– IaaS (« ***infrastructure as a service*** », ou infrastructure en tant que service) : mise à disposition d'une ressource matérielle virtualisée (services de calcul, de stockage et de réseau), gérée et administrée par un fournisseur ;

– PaaS (« ***platform as a service*** », ou plateforme en tant que service) : mise à disposition de plateformes nécessaires au développement ou à l'exécution d'applications ;

– SaaS (« ***software as a service*** », ou logiciel en tant que service) : mise à disposition de logiciels en ligne prêts à l'usage après un simple paramétrage.

L'utilisation d'une adresse *e-mail* constitue un usage courant et désormais bien établi du *cloud*. S'y est ajouté plus récemment l'utilisation à distance d'outils informatiques classiques (traitement de texte ou tableur, par exemple), puis l'utilisation des réseaux sociaux, qui constituent également des espaces de stockage pour des données personnelles de toutes sortes.

C'est afin de fournir l'ensemble de ces services qu'un acteur comme **Google** a bâti son propre *cloud* et représente, avec 50 milliards de dollars de chiffre d'affaires, le *leader* du secteur. Mais des groupes comme Amazon, Apple, Facebook, Twitter, eBay et YouTube recourent également à la technologie du *cloud* pour héberger les volumes extrêmement lourds de documents de leurs utilisateurs[1].

L'émergence réelle du *cloud* coïncide en réalité avec le recours massif des entreprises à ses services, dans le cadre d'un **modèle *BtoB*** (« *business to business* », c'est-à-dire entre entreprises). Il leur permet en effet de réduire très sensiblement les dépenses d'investissement et de fonctionnement informatiques, mais aussi d'harmoniser les services, de faciliter leur accès pour tous les collaborateurs et de garantir leur mise à jour permanente. C'est ce secteur qu'ont investi des entreprises anciennement implantées dans le secteur de l'informatique, telles que Microsoft, Oracle, IBM, HP, Accenture…

En moins d'une quinzaine d'années, le *cloud*, véritable révolution technologique dans le monde de l'informatique, s'est développé « *à la vitesse de la lumière* » et représente aujourd'hui une « ***fantastique opportunité en termes de croissance, de productivité et d'emploi*** », ainsi que le soulignent dès la première phrase de leur rapport sur le sujet MM. Thierry Breton, ancien ministre de l'économie, des finances et de l'industrie, président directeur-général d'Atos,

[1] *Et, pour la première, proposer également des services à des fournisseurs, y compris européens.*

chargé de deux missions sur le *cloud* par le Gouvernement et par la Commission européenne, et Octave Klaba[1].

Quelques chiffres tirés de ce rapport donnent la mesure de l'**importance fondamentale du *cloud*** pour le secteur des services informatiques, et au-delà pour l'économie en général. Représentant un marché de plus de 50 milliards de dollars dans le monde en 2013, il connaît une croissance de 20 à 30 % par an, et devrait représenter plus de 50 % des dépenses informatiques mondiales d'ici 2020.

b) Une importante avance des États-Unis sur l'Europe et la France

Ainsi que cela a été indiqué précédemment, **les États-Unis sont en pointe** dans le secteur du *cloud*, avec des acteurs occupant des positions de *leader*. **L'Europe n'est certes pas dépourvue d'atouts** en ce domaine, mais le paysage des fournisseurs européens de *cloud* est à la fois plus limité en volume et composé essentiellement d'acteurs des métiers informatiques traditionnels.

Il convient également de relever, comme le fait le rapport Breton-Klaba, que **l'Irlande a attiré sur son territoire de très importants *data centers*** (Amazon, Google et Microsoft) pouvant délivrer des services *cloud* depuis ce pays en garantissant la localisation des données en Europe, mais sans pour autant garantir leur traitement sur le sol européen, et en étant potentiellement soumis aux normes ou législations non-européennes.

La France, comme le rappelle le rapport précité, « ***occupe une position privilégiée*** *avec une communauté* Open Source *très active et de nombreuses* startups *proposant diverses solutions*[2]*, projets*[3] *et une plateforme d'expérimentation à grande échelle, Grid'5000* ». Représentant 2,8 milliards d'euros dans notre pays en 2012, le *cloud* a été défini comme l'un des 34 plans dans le cadre du projet de « Nouvelle France industrielle ». Par ailleurs, deux projets de centrales numériques (CloudWatt et Numergy) sont développés dans le cadre des Investissements d'avenir, qui prévoit également des subventions à des projets de R&D collaboratifs.

Pour autant, **nous sommes aujourd'hui « à la traîne » des États-Unis**, dans ce secteur qui sera demain capital à plusieurs égards. Ledit rapport fait ainsi état d'une situation « *préoccupante dans la mesure où la majeure partie des services* cloud *aujourd'hui consommés dans l'Hexagone est délivrée à partir de sites situés hors de France, et même le plus souvent hors d'Europe (si l'on excepte le cas de l'Irlande), ce qui peut à terme poser des problèmes d'indépendance et de souveraineté, voire, dans certains cas, de sécurité nationale pour notre pays* ».

---

[1] Nouvelle France industrielle, Rapport *Cloud computing, par MM. Thierrry Breton (Atos) et Octave Klaba (OVH), 31 janvier 2014.*
À noter que M. Thierry Breton a également été chargé par la Commission européenne, en binome avec M. Jim Snabe, le président-directeur général de SAP, d'un autre rapport sur le cloud dans sa dimension communautaire.

[2] *Alterway, eNovance, Lyatiss, Nuxeo, Nexedi, Treeptik, VDOM …*

[3] *OW2, Compatible One, Easi-clouds, Seed4C …*

Ce retard français, et plus globalement européen, s'explique par **divers facteurs** : une fragmentation des marchés locaux, le manque d'investisseurs dans les entreprises de taille intermédiaire, l'inadéquation des procédures de marché public aux offres *cloud*, les réticences nourries à son encontre en termes de sécurité des données et de continuité de service, les carences des dispositifs de formation et l'attirance des plus jeunes utilisateurs pour les acteurs mondiaux de pays tiers…

Fort heureusement, estime le rapport, cette **situation est « *encore réversible* »**, à la condition toutefois d'agir « *rapidement et en profondeur* », et cela tant sur notre territoire national qu'en Europe. Sachant que « *l'État – et, plus généralement, la puissance publique – ont un rôle moteur à jouer d'exemplarité, d'entraînement et de mise en place d'un environnement propice au développement d'un [tel] écosystème* ».

c) Plusieurs initiatives à l'échelle européenne en faveur du cloud

L'Union européenne est le cadre de plusieurs projets ou initiatives communes concernant le *cloud computing*.

Les conclusions du Conseil européen d'octobre 2013 prévoient la constitution d'un **réseau solide de coordinateurs nationaux** en matière numérique, qui pourrait jouer un rôle stratégique dans le développement de l'informatique en nuage. Son organisation et ses missions sont en cours de discussion.

Lors du 16ème conseil des ministres franco-allemand, en février 2014, la chancelière allemande, Mme Angela Merkel, a plaidé pour la création d'un **réseau européen de communications** pour éviter que les données des Européens transitent par les États-Unis. Ce projet, qui implique de contraindre les fournisseurs d'accès à Internet à stocker et traiter les données personnelles des citoyens de l'Union sur le territoire européen, requiert donc le développement du stockage et du traitement des données en Europe, *via* le *cloud* et le *big data*.

Parallèlement à ces initiatives, la Commission européenne a mis en place **l'*European cloud partnership*** (ECP), qui vise à développer les services et prestations d'informatique dans les nuages dans un cadre sécurisé.

L'European cloud partnership

L'*European cloud partnership* (ECP), ou partenariat européen en faveur de l'informatique en nuage, rassemble les entreprises et les pouvoirs publics afin de contribuer à la création d'un **marché unique du numérique pour l'informatique en nuage** en Europe. Il a été instauré dans le cadre de la stratégie numérique pour l'Europe 2010-2020, qui appelait à « *mettre en place une stratégie européenne sur «l'informatique en nuage», notamment dans les domaines de l'administration publique et de la science* ».

Ce projet commun, initié par la Commission européenne dans une communication de septembre 2012, se fonde sur ses **projections prometteuses pour le secteur de l'informatique en nuage** à l'échelle européenne : enregistrant actuellement une croissance de plus de 20 %, il pourrait peser près de 940 milliards d'euros dans le PIB communautaire et créer 3,8 millions d'emplois en Europe d'ici à 2020.

La stratégie définie par la Commission européenne dans le cadre de l'ECP poursuit **quatre grands objectifs** : garantir le transfert des données d'un prestataire de services en nuage à un autre, ou leur retrait complet ; établir un système de certification à l'échelle de l'Union pour les prestataires fiables ; élaborer des modèles de contrats d'informatique en nuage indiquant clairement les obligations contractuelles ; et créer un partenariat européen en faveur de l'informatique en nuage associant secteurs public et privé, afin de déterminer les besoins existants et de veiller à ce que le secteur européen des technologies de l'information puisse y satisfaire, de sorte que les entreprises soient plus compétitives face à la concurrence étrangère.

Composé de représentants de haut niveau du secteur de l'informatique et des télécommunications et de décideurs chargés des politiques publiques en matière de TIC[1], le comité directeur de l'ECP a été invité à conseiller la Commission européenne sur les **options stratégiques à suivre** pour faire de l'informatique en nuage un moteur de croissance économique durable, d'innovation et de maîtrise des coûts des services publics. Dirigé par M. Toomas Hendrik Ilves, Président de la République d'Estonie, il a tenu sa première réunion le 19 novembre 2012 et a mis la dernière main à sa proposition de « *Trusted Cloud Europe* » le 13 février 2014.

Ces **premières pistes d'action** visent à :

– favoriser la confiance des utilisateurs (guides de bonnes pratiques, mise en place de standards européens de sécurité, création d'un code de bonne conduite des fournisseurs …) ;

– lever les restrictions nationales en matière de localisation des données, proposition qui a suscité des réserves des autorités françaises.

La Commission européenne a présenté, le 26 juin, des **lignes directrices sur le *cloud*** visant à aider les utilisateurs professionnels à faire des économies en tirant le meilleur parti de ces services. Élaborées par un groupe de parties prenantes du secteur, dans le cadre de la stratégie de la Commission en matière de *cloud*, elles constituent une première étape vers la normalisation de la terminologie et des paramètres des accords de niveau de service *(Service Level Agreements - SLA)*. Elles aideront les utilisateurs à vérifier que certains éléments

[1] *La France est représentée par la Direction générale de la compétitivité, de l'industrie et des services (DGCIS), au titre des pouvoirs publics, et par M. Thierry Breton, PDG d'Atos, au titre du monde de l'entreprise.*

essentiels figurent en termes clairs dans les contrats conclus avec les fournisseurs de services d'« infonuage ».

La Commission européenne va maintenant tester ces lignes directrices auprès des utilisateurs, en particulier des PME. Elles seront également examinées par le groupe d'experts en matière de contrats d'informatique « en nuage », mis sur pied par la Commission en octobre 2013.

Aux yeux de votre mission, le maître-mot de ce « *cloud* à l'européenne » doit être la **sécurisation des données** transférées, par contraste avec les solutions de pays tiers. Plusieurs degrés de sécurisation peuvent être envisagés à cet égard, dont il n'est pas certain que le plus radical soit le plus efficace, ou du moins le plus opérationnel.

d) La « fausse bonne idée » d'un cloud *souverain pour répondre à une vraie menace*

- **Une volonté légitime de répondre au déficit de sécurité dû au caractère extraterritorial de la législation américaine**

Le projet de créer un *cloud* européen souverain se justifie, selon ses promoteurs, par l'**absence de protection suffisante des données confiées à des solutions fournies par des prestataires de pays tiers**. Ce sont les hébergeurs américains, principaux acteurs du marché, qui sont naturellement au cœur des suspicions, du fait de la règlementation à laquelle ils sont soumis.

Les lois sécuritaires adoptées par les États-Unis dans les années 2000 (« Patriot Act », « FISA Act » …) donnent en effet aux autorités américaines (FBI, CIA, NSA) d'**importants instruments d'interception de données** de toutes sortes détenues par des entreprises privées et leur permettant de faire avancer leurs investigations. Ces mêmes autorités, dans une interprétation extensive des textes, vont jusqu'à exiger la remise de données possédées par des entreprises ou filiales d'entreprises américaines situées hors des États-Unis, voire d'entreprises étrangères, européennes notamment, ayant seulement des relations d'affaires systématiques avec les États-Unis.

Les révélations de l'affaire Snowden ont mis en lumière avec acuité de tels risques. Ainsi que l'indique très explicitement la DGCIS, dans la contribution remise à votre mission, « *il ne peut pas […] être tout à fait exclu que les* ***autorités américaines se considèrent en droit de requérir de prestataires français de*** **cloud** ***la communication de données*** *: si les acteurs hexagonaux de* cloud *venaient à commercialiser leurs offres de* cloud *sur le marché américain, si leur actionnariat venait à être contrôlé par des intérêts américains ou si des implantations de serveurs étaient envisagées sur le sol américain, ces prestataires français deviendraient alors directement soumis au* Patriot Act ».

Les entreprises européennes, au final, sont mal protégées de l'effet extraterritorial de la législation américaine, et hésitent à mobiliser les outils existants. Soucieuses de maintenir de bonnes relations avec les autorités américaines, elles n'invoquent ainsi que très rarement la loi dite « de blocage » du

26 juillet 1968[1]. Ainsi, insiste la DGCIS, « *les entreprises françaises ou européennes qui recourent aux services de* cloud *de prestataires américains […] ne disposent d'aucune garantie quant à la non-communication de ces données aux agences de sécurité américaine, voire aux risques d'intelligence économique* ».

- **Un projet de *cloud* souverain difficile à mettre en place en pratique**

La **solution d'un *cloud* souverain européen** est la plus radicale et, partant, la plus attirante *a priori* pour sécuriser le développement de notre industrie et la protection de nos données. Elle consiste à exiger, outre l'implantation sur le territoire européen du ***data center*** fournissant le service de *cloud*, que la **pile matérielle et logicielle** le constituant soit entièrement européenne, voire française.

Ainsi, aucun composant de pays tiers – américain, notamment, mais aussi chinois – n'entrerait dans la fabrication du système. Il serait alors **impossible à des entreprises ou agences étrangères d'introduire des mécanismes de surveillance cachés**, comme des « chevaux de Troie », dans le matériel ou le logiciel en vue d'« interroger » le système à distance. C'est ce qui a conduit les États-Unis, de leur côté, à interdire à Huawei, équipementier chinois, de fournir des routeurs aux entreprises américaines.

Si cette approche est tentante en théorie, elle semble en réalité peu praticable. En effet, elle requiert de **développer et produire en Europe l'ensemble de la plateforme *cloud***, depuis les puces électroniques jusqu'au service Saas. Or, selon la contribution fournie par l'Institut national de recherche en informatique et en automatique (INRIA), « *cela n'est* ***clairement pas réaliste*** », pour au moins deux raisons.

D'une part, l'Europe ne dispose pas forcément des **capacités industrielles** permettant d'assurer ce type de production rapidement et dans les volumes importants que nécessiteront le développement du *cloud*. Par ailleurs, l'interdiction de fournisseurs étrangers n'est **pas une solution imparable** : la multiplication des degrés de sous-traitance rend difficile la traçabilité des produits électroniques[2] ; en outre, certaines solutions entièrement nationales n'ont pas empêché des cyberpiratages[3].

Par ailleurs, d'un point de vue plus juridique, et selon l'analyse opérée par le ministère de la justice, un *cloud* européen ne **garantirait pas l'application du seul droit européen** pour les entreprises soumises à la fois à la règlementation de l'Union européenne et à la loi américaine, et ce quand bien même les données seraient localisées sur le sol européen.

---

[1] *Loi n° 68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères.*

[2] *En 2008, une agence fédérale américaine s'est ainsi aperçue que certains routeurs Cisco seraient en fait des contrefaçons chinoises.*

[3] *Comme lors du piratage de Belgium Telecom qu'aurait effectué la NSA pour récupérer des méta-données sur les appels passés en Belgique.*

« *Méfions-nous donc de notre propension à renouer avec le cadre familier de la frontière ; pousser trop loin la logique de souveraineté, notamment en militant pour des* clouds *nationaux, pourrait nous faire perdre une bonne part des bénéfices que le partage des infrastructures et le* cloud *peuvent apporter* », a ainsi alerté Bertrand de La Chapelle. « *Certes, les abus constatés ne sont pas admissibles, mais préconiser, pour y remédier, la relocalisation des données et le* cloud *national reste une vue de court terme, qui pourrait provoquer une fragmentation, source de dommages irréparables à long terme.* »

- **Une exception envisageable pour les données les plus sensibles**

En réalité, la **solution du *cloud* souverain européen**, si elle n'est pas généralisable pour l'ensemble des données pour des raisons de praticité et de coût, pourrait être **indiquée pour une partie d'entre elles, à savoir les plus sensibles** telles celles relatives à la défense ou à la fiscalité, qui touchent aux missions régaliennes de l'État, ou encore à la santé.

Une telle solution trouverait d'ailleurs un **appui dans une récente décision de la Cour de justice de l'Union européenne**[1], qui invalide la directive européenne sur la conservation des données de 2006 du fait notamment qu'elle « *n'impose pas une conservation des données sur le territoire de l'Union* », et qu'ainsi elle « *ne garantit pas pleinement le contrôle du respect des exigences de protection et de sécurité par une autorité indépendante, comme cela est pourtant explicitement exigé par la charte des droits fondamentaux de l'Union européenne* », contrôle qui « *constitue un élément essentiel du respect de la protection des personnes à l'égard du traitement des données à caractère personnel* ».

Comme le souligne le ministère de la justice dans la réponse au questionnaire adressé par votre mission, la perspective d'un *cloud* européen pour les données sensibles serait **favorable aux droits des justiciables français**, car les détenteurs des données resteraient responsables du traitement réalisé dans l'Union européenne. Cela éviterait à des entreprises européennes, pour la gestion de ces données capitales, de faire appel à des sous-traitants et prestataires de *cloud* établis hors de l'Union. Il n'est pas non plus souhaitable que des collectivités publiques confient la gestion de leurs données sensibles à des prestataires non européens, comme l'a fait la région de Bretagne en confiant ses données de santé à Amazon.

Pour les autres données que ces données d'une particulière importance, il ne serait donc pas nécessaire de requérir un *cloud* européen souverain, mais des solutions plus souples, comprenant une partie plus ou moins grande d'externalisation hors Union, mais dont les procédures feraient l'objet d'une certification garantissant leur sécurité.

[1] *CJUE, gr. ch., 8 avril 2014, Digital Rights Ireland et Seitlinger e.a., C-293/12.*

e) La préférence pour un dispositif général de labellisation de services cloud *sécurisés*

Plutôt que de développer un dispositif de *cloud* souverain paraissant peu réaliste, les analystes semblent converger sur la nécessité de **sécuriser l'usage du *cloud***, en favorisant l'émergence d'une **offre qui se différencie par sa qualité et sa transparence**. Créer un cadre pour restaurer la confiance des utilisateurs, c'est le principe qui doit guider l'intervention publique en ce domaine : après l'affaire Snowden, trop d'entreprises – cela a été rappelé à plusieurs reprises lors des auditions – hésitent aujourd'hui à mettre leurs données sur le *cloud* pour des raisons de sécurité et de confidentialité.

Cette volonté de **conforter les opérateurs en sécurisant le *cloud*** est justement l'objectif de la première des propositions du rapport Breton-Klaba. Elle rejoint d'ailleurs en cela les préoccupations de l'ECP, l'initiative franco-allemande et les propositions du Parlement européen. Cette proposition vise à définir « *une classe de services labellisée « Secure Cloud »* », ouvrant à leurs détenteurs une sorte de « permis d'opérer » dans ce secteur.

Selon ses auteurs, les opérateurs s'engageant dans cette voie proposeraient un « ***référentiel de conditions contractuelles types*** » touchant notamment à la sécurité, à l'accès au service, à la confiance et surtout à la localisation des données et de leur traitement. À cet égard, et sauf exception approuvée par le client, les infrastructures et les données, ainsi que leur traitement, se situeraient dans une « ***zone de confiance*** » formée par les pays adhérant aux recommandations de l'ECP.

Votre mission observe malgré tout qu'une telle zone de confiance ne serait pas à l'abri de l'application extraterritoriale des lois américaines. Lors de son audition, M. Thierry Breton a considéré que « *les données des Européens doivent être stockées et processées en Europe. C'est là un point sur lequel il ne faut pas transiger : nos données nous appartiennent.* » Il a préconisé, dans cet esprit, qu'une **politique d'*opt-in***, c'est-à-dire de consentement préalable, soit mise en œuvre par les pays qui s'accordent sur une approche régulatrice du traitement et du stockage des données, voyant dans l'Allemagne et la France deux pays moteurs pour l'initier.

M. Philippe Lemoine a également estimé nécessaire, « *si l'on veut mettre en avant l'idée que nous pouvons offrir une* ***industrie de l'hébergement de données plus digne de confiance que l'industrie américaine****, […] qu'existent des mécanismes juridiques* ad hoc ». À cet égard, il a souligné que « *la clarté des normes techniques appliquées à un traitement et la capacité à prouver, par un contrôle effectif, que la pratique des entreprises est bien conforme à la loi, sont des exigences déterminantes* ».

Toutes ces idées visant à sécuriser le *cloud* par des mécanismes juridiques adaptés rejoignent d'ailleurs la proposition n° 8 du précédent rapport de votre rapporteure, qui consistait, « *au nom de la sécurité, [à] conditionner dans l'Union européenne l'achat d'équipements hautement stratégiques, comme les routeurs de cœur de réseaux, à leur* ***labellisation par une autorité nationale ou européenne de sécurité***,

afin de se prémunir contre l'espionnage par les pays fournisseurs de tels équipements à bas prix, comme la Chine ».

La labellisation préconisée par le rapport Breton-Klaba, qui s'étendrait donc à l'ensemble des éléments constitutifs du *cloud* – infrastructures, plateformes et logiciels – serait ouverte à tous les opérateurs mettant effectivement en œuvre ces bonnes pratiques, sans condition de nationalité. Un **acteur européen d'émission de certificats de sécurité** gagnerait à être promu pour institutionnaliser les procédures et renforcer la confiance dans le dispositif.

Ainsi que le préconise également le rapport Breton-Klaba, le lancement d'un **appel à projets du Commissariat général à l'investissement** (CGI) sur les solutions de sécurité *cloud* permettrait de valider l'approche au regard des préconisations des autorités françaises (ANSSI, CNIL) et européennes, notamment en matière de cybersécurité, et de compléter l'éventail des offres existantes.

Proposition n° 38 : définir une classe de services labellisés « *Secure cloud* », faisant l'objet de cahiers des charges stricts et protecteurs, et promouvoir un acteur européen compétent pour émettre des certificats de sécurité correspondants.

f) Mobiliser le levier de l'achat public

Le recours au *cloud* par l'ensemble des personnes publiques – État, agences, instituts de recherche, collectivités… – est source de **nombreux avantages** : optimisation des investissements, réduction des coûts de fonctionnement, amélioration des services rendus aux États-Unis… De plus, l'exemplarité des pouvoirs publics en la matière serait de nature à créer un effet d'entraînement sur les acteurs privés, et de permettre d'accéder à une masse critique rendant le prix des services plus attractif.

Les facilités et atouts du *cloud* s'inscrivent en effet dans les **préoccupations d'économie** des pouvoirs publics. Ainsi, les 500 à 800 millions d'euros d'économies demandées par le Premier ministre lors du Comité interministériel de modernisation de l'action publique (CIMAP) du 18 décembre dernier au secrétariat général pour la modernisation de l'action publique (SGMAP) et à la direction interministérielle des systèmes d'information et de communication (DISIC) seraient plus aisément atteints en recourant au *cloud*.

Dans cette perspective, le rapport Breton-Klaba préconise deux types de mesures de nature à développer le *cloud* grâce à une impulsion publique. La première serait d'**utiliser les marchés publics informatiques comme un « *puissant levier du passage au* cloud »**. Les procédures d'achats de la puissance publique devraient, dans cette perspective, être conçues pour permettre une réponse en mode *cloud*, ce qui n'est pas le cas aujourd'hui, le plus souvent. À l'inverse, les responsables administratifs devraient être fortement incités à intégrer une part de services *cloud* dans les réponses sélectionnées.

Surtout, les réponses aux marchés publics utilisant les services labellisés « *Secure Cloud* » devraient bénéficier d'une attention accrue de la part des pouvoirs publics, dès lors que cette certification garantit le respect des principes de qualité et de sécurité de service poursuivis par l'action publique.

Cet objectif de systématisation du recours au *cloud* dans la commande publique rejoint la proposition n° 21 du rapport précité de votre rapporteure, qui visait à « *encourager l'achat public avant commercialisation de services européens de fourniture de contenus et d'applications numériques, afin d'accompagner le développement des start-up européennes et, pour ce qui concerne les services de* cloud computing*, de sécuriser les données personnelles des Européens* ».

La seconde proposition consiste **à mettre en place, sur des plateformes *cloud* de type « Appstore » ou « Androïd market », des applications validées à destination des personnes publiques** et présentant toutes garanties en termes d'adéquation aux besoins et de sécurisation des données.

Ce concept de « place de marché », où un certain nombre de solutions de *cloud* pourraient être pré-référencées par un processus centralisé, puis mises à la disposition des organismes publics, ferait l'objet d'une obligation de consultation avant tout autre processus d'achat. Une telle contrainte faciliterait son adoption et accélèrerait l'atteinte d'un objectif légitime de « retour sur investissement ».

Proposition n° 39 : mieux intégrer les solutions *cloud* dans la commande publique et mettre en place un espace de services *cloud* sécurisés à destination des administrations publiques.

4. Exploiter les atouts européens en matière de sécurité sur l'Internet

a) L'importance du chiffrement dans la sécurisation des échanges sur l'Internet

La sécurisation des échanges sur l'Internet peut être favorisée par des procédés de cryptographie tels que **le chiffrement et le codage**[1]. Le chiffrement consiste ainsi à rendre impossible la compréhension d'un document à toute personne n'en possédant pas la clef de déchiffrement, l'algorithme utilisé n'étant quant à lui pas spécialement protégé.

L'usage de logiciels de chiffrement a **longtemps été interdit en France** pour des raisons de sécurité publique. Ainsi n'était-il pas permis, jusqu'il y a moins d'une vingtaine d'années, de recourir au PGP *(Pretty Good Privacy)*, l'un des premiers logiciels de ce genre disponible sur l'Internet. C'est la loi du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) qui a totalement libéralisé

[1] *En réalité, seul le chiffrement a pour objet de rendre les informations illisibles pour une tierce personne : le codage, s'il rend* de facto *plus difficile l'accès à des contenus du fait qu'il transforme des données en des symboles, vise à en réduire la taille par compression, et non à les dissimuler.*

l'usage de tels logiciels, tout en maintenant leur importation ou exportation à déclaration ou autorisation.

La complexité croissante des systèmes informatiques intégrés accroît leur fragilité et leur exposition aux virus et menaces de toutes sortes, qui plus est du fait de dispositifs de protection souvent insuffisants. **Le danger est aujourd'hui bien présent**, et ce **dans des secteurs sensibles**. Devant votre mission, le responsable de Netopia, Per Strömbäck, a par exemple fait état de la vulnérabilité des codes utilisés par les centrales nucléaires américaines. Il a également attiré l'attention sur les conséquences de la diffusion des attaques liées à la faille de sécurité *Heartbleed* jusque dans le centre fédéral des impôts canadiens. On pourrait ajouter à cette liste les attaques dont a été victime l'opérateur historique belge Belgacom, en septembre 2013.

L'INRIA, dans la contribution qu'elle a adressée à la mission d'information, attire l'attention sur la **vulnérabilité de l'Internet et les conséquences potentiellement délétères d'une corruption de grande ampleur**. « *Pour les mots de passe, il arrive trop souvent que les bases de données des sites web ne soient pas chiffrées (ou faiblement) et que des grands ensembles de mots de passe se retrouvent dans le domaine public. […] De plus, une grande partie du chiffrage des communications repose sur le protocole SSL (https par exemple). Hors, tout comme les noms de domaines, les certificats SSL utilisés pour l'authentification du serveur reposent sur une structure stricte et très contrôlée par les ÉTATS-UNIS. La corruption du système de certificat aurait des impacts encore plus grands en termes de sécurité que celles des serveurs DNS. En effet, il serait possible de se faire passer pour un site commercial ou gouvernemental et de lire les informations envoyées entre les utilisateurs et le site.* »

Or, la **cryptographie peut contribuer à se prémunir contre ces risques d'intrusion en ligne**. L'Américain Bruce Schneier, l'un des experts en sécurité mobilisés sur l'étude des documents de la NSA, mais aussi Edward Snowden, ont plaidé en faveur d'un usage généralisé du chiffrement. Les travaux récents de l'IETF et du W3C se sont également intéressés à ces moyens de protéger la confidentialité de l'Internet : la future version « 2.0 » du protocole Http, utilisée pour naviguer sur le web, serait chiffrée par défaut, tandis que le réseau Tor – réseau mondial décentralisé favorisant l'anonymat – serait étudié comme un futur standard[1].

De plus, nous possédons sur le territoire européen d'**excellents spécialistes de la cryptographie**, dont le recours pourrait nous être précieux pour sécuriser les transferts de courriels, fichiers et données. M. Louis Pouzin a ainsi vanté les mérites de nos « *très bons ingénieurs du chiffre, que l'on pourrait valoriser* » selon lui, tandis qu'Edward Snowden a fait référence à l'excellence des cryptographes belges.

[1] *Voir, pour l'ensemble de ces références, l'article « Chiffrer le Net pour retrouver notre vie privée en ligne : une bonne solution qui pose des problèmes », Slater, 23 avril 2014.*

b) Une place à prendre pour l'Europe dans le domaine de la sécurité de l'Internet

Il résulte des éléments précédents que **le chiffrement est une technologie dotée d'une utilité reconnue par les experts, et dont l'Europe possède la maîtrise**. En conséquence, il y a là une réelle « carte à jouer » pour développer des solutions de cryptographie plus poussées, qui soient adaptées à la nature des différents besoins et deviennent des références à l'échelle internationale.

Favorable au développement de la cryptographie, dans laquelle il voit un instrument propre à renforcer la protection de l'Europe vis-à-vis, notamment, des systèmes d'investigation américains, M. Louis Pouzin a proposé d'**adapter le chiffrement aux besoins** : « *on peut chiffrer faiblement des choses qui n'ont pas grande importance, comme le courrier personnel, certains rapports, ..., mais lorsque le sujet devient critique, il faut des chiffres très difficiles à casser, susceptibles de poser de sérieux problèmes aux attaquants* ».

Il a également plaidé pour **rendre plus faciles à utiliser les certificats**, qui permettent d'institutionnaliser la pratique de certains chiffrements en cas de transfert d'argent ou de données personnelles exigeant un haut degré de sécurisation. Du fait d'une interface inaboutie avec les personnes, l'actuel système, PGP, serait en effet « *assez barbare et décourageant* ».

Proposition n° 40 : développer les compétences européennes en matière de chiffrement, notamment en facilitant l'utilisation de certificats.

c) Sécuriser juridiquement l'Internet en promouvant le recours à des noms de domaine sous juridiction française ou européenne

Les extensions de noms de domaine se référant à des territoires européens offrent une sécurité pour les acteurs européens de l'écosystème numérique, en ce qu'elles les placent sous le ressort des juridictions européennes.

Lors de son audition, M. Mathieu Weill, directeur général de l'Association française pour le nommage Internet en coopération (AFNIC), indiquait : « *notre mission de service public est de développer le « .fr », qui comprend environ 2,5 millions noms de domaine, face au « .com » qui demeure* leader, *y compris en France. Or le fait d'être enregistré en « .com » donne un point d'appui à la juridiction américaine.* » Ce dernier point est d'autant plus important que, contrairement au registre des noms de domaine en « .com », la base de données associée à la gestion des noms de domaine en « .fr » n'est pas publique : ces données ne sont communiquées qu'aux autorités françaises et seulement si elles en font la demande sur la base d'un fondement légal.

Votre mission se réjouit que « *la base de données enregistrée en France demeure l'une des plus protectrices au monde* », selon les mots de M. Mathieu Weill. Elle déplore en revanche que **le « .fr » ne soit classé qu'au quatorzième rang mondial** avec 2 652 702 noms de domaine enregistrés en septembre 2013. Cela le place certes juste devant Italie, l'Argentine et la Pologne, mais bien après le « .de » géré par l'équivalent allemand de l'AFNIC, la DENIC eG, qui compte plus de

15 730 000 noms de domaine et même le « .nl » néerlandais qui comptabilise en mars 2014 près de 5 441 358 noms de domaine. L'extension « .nl » se classe ainsi en neuvième position mondiale et représente 73,5 % de parts de marché aux Pays-Bas.

Classement mondial des extensions pays au mois de septembre 2013[1]

Rang de classement	Extension	Nombre de noms de domaine enregistrés
1	.com - Générique	111 476 933
2	.tk - Tokelau, Gratuit	19 118 740
3	.de - Allemagne	15 504 792
4	.net - Générique, Réseaux	15 460 439
5	.co.uk - Royaume-Uni	10 460 115
6	.org - Générique, Organisation	10 284 293
7	.cn - Chine	7 808 360
8	.info - Générique	6 691 674
9	.nl - Pays-Bas	5 309 125
10	.ru - Russie	4 757 635
11	.eu - Union Européenne	3 703 240
12	.br - Brésil	3 280 402
13	.au - Australie	2 730 138
14	.fr - France	2 652 702
15	.it - Italie	2 586 024
16	.ar - Argentine	2 500 000
17	.pl - Pologne	2 456 407
18	.biz - Générique	2 408 791
19	.ca - Canada	2 118 521
20	.us - États-Unis	1 844 661

Pour les raisons juridiques susmentionnées et afin de mieux ancrer la France dans le cyberespace, votre mission estime donc souhaitable une meilleure diffusion du « .fr ». L'Union européenne devrait aussi promouvoir plus largement le recours au « .eu ».

Proposition n° 41 : promouvoir la diffusion du « .fr » et du « .eu ».

5. Préparer la place de l'Europe dans l'Internet de demain

a) Promouvoir l'open source et les logiciels libres

(1) Une approche alternative aux univers fermés en plein développement

Face à la progression des systèmes fermés et des considérations marchandes dans l'univers de l'Internet, les **logiciels *open source* ou « libres » constituent des alternatives intéressantes pour l'Europe et la France**, en ce qu'ils rompent avec les « *logiques de rente et de commercialisation* » dénoncées devant

[1] Cf. *http://www.prodomaines.com/classement-noms-domaine-extension-septembre-2013.*

votre mission par M. Francesco Ragazzi, et qu'ils maintiennent la maîtrise des utilisateurs sur les systèmes.

M. Jérémie Zimmermann a insisté, dans cet esprit, sur l'importance, face à une montée en puissance depuis une quinzaine d'années des logiciels et matériels fermés, de se « *concentrer sur les valeurs universelles à défendre sans compromis* », parmi lesquelles « *l'ouverture et la maîtrise des technologies par les citoyens* », qui passent notamment par le développement des logiciels libres. Même analyse pour Roberto di Cosmo, selon lequel « *il faut encourager les logiciels libres et les formats ouverts, qui sont la clé de la maîtrise de la technologie* ».

Open source et logiciels libres :
un même produit pour deux approches différentes

Si *open source* et logiciel libre décrivent **à peu près le même type de produits**, c'est-à-dire des logiciels dont l'utilisation, l'étude, la modification et la reproduction sont autorisées techniquement et juridiquement, les deux concepts sont porteurs de valeurs et approches fondamentalement différentes[1].

Les deux communautés, qui n'en faisaient qu'une à l'origine, **ont « divorcé » à la fin des années 90**, lorsque ceux défendant l'*open source* voulurent mettre en avant les aspects de puissance et de fiabilité, tout en rejetant les valeurs morales véhiculés par le mouvement à l'origine.

L'*open source* est ainsi devenu une **méthodologie de développement basée sur des considérations pratiques** : selon ses partisans, les logiciels non libres représentent des solutions sous-optimales aux problématiques à résoudre. Au cœur de l'*open source*, se trouve la faculté, reconnue à l'utilisateur, d'accéder aux codes sources du logiciel.

Les défenseurs du logiciel libre s'inscrivent davantage dans un **mouvement de société défendant des valeurs éthiques et philosophiques** : liberté, solidarité sociale, partage et coopération. Les droits relatifs aux logiciels libres peuvent être soit disponibles (s'ils relèvent, par exemple, du domaine public), soit établis par une licence dite « libre ».

Open source et logiciel libre se retrouvent toutefois dans leur **hostilité au logiciel propriétaire ou privateur**, c'est-à-dire non libre, sur lequel seul le développeur dispose de droits.

Open source et logiciels libres ne sont **pas forcément synonymes de gratuité**. Même si ce n'est pas le plus courant, ils peuvent faire l'objet de rémunérations pour couvrir les travaux de création, développement et soutien technique. À l'inverse, un logiciel gratuit (ou « *freeware* ») n'est pas forcément un logiciel libre, dans la mesure où son code source n'est pas systématiquement accessible, et où la licence ne correspond pas toujours à la définition du logiciel libre.

D'un niveau de qualité et de fiabilité en progression constante, les logiciels libres **ont intégré, ces dernières années**, les systèmes d'information de **nombreuses entreprises**, des PME aux grands groupes : environnements serveurs, domaines applicatifs, outils d'ingénierie, solutions de sécurité... Ils ont également investi les **administrations**, tant au niveau centralisé qu'à celui des

[1] *Sera conservée, dans la suite du rapport, le terme de « logiciel libre ».*

agences de l'État ou des collectivités : l'exemple le plus emblématique est la gendarmerie nationale, dont les ordinateurs ont migré vers Linux.

Le Conseil national du logiciel libre (CNLL) a rendu compte du **succès croissant des formats libres de logiciels** : représentant 6 % de l'ensemble des logiciels et services, soit une valeur de 2,5 milliards d'euros, ils occupent 30 000 personnes – dont 3 000 chez les « *pure players* » – réparties dans 300 entreprises, essentiellement des PME et TPE. La filière, qui a crû de 68 % en 2012, devrait avoir progressé de 83 % en 2013.

Début 2013, le succès du logiciel libre tient à plusieurs raisons :

– il est **source d'économies et de compétitivité** : en rendant, comme l'observe le Premier ministre dans la circulaire DISIC[1] de septembre 2012[2], un service égal ou supérieur, pour un coût sensiblement moindre, aux entreprises et administrations qui le déploient, le logiciel libre est un atout en temps de crise car il améliore de manière immédiate la compétitivité de l'ensemble de notre industrie ;

– il permet aux entreprises, et notamment aux plus petites, d'**innover à moindre coût** et ainsi de **monter en gamme** : selon le cabinet d'étude Forrester[3], l'innovation dans le logiciel est aujourd'hui dix fois moins onéreuse qu'il y a dix ans grâce au logiciel libre. Accélérant les échanges et s'opposant à un « verrouillage » durable du marché, il pousse en effet les acteurs économiques à se démarquer par l'innovation ;

– il permet de **réduire la dépendance, stratégique et économique, de la France vis-à-vis de fournisseurs étrangers** : « *En ces temps de vaches maigres, on trouverait bien des avantages à utiliser des programmes ouverts comme LibreOffice, OpenOffice ou Firefox au lieu de verser des fortunes à Microsoft* » a ainsi souligné M. Francesco Ragazzi ;

– il est **plus protecteur en termes de sécurité** : ainsi que l'a expliqué M. Francesco Ragazzi, il « *laisse à la communauté les mains libres pour remédier aux failles de sécurité et prévenir la pratique des* backdoors » et, en outre, permet « *d'assurer la confidentialité de la navigation sur Internet* », telle que celle qui a donné naissance au réseau Tor[4].

(2) Des compétences nationales qu'il faut encourager par une politique adaptée

La France est parmi les pays les plus en pointe dans le domaine du logiciel libre. Ainsi que le notait une étude du cabinet Pierre Audoin Consultants de 2012[5], « **la France reste le marché phare du logiciel libre dans le monde**, *avec*

[1] *Direction interministérielle des systèmes d'information et de communication.*
[2] *Voir infra.*
[3] *http://www.wcm.bull.com/internet/pr/rend.jsp?DocId=412283&lang=fr*
[4] *Réseau informatique mondial et décentralisé pouvant garantir l'anonymat des échanges entre utilisateurs.*
[5] Le logiciel libre continue sa percée au sein des entreprises françaises, *étude de Pierre Audoin Consultants, janvier 2012.*

de nombreuses compétences de haut niveau qui ont une influence non négligeable dans les communautés ».

C'est donc la bonne formation et les aptitudes reconnues de sa main d'œuvre qui déterminent l'avance dont la France bénéficie dans ces technologies, dont le rapport anticipe qu'elles pourraient représenter 9 % du marché des logiciels et services en 2015.

Depuis 2003, **plusieurs *clusters* et associations d'entreprises du logiciel libre ont été mis en place** en vue de fédérer les moyens et les projets développés dans le secteur : Prolibre, Libertis, Alliance libre, GTLL, PLOSS, PLOSS RA et Aquinetic, répartis sur l'ensemble du territoire et regroupés au sein du CNLL. Ce riche écosystème a donné naissance à plusieurs jeunes pousses en pleine ascension, à l'image de la première d'entre elles, l'éditeur de logiciels libres Talend.

Notre pays dispose donc d'importantes ressources et compétences dans le domaine du logiciel libre, qu'il lui faut aujourd'hui pousser davantage pour maintenir et conforter cet atout économique autant que stratégique.

- **Conserver une approche prudente dans le recours aux logiciels libres sans obérer leur développement**

En premier lieu, certains écueils doivent être évités afin de ne pas brider la croissance de la filière. À ce titre, il convient d'abord de **conserver une certaine prudence, et ne pas voir dans le logiciel libre une « solution miraculeuse** » : en témoignent les attaques récentes liées à la faille de sécurité *Heartbleed*, découverte au sein de la bibliothèque de cryptographie *open source OpenSSL*, à l'occasion de corrections proposées par un développeur bénévole et validées par l'équipe Open SSL[1]. En ce sens, la publication du code source, qui caractérise le logiciel libre, le rend davantage susceptible de modifications pouvant le corrompre, en même temps qu'elle permet également de les repérer et corriger plus facilement.

Par ailleurs, le logiciel libre n'est **pas synonyme de protection des petits développeurs et des PME contre les grands éditeurs de logiciels et les multinationales de l'informatique**. Ainsi, de grands groupes participent fréquemment à la mise au point de logiciels libres : IBM a largement contribué à la création du système d'exploitation GNU/Linux, tandis que le système Androïd est la propriété de Google[2]. Du reste, comme l'a souligné M. Roberto di Cosmo, « *les services qui font fonctionner Internet aujourd'hui – chez Google, Facebook, Tweeter ou Amazon – utilisent une quantité de logiciels libres impressionnante* ».

---

[1] *En effet, les moyens humains alloués à la découverte d'éventuelles failles étaient très insuffisants. Ils ont depuis été augmentés par un financement conjoint des grandes sociétés de l'Internet dans le cadre de la* Core Infrastructure Initiative. Cf. *http://www.generation-nt.com/openssl-google-boringssl-libressl-fork-actualite-1896622.html*

[2] *Androïd est un système open source utilisant le noyau Linux.*

Enfin, et en rapport avec l'observation précédente, il convient de veiller à **ne pas brider excessivement l'innovation des PME en brevetant les logiciels**. Cette limite a été observée par la mission lors de son déplacement aux États-Unis : certaines grandes entreprises du secteur des TIC y ont déposé des brevets sur des algorithmes cruciaux dans le fonctionnement de logiciels libres, rendant leur accès plus délicat et onéreux pour de petits entrepreneurs. Par ailleurs, la « guerre des brevets » que se livrent par tribunaux interposés Apple et Samsung depuis 2012[1] illustre bien les risques de blocage de l'innovation qu'entraîne la brevetabilité des logiciels.

La promesse de campagne faite par l'actuel Président de la République en avril 2012, selon laquelle il fallait veiller « *à ce que la mise en œuvre du brevet communautaire ne soit pas l'occasion de légitimer les brevets sur les logiciels* », mériterait à cet égard d'être réaffirmée et réactualisée.

Proposition n° 42 : veiller à la préservation du principe européen de non brevetabilité des logiciels.

- **Développer l'usage des logiciels libres dans un cadre sécurisé**

Mais la défense des logiciels libres passe également, dans une perspective plus dynamique, par la promotion de leur recours et de leur usage dans les entreprises et les administrations nationales et communautaires.

La **circulaire du Premier ministre « Usage du logiciel libre dans l'administration » de septembre 2012** constitue une première reconnaissance par l'État de l'intérêt du logiciel libre pour les structures publiques. « *Moindre coût, souplesse d'utilisation, levier de discussion avec les éditeurs* » sont ainsi énumérés et font l'objet d'amples développements.

Toutefois, de l'avis des communautés de soutien, ce texte n'irait pas assez loin, notamment sur la question des standards ouverts[2] et de la généralisation de ce type de logiciels.

Continuer de progresser dans la voie du logiciel libre signifie aujourd'hui, pour les pouvoirs publics, **favoriser une migration progressive d'une partie croissante de leur parc informatique vers les logiciels libres**. Cela peut passer, notamment, par une préférence pour les logiciels libres dans les procédures d'appel d'offre des achats publics ainsi que par l'imposition de standards ouverts.

D'autres pays vont encore plus loin, comme l'Italie qui, ainsi que l'a rapporté M. Roberto di Cosmo, a publié une circulaire **imposant à toutes les administrations des règles draconiennes en faveur des logiciels libres**. La responsabilité des fonctionnaires, notamment, peut être invoquée s'ils recourent à un logiciel propriétaire alors qu'il existe un logiciel libre équivalent.

---

[1] *Et qui a abouti début mai à la condamnation de l'entreprise sud-coréenne par un jury de San José, en Californie, à verser à sa rivale américaine 119,6 millions de dollars de réparation pour avoir violé ses brevets.*

[2] *Protocoles ou formats de données dont les spécifications techniques sont publiques et ne peuvent faire l'objet d'aucune restriction de mise en œuvre.*

En outre, il paraîtrait de bonne politique d'**encourager l'usage des logiciels libres dans les enseignements informatiques**. Basé sur l'ouverture et la collaboration, valeurs en phase avec la démarche scientifique, le logiciel libre peut être étudié librement de droits. Et la formation supérieure aux méthodes de création de logiciels libres peut conduire à d'importants débouchés professionnels.

À cet égard, ainsi que l'a souligné M. Roberto di Cosmo, « *il faut aussi avoir les compétences pour se servir des logiciels libres. Je l'observe en permanence : tous les étudiants en informatique trouvent un emploi presque immédiatement*. »

Proposition n° 43 : encourager le développement des logiciels libres par leur intégration dans les marchés publics et par l'imposition de standards ouverts, à condition de développer les compétences pour l'utilisation de ces logiciels et standards.

b) Affirmer la place de l'Union européenne dans les organes de standardisation

(1) La standardisation, un enjeu allant bien au-delà de considérations purement techniques

La question des standards revêt une **importance, dans la gouvernance mondiale de l'Internet, allant bien au-delà d'un simple enjeu technique**. Leur définition répond en effet à des considérations d'ordre politique et économique, qui excèdent donc largement la simple mise au point de protocoles.

D'une façon générale, le rapport Revel sur l'influence normative de la France souligne combien « *le numérique met en jeu des options juridiques et politiques dans toutes les industries* » et comment « ***la gestion du numérique mêle inextricablement le technique et le politique**, le privé et le public et demande une doctrine de l'État et une stratégie à long terme, qui pourrait passer aussi par la normalisation*[1] ».

Ainsi que le souligne M. Jérémie Zimmermann, « *les décisions d'ordre technique sont prises par l'IETF et le W3C, organes de standardisation, or elles ont un impact réel sur l'Internet au jour le jour, sur la structuration du réseau* ». En outre, ajoute-t-il, ces « *organes de standardisation de l'Internet sont étroitement encadrés par la NSA, sous prétexte de préoccupations techniques, comme cela a été le cas pour l'IPsec* (Internet Protocol Security). *Il faudrait donc* ***davantage prendre en compte la nature politique de ces standards***. »

Selon le rapport Revel, ces organes de standardisation sont d'une importance majeure et il est « *nécessaire d'y être car les* ***protocoles techniques sont parfois des choix qui ont des conséquences sur les citoyens*** ».

Pour M. Pierre-Jean Benghozi également, « *l'IETF, l'organisme de standardisation des protocoles Internet, a […] soulevé bien des critiques* », dont celle

[1] Développer une influence normative internationale stratégique pour la France, *rapport de Mme Claude Revel à Mme Nicole Bricq, ministre du commerce extérieur, décembre 2012.*

consistant à s'inscrire dans un « ***environnement de régulation axé sur la technique alors que les enjeux peuvent aller bien au-delà**, et se chiffrent en milliards de dollars* ».

Or, il existe une **asymétrie d'influence entre un État et le reste du monde dans la définition de ces standards**. Ainsi que le pointe Mme Pauline Türk, le « World Wide Web consortium *(W3C) rassemble quatre cents entreprises partenaires ; sa gestion relève du* Massachusetts Institute of Technology *(MIT). Les standards développés par l'*Internet engineering task force *(IETF) sont également issus du monde anglo-saxon.* »

Cette surreprésentation de l'influence anglo-saxonne, et nord-américaine plus précisément, va de pair avec une **présence trop diluée des représentants européens et nationaux**. Comme le constate M. Mathieu Weill, l'AFNIC prend part aux « *forums de standardisation tels que l'IETF, avec quelques autres acteurs français tels que Orange et l'Université Paris 6, sur des questions de réglementation technique et de sécurisation des données personnelles* ». Or, ajoute le directeur général de l'AFNIC, « *sur 2 000 participants internationaux, nous envoyons deux ingénieurs, pour vous donner une idée de la faible participation française* ».

Ainsi que le souligne le rapport Revel d'une façon plus générale, notre pays est représenté dans ces instances « *surtout [par] des chercheurs de très haut niveau qui y contribuent en scientifiques désintéressés économiquement et politiquement. Ils n'ont pas d'objectifs industriels, qu'on ne leur a pas donnés du reste. Les Américains et les Chinois y vont avec des feuilles de route et des instructions dans le but de **promouvoir leurs industries, leurs groupes, leurs normes**.* »

(2) L'importance d'une présence européenne dans les enceintes de standardisation

La présence européenne dans les structures élaborant les standards de l'Internet est essentielle, car la bataille des normes conditionne – en partie au moins – toutes les autres. Autant l'Europe est très présente sur le front de la protection des libertés individuelles, à travers des structures institutionnelles dédiées, autant la régulation par les normes **– la *smart regulation* – lui fait défaut** en matière industrielle.

Comme le souligne Vincent Champain, « *la régulation, au niveau européen, n'est pas homogène. Il existe autant de spécifications que de pays. En matière de normes, on a raté le coche.* » Or, il y a là une problématique économique d'une importance première, pour laquelle **l'Europe aurait intérêt à se rapprocher des États-Unis afin de déterminer ensemble les standards de demain**, qui seront ensuite repris par le reste de la planète. « *Nos normes ne s'imposeront pas si nous jouons seuls* », souligne Vincent Champain. « *L'enjeu central est bien […] d'avoir, en copropriété avec les Américains, des normes susceptibles de s'imposer par la masse critique.* »

- **La standardisation de l'Internet en tant que tel**

Ce besoin de « plus d'Europe » dans l'établissement des normes et standards de demain vaut, bien sûr, pour ce qui est de la régulation du net dans son acception la plus stricte.

De **nombreux organismes participent à l'élaboration des standards de l'Internet** – comme le W3C, l'*Open Grid Forum* (OGF), l'*Institute of Electrical and Electronics Engineers* (IEEE), l'*European Telecommunications Standards Institute* (ETSI), l'*Internet Engineering Task Force* (IETF) ou l'*Union internationale des télécommunications* (UIT). Ces trois derniers méritent que l'on s'attarde plus spécifiquement.

L'ETSI a mis sur pied un comité technique Cybersécurité (TC CYBER) en avril dernier. Il travaillera en étroite collaboration avec l'ensemble des acteurs du secteur, en interne et en externe, pour collecter, identifier et spécifier les besoins dans le domaine. Ce travail permettra à l'ETSI de développer les normes adéquates et d'améliorer la protection de la vie privée et la sécurité des entreprises et des particuliers au sein de l'Europe. Plus de 100 organisations provenant de l'industrie et du monde académique ont déjà manifesté leur intérêt de rejoindre ce nouveau comité technique.

Quant à l'**IETF**, il **occupe une place spécifique dans la standardisation de l'Internet**. Il s'agit, on l'a vu plus haut, d'une organisation ouverte où les participations sont individuelles et libres, mais où leur poids est directement lié à la capacité d'agir et à la qualité des propositions de protocoles formulées. L'objectif premier de l'IETF est de produire des spécifications de protocoles appelées RFC les plus efficaces, les plus simples et les plus lisibles possibles. Pour cela, quelques règles simples sont mises en œuvre, telles que la discussion et la publication de ses documents.

À titre indicatif, l'IETF produit environ 250 RFC par an, dont la moitié de propositions de standards. Chaque année, deux à trois de ces propositions deviennent des standards aboutis ayant un caractère obligatoire. L'implication de la France est notable dans ce processus et représente 4 % de cette production à travers des auteurs issus du monde académique et industriel (France-Telecom, Orange, INRIA, AFNIC, Alcatel Lucent, Renater, SFR, Bouygues Telecom, Institut Telecom…).

Enfin, l'UIT est organisée en trois groupes de travail, dont l'un, l'**UIT-T, traite des questions techniques et de normalisation**. L'UIT-T produit principalement des recommandations ; plus de 3 000 d'entre elles sont en vigueur à l'heure actuelle. Elles constituent des normes qui définissent les modalités d'exploitation et d'interfonctionnement des réseaux de télécommunication. Bien que non contraignantes, elles sont généralement respectées en raison de leur qualité élevée, et du fait qu'elles garantissent l'interconnectivité des réseaux et permettent de fournir des services de télécommunication dans le monde entier.

Un accord de coopération a par ailleurs été conclu entre le CEN (Comité européen de normalisation), **le CENELEC** (Comité européen de normalisation en électronique et en électrotechnique) **et l'ENISA** (Agence européenne chargée de la

sécurité des réseaux et de l'information), en juillet 2013, pour travailler ensemble au cours des années à venir sur un ensemble de questions liées à la cybersécurité et à la normalisation.

Le rapport Revel s'interroge, à ce niveau très général de « régulation du web », sur l'opportunité d'**organiser à l'échelon ministériel une rencontre régulière entre dirigeants privés et publics sur la question de la normalisation**, pour envisager une stratégie d'ores et déjà européenne, à visée internationale. Il préconise d'y associer l'APIE (Agence du patrimoine immatériel de l'État), du fait des aspects « protection des données » et « propriété intellectuelle ».

En tout état de cause, il est **impératif pour l'Union européenne de « pousser » à la prise en compte de ses critères de standardisation**, que ce soit au moyen d'instances européennes dédiées (ETSI) ou dans des organisations internationales (IETF, UIT).

Proposition n° 44 : conforter, au service d'objectifs industriels, la présence de l'Union européenne dans les grandes instances internationales de standardisation de l'Internet et développer les travaux menés par les organisations spécifiquement européennes en ce domaine.

- **La standardisation des secteurs et technologies liés à l'Internet**

Mais au-delà de cette coordination très générale, il conviendrait que l'Europe et la France s'intéressent de plus près à **tous les « micro-enjeux » de standardisation d'un niveau inférieur, qui peuvent se révéler également cruciaux** pour l'avenir de notre industrie et de nos emplois.

Cette analyse a été clairement faite par Mme Valérie Peugeot devant la mission. Selon elle, « *les acteurs européens gagneraient également à* ***investir davantage les espaces où se construisent les normes et les protocoles de demain, dans lesquels ils sont sous-représentés****. J'ajoute que c'est dans des domaines nouveaux comme l'Internet des objets ou de la ville intelligente que se construisent les standards de demain : en l'absence d'espace de gouvernance, ce sont les entreprises américaines qui tirent le processus. Si bien que l'on risque de voir disparaître les standards ouverts, interopérables, qui ont présidé à la création de l'Internet et fait la philosophie originaire du web, qui mérite d'être préservée.* »

L'exemple de l'Internet des objets est à cet égard éclairant. Cette filière va acquérir un poids substantiel dans l'économie : d'après les dernières prévisions publiées par le cabinet d'études Gartner[1], le monde devrait recenser 26 milliards d'objets connectés à l'Internet à l'horizon 2020, pour un marché qui pèserait alors quelques 300 milliards de dollars. Or, ainsi que le souligne M. Daniel Nabet, président du Centre national de référence RFID (CNRFID), « *aujourd'hui encore,* ***trop peu d'entreprises et d'organisations françaises et européennes sont présentes dans les instances de normalisation****, pour définir et influencer les standards de*

[1] *http://technologies.lesechos.fr/revue-de-web/26-milliards-d-objets-connectes-en-2020_a-42-1072.html*

demain, ce qui place notre pays et notre continent dans une position de suiveurs par rapport à des règles définies par d'autres[1] ».

La première version du standard ONS *(Object Naming Service)*, service de nommage pour les objets de l'Internet, a été mise en oeuvre en 2008 par la société VeriSign, qui est également à l'origine du système DNS. Il a fallu **près de cinq ans de travaux conjoints, menés principalement par des acteurs français**, notamment GS1 France[2], Orange, l'INRIA et l'AFNIC, **pour aboutir à l'adoption d'un nouveau standard** – dit ONS 2.0 – s'appuyant sur un système fédérant plusieurs racines, évitant ainsi une dépendance stratégique supplémentaire de l'Europe vis-à-vis des États-Unis. Or, **les États-Unis risquent de reprendre les devants**, car ils viennent de regrouper les grands acteurs américains du secteur – IBM, Intel, Cisco, AT&T et General Electrics – en une structure, l'*Industrial Internet Consortium*, mise sur pied avec la coopération du gouvernement américain.

Selon M. Daniel Nabet, il faut impérativement « *se préoccuper fortement du développement et de la gouvernance de l'Internet des objets, en* ***s'appuyant sur les atouts de notre pays dans ce domaine*** *: culture scientifique de haut niveau, ingénieurs de grande qualité et dynamisme de nos entrepreneurs, mais également qualité de la réglementation sur la protection de données et de la vie privée, qui peuvent devenir le levier d'une politique industrielle ambitieuse* ». Le groupe de travail « objets connectés industriels » mis sur pied dans le cadre des 34 plans de la « Nouvelle France industrielle » serait à cet égard une instance particulièrement adaptée, pour ce qui est de l'échelon national.

M. Louis Pouzin a également appelé à investir l'Internet des objets connectés, qui représente des masses d'information considérables et amenées à croître très rapidement. « *C'est un domaine très flou, qui n'a pas encore été absorbé par Facebook ou Google. C'est là qu'il faut se positionner et mettre une organisation en place* », a-t-il estimé. Il s'agirait, selon lui, d'**inciter les différents métiers échangeant continuellement des données à instaurer un système de normalisation, avec les bases correspondantes**, comme le fait GS1 pour les codes-barres ou la radio identification (RFID). Ceci permettrait la constitution d'un écosystème servant à la normalisation de certains modes de gestion des étiquettes ou des identifiants, afin qu'ils puissent circuler, soient reconnus de façon généralisée, sécurisés, et puissent évoluer.

Proposition n° 45 : veiller à la mise en place en Europe d'un système de normalisation des objets connectés afin de favoriser leur reconnaissance mutuelle, leur interconnexion et leur sécurité à l'encontre d'attaques extérieures.

La même insuffisance de *leadership* européen se retrouve dans un autre secteur prometteur : les *smart grids*, ou réseaux intelligents, dont le chiffre

[1] *« La gouvernance, facteur clé pour le leadership européen sur le futur Internet des objets », chronique parue dans le* Journal du Net *du 26 mai 2014.*

[2] *Émanation nationale de GS1, organisme mondial actif dans la normalisation des méthodes de codage utilisées dans la chaîne logistique.*

d'affaires devrait doubler d'ici 2020 pour atteindre 55 milliards d'euros chaque année, selon un rapport du cabinet Navigant Research paru en janvier dernier[1]. « *En France comme en Europe, si l'on parle des compteurs et des réseaux concernant les clients individuels,* ***aucune position politique de principe ne semble prise*** », déplore ainsi le rapport Revel, qui conclut qu'« *un renforcement de la prise en main du sujet à l'Union européenne semblerait opportun* ». Estimant qu'il s'agit là « *d'un sujet hautement politique, mêlant libertés individuelles, équipements électriques industriels et économies d'énergie, où* ***l'Union pourrait jouer pleinement son rôle*** », il juge que notre pays « *devrait s'organiser pour apporter un contenu, à déterminer avec les industriels et services concernés* ».

Enfin, dernier exemple de secteur industriel dont l'avenir économique se joue dans la définition des standards et normes, celui de l'identité numérique. M. Vincent Champain, qui a participé au projet IDéNum, visant à retenir une norme d'authentification pour les usages commerciaux, observe « *qu'en [la] matière […], on s'attache beaucoup plus, en Europe, aux questions qui touchent à Schengen qu'aux questions industrielles. Or, l'identité numérique, c'est aussi l'accès à différents usages, comme la banque, avec le cryptage que cela suppose* ». En ce domaine également, l'Europe aurait une « carte à jouer », à condition qu'elle s'organise de façon efficace pour élaborer les standards de demain.

Proposition n° 46 : renforcer la présence européenne dans les structures de standardisation des technologies industrielles recourant à l'Internet (réseaux intelligents, identité numérique…) et en faire un véritable enjeu économique.

c) S'atteler à dessiner l'Internet du futur

- **Le futur Internet, un enjeu technologique fondamental qui se prépare dès aujourd'hui**

De l'avis de plusieurs des personnes auditionnées, l'Internet que l'on connaît aujourd'hui serait arrivé en « fin de vie » et devra tôt ou tard, du fait de son obsolescence, être remplacé par un nouveau dispositif.

« ***Le web 2.0 atteint ses limites*** », a ainsi annoncé M. Bernard Stiegler, et ceci pour plusieurs raisons. Parce que « ***l'opinion publique se retourne*** », comme le montre l'exemple de Facebook, à propos duquel « *ce qui était positif devient négatif* ». Également parce que, ainsi que le montre M. Frédéric Kaplan, chercheur à l'école polytechnique de Lausanne, cité par M. Bernard Stiegler, **le système est « *devenu entropique* :** *dès lors que les annonceurs ont pris le dessus sur les contributeurs du réseau, la hiérarchie sémantique qui commande les moteurs de recherche devient toujours plus étroite, le langage lui-même s'appauvrit, et avec lui l'orthographe – et à mesure que la dysorthographie se répand, voyez comment on écrit aujourd'hui les mails, les moteurs de recherche eux-mêmes perdent en précision et pourraient devenir parfaitement inefficaces, saturés par leur propre entropie* ».

[1] *http://www.navigantresearch.com/newsroom/utility-spending-on-smart-grid-it-systems-will-reach-nearly-20-billion-by-2022*

« *Conçu pour créer un espace de débat entre scientifiques et savants, pour débattre d'idées* », l'Internet se meurt, selon M. Bernard Stiegler, d'être « *devenu le principal vecteur du business mondial* » et de ne plus constituer le lieu d'échange, d'information et de débat qu'il était à l'origine. Afin de mieux identifier les « apporteurs de contenus » et de mieux comprendre les processus de construction du savoir sur l'Internet, M. Bernard Stiegler propose de **réintroduire de « *l'herméneutique* », à travers une « *traçabilité des contributions* »**. Cette approche permettrait selon lui de rétablir « *un débat sur les sources et finalement la diversité des savoirs elle-même* ».

Pour M. Louis Pouzin, l'archaïsme de l'Internet tient à sa conception, qui date désormais et ne permet plus de garantir le respect des droits des internautes. « ***Un des gros problèmes réside dans le fait que le système Internet TCP/IP a aujourd'hui quarante ans. C'est le plus ancien, et on peut considérer qu'il est à présent obsolète***. *Rien ne permet d'assurer la sécurité, l'authentification, la duplication des flux, ou le multilinguisme. […] Ce système a été construit comme un système qui fonctionne bien si l'on n'essaye pas de le casser. À partir du moment où le commerce est passé par là et, du même coup, la criminalité, le système est devenu extrêmement vulnérable, au moins à un certain niveau de fonctionnement*. »

Si l'Internet actuel est parvenu à son terme, alors il faut lui en substituer un nouveau, adapté aux évolutions les plus récentes des pratiques et de l'environnement. Or, selon M. Louis Pouzin, « ***il n'existe pas de projet européen pour le remplacer. C'est pourtant le bon moment, car cette situation ne se présente qu'une fois tous les quarante ans***. *On a laissé passer le premier cycle, dans les années 1970-1980, et les États Unis ont ainsi eu le champ libre. Si on ne fait rien maintenant, on est à nouveau reparti pour un cycle qui va durer 20, 30 ou 40 ans ! Il faudrait un projet ciblé, comme Eureka en Europe autrefois. Actuellement, on ne fait que de l'arrosage* ».

M. Louis Pouzin relève **trois types d'obstacles différents à l'avènement d'un nouvel Internet** à l'initiative de l'Europe. Le premier tiendrait au conservatisme de « *ceux qui font aujourd'hui tourner l'Internet* » : ils en retirent des intérêts financiers substantiels et ne seraient pas prêts à s'engager dans un nouveau modèle tant qu'ils n'en connaîtraient pas le contenu. Le deuxième frein résiderait dans la démographie des techniciens qui « *pour la plupart, ne sont pas tout jeunes* » et, pour les plus vieux du moins, « *n'ont pas envie que les choses bougent* ». Enfin, le dernier obstacle a trait au « *risque* » que présente toute nouveauté, qui ne peut aller « *sans un certain nombre de surprises, ou de points à corriger* ».

À bien y regarder cependant, l'idée d'un nouvel Internet, ou d'un « futur Internet », ainsi qu'il est appelé le plus souvent, circule activement dans les communautés concernées. M. Louis Pouzin reconnaît ainsi que « ***le futur Internet (FI) est maintenant partout*** *dans les milieux scientifiques, techniques, et ceux qui financent la recherche. Il est aussi dans les programmes de la Commission européenne*. » Le problème, ajoute-t-il, est qu'« *on ne s'en sert pas correctement* ».

Le **web 3.0**, qui désigne la version ultérieure du web 2.0 et constitue l'étape prochaine du développement du *World Wide Web*, constitue une partie importante de cet Internet du futur. Cependant, **son contenu exact fait l'objet de discussions**, chacun l'utilisant pour désigner sa vision du futur de l'Internet : « web sémantique » pour certains, des objets pour d'autres, de la 3D pour d'autres encore… Quel qu'il soit, l'Internet du futur sera l'objet d'un **nouveau protocole, IPv6**, dont le développement est inéluctable pour répondre aux besoins de croissance du net. Ce protocole réseau de nouvelle génération, dont le déploiement a commencé, devrait supplanter à terme l'actuel protocole, IPv4, victime d'une pénurie d'adresses IP dans le monde.

- **Une nécessaire « montée en puissance » de la France et de l'Europe**

L'Europe n'est pas absente de ce débat sur l'Internet du futur, mais il est vrai que **ses travaux sont loin d'aboutir pour l'instant**. L'impulsion est venue de la Commission européenne, qui a publié le 29 septembre 2008 une **communication sur les réseaux et l'Internet du futur**.

Début mars 2011, la vice-présidente de la Commission européenne, chargée de la stratégie numérique, Mme Neelie Kroes, avait confié **trois groupes de travail** à MM. Jean-Bernard Lévy, président du directoire de Vivendi, René Obermann, président-directeur-général de Deutsche Telekom, et Ben Verwaayen, directeur général d'Alcatel-Lucent, **sur la physionomie de l'Internet du futur en Europe**. Mais la commissaire, à qui les travaux avaient été remis en juillet de la même année, avait indiqué que la discussion « *n'[avait] pas débouché sur un consensus* ».

En France, le sujet est à l'ordre du jour politique depuis le précédent Gouvernement. La secrétaire d'État à l'économie numérique, Mme Nathalie Kosciusko-Morizet, avait lancé le 20 mai 2008 une **consultation publique sur l'Internet du futur**, en collaboration avec la ministre de l'enseignement supérieur et de la recherche, Mme Valérie Pécresse, et le secrétaire d'État chargé de l'industrie, M. Luc Chatel. L'objectif de cette consultation était d'identifier les évolutions possibles de l'Internet pour définir un plan d'actions « *destiné à positionner favorablement la France dans le développement de l'Internet du futur, et favoriser ainsi les retombées économiques et industrielles pour notre pays* ».

Malgré la multiplication d'initiatives, il ne se dessine pas d'orientation claire autour d'un Internet du futur ni au niveau national ni au niveau européen ; ce dernier niveau étant pourtant le plus pertinent au regard de l'ampleur du sujet.

Dans le milieu de la recherche et de l'industrie, plusieurs projets touchant à l'Internet du futur sont actuellement portés.

SystemX, l'institut de recherche technologique francilien dédié à l'ingénierie des systèmes du futur, a ainsi lancé, le 6 mai dernier, un nouveau programme de recherche baptisé « projet ARE » (architecture de réseaux). Ce projet s'insère dans le cadre du partenariat qui l'unit au Lincs (*Laboratory of information, networking and communication*), lequel rassemble le groupe Alcatel-

Lucent, l'INRIA, l'Institut Mines Telecom ainsi que l'université parisienne Pierre et Marie Curie.

Constatant que l'architecture de l'Internet, conçue il y plus de trente ans, n'est plus idéalement adaptée aux applications d'aujourd'hui et répond de plus en plus difficilement à la croissance du trafic, ce projet entend « *développer de nouvelles solutions pour l'Internet du futur en repensant l'organisation du réseau, la distribution et l'implémentation de ses fonctions, afin de définir une architecture répondant mieux aux exigences des multiples acteurs* ».

Par ailleurs, le **projet FIT** (« *Future Internet of Things* »), l'un des 52 projets lauréats de la première vague d'appel à projets « Équipements d'excellence » (Equipex)[1], vise à développer une plateforme expérimentale globale au travers de la fédération d'infrastructures, compétitive au niveau mondial, et comprenant une large base d'utilisateurs. Il est censé donner aux acteurs de l'Internet français un moyen d'expérimenter avec des réseaux mobiles sans fil dans les couches réseau et applicatives, accélérant ainsi la conception de technologies avancées pour l'Internet du futur.

Si l'Europe et la France ne sont donc pas inexistants dans la préparation du futur Internet, il **convient d'accélérer l'investissement en ce domaine afin d'être aux avant-postes de cet environnement qui conditionnera le monde de demain**. Nous possédons les compétences techniques indispensables pour faire émerger des solutions d'avenir, mais aussi un important capital de crédibilité et de confiance quant à la prise en compte des libertés individuelles et du respect des données privées. Reste à mieux coordonner les projets existants et à leur donner l'appui politique qui assoira leur développement.

Proposition n° 47 : préparer l'Internet du futur par une coordination plus poussée des initiatives et un soutien aux solutions mettant en avant la préservation de la confidentialité sur le réseau.

D. PROMOUVOIR UNE APPROPRIATION CITOYENNE DE L'INTERNET

Lors de son audition par votre mission d'information, M. Louis Joinet, ancien directeur juridique de la Commission nationale de l'informatique et des libertés, déclarait : « *la transparence passe par la participation de la société civile à la protection des données*. » Rejoignant ce constat, votre mission a souhaité explorer les pistes permettant une meilleure appropriation de l'Internet par les citoyens européens.

Partageant la conviction de M. Louis Joinet selon laquelle « *il est plus intéressant d'éduquer les opinions que de provoquer des débats de spécialistes* », votre

[1] *Projets financés par le programme des « investissements d'avenir » et destinés à améliorer les équipements des laboratoires de recherche scientifique français*.

mission estime indispensable de développer les compétences numériques de chacun et ce, dès le plus jeune âge.

Ainsi formés, les citoyens n'en seront que plus sensibles aux questions de protection de la vie privée sur l'Internet, donc plus exigeants à l'égard de leurs représentants s'agissant de l'encadrement démocratique des activités de renseignement.

Votre mission souhaite enfin inverser la tendance dénoncée par M. Louis Joinet qui regrettait que les États européens se soient jusqu'à présent montrés peu enclins à faire participer la société civile dans le domaine de la gouvernance. Aussi préconise-t-elle une meilleure association de la société civile tant à la réflexion politique qu'à l'action diplomatique.

1. Sensibiliser les citoyens aux libertés numériques et former à la programmation

D'après une enquête parue en mars 2014[1], **75 % des Français estiment que les cours d'informatique et de sciences du numérique doivent être proposés avant la terminale**. Cette opinion rejoint l'avis exprimé dans un rapport publié en mai 2013 par l'Académie des sciences[2], ou encore, plus récemment, dans une lettre ouverte adressée en février 2014 au Président de la République, cosignée par des universitaires et d'autres personnalités, notamment deux anciens Premiers ministres, MM. Lionel Jospin et Michel Rocard[3]. Un collectif avait même été constitué à l'automne 2013, notamment autour de la Commission nationale de l'informatique et des libertés (CNIL), pour demander que l'éducation au numérique soit reconnue grande cause nationale pour 2014, sans toutefois que cette initiative aboutisse[4].

Ainsi, **la volonté de développer l'enseignement du numérique dans notre pays paraît largement partagée**. Elle se justifie par **deux enjeux majeurs : la capacité à relever les défis d'une économie en mutation** et **l'éducation au respect de la vie privée** et à l'usage des données personnelles.

a) La formation au numérique : s'adapter à une économie de la connaissance

Comme l'a soutenu devant votre mission M. Roberto di Cosmo, « ***il ne faut pas voir dans l'informatique la voie de délestage*** *pour les bras cassés des autres filières, alors que c'est le domaine sur lequel se fonde notre futur* ». Lors de son audition, M. David Fayon n'a pas dit autre chose, relevant que « ***nous n'avons pas***

---

[1] *Deuxième édition du baromètre INRIA-TNS-Sofres sur les Français et le numérique, publiée le 11 mars 2014.*

[2] L'Enseignement de l'informatique en France. Il est urgent de ne plus attendre. *http://www.academie-sciences.fr/activite/rapport/rads_0513.pdf*

[3] *Lettre publiée en février 2014 à l'initiative de la Société informatique de France. http://www.epi.asso.fr/revue/docu/d1402b.htm*

[4] *Voir notamment sur le site de la CNIL : http://www.cnil.fr/linstitution/actualite/article/article/education-au-numerique-grande-cause-nationale-2014/*

de culture numérique *: à l'école, l'anglais est enseigné dès la maternelle, mais le numérique est absent jusqu'en Terminale, et encore c'est une option ! Nous abordons une nouvelle frontière numérique, sans nous mobiliser du tout. Les citoyens doivent comprendre ce qu'est un algorithme, un référencement naturel, quels sont les impacts de la géolocalisation, pour avoir des choix éclairés*. »

Il existe un risque réel de décrochage de l'Europe vis-à-vis du reste du monde, « *au moment même où outre-Atlantique le Président Obama affirme que chaque Américain devrait faire une heure de code par jour* », comme l'indiquait Mme Isabelle Falque-Pierrotin au cours de son audition.

L'enseignement du numérique doit concerner tous les élèves, aussi bien ceux qui se destinent à des carrières dans ces domaines que les autres. Au sujet des premiers, plusieurs des personnalités entendues par votre mission ont déploré qu'ils ne soient pas plus nombreux. M. Hervé Collignon a ainsi rappelé les faibles effectifs des « *ingénieurs diplômés en sciences dures – mathématiques, physique, technologie, informatique : 17 % des étudiants européens, contre 30 % à Taïwan ou en Chine, laquelle produit chaque année 700 000 diplômés dans ces disciplines contre 500 000 pour toute l'Europe* ». Quant à Mme Gabrielle Gauthey, elle a complété ainsi ce constat : « ***la France dispose de bons ingénieurs, mais en nombre insuffisant****, d'autant que 40 % des diplômés des grandes écoles partent à l'étranger pour leur premier poste : reviennent-ils par la suite ? La crise des vocations scientifiques touche tout l'Occident, la diffusion de la culture scientifique et technique doit être un combat*. » Comme le précisait M. Loïc Rivière au cours de la même réunion, ces lacunes entraînent « *une pénurie de certains profils, en particulier de développeurs et d'intégrateurs web* ».

Plus largement, tous les élèves, quelle que soit leur orientation professionnelle future, devraient acquérir des connaissances solides en matière numérique. Le 16 avril 2014, l'Office parlementaire d'évaluation des choix scientifiques et technologiques (OPECST) a organisé une série d'auditions ouvertes au public sur le thème de l'éducation au numérique. L'un des intervenants, Mme Sophie Pène, professeur en sciences de l'information et de la communication à l'Université Paris Descartes, envisageait dans un avenir proche la reconfiguration de nombreux emplois – avocat, professeur, médecin… – dans lesquels la part créative prendrait une importance croissante, dans une culture de la coopération, de la collaboration pair à pair favorisée par le numérique. Elle donnait l'exemple d'un archéologue, qui doit aujourd'hui maîtriser des algorithmes pour reconstituer des poteries cassées en morceaux. **La diffusion de ces techniques concernera donc à terme, de façon quotidienne, de plus en plus de métiers, pour lesquels une formation rudimentaire aux technologies de l'information et de la communication s'avérera insuffisante**. Le traitement des données, la conception de programmes requièrent bien un apprentissage.

b) Promouvoir un usage éclairé du numérique

L'éducation au numérique ne répond pas seulement à des besoins professionnels et économiques, elle relève d'une exigence civique. Comme

M. Laurent Sorbier en témoignait devant votre mission, « *l'action politique se heurte au fait que la conscience des citoyens et la mobilisation des décideurs face aux dangers d'Internet paraissent assez faibles, hormis la sphère assez spécialisée des activistes et des associations de défense des libertés ;* ***la dissémination des données personnelles provoque une faible inquiétude, en particulier chez les jeunes*** *: la génération qui nous suit a un rapport à l'intime très différent de celui des générations précédentes – on parle même de « l'extimité », ce désir de rendre visibles des aspects de soi qui sont considérés comme relevant de l'intimité : la jeune génération accepte une porosité entre l'intime et le public, là où nous voulions précisément une séparation. Des affaires montrent combien les jeunes n'en mesurent pas les conséquences* (…) »

Dans ce contexte, le développement d'une culture numérique commune à tous les élèves semble indispensable, ne serait-ce que pour avertir des risques multiples liés à l'Internet : perte de contrôle de données à caractère personnel, piratage, exposition à des sites dangereux, phénomènes de dépendance…

Le Sénat est conscient de cette nécessité depuis déjà plusieurs années. En 2008, à l'occasion de l'examen du projet de loi favorisant la diffusion et la protection de la création sur Internet[1], il avait adopté deux amendements, dont l'un de votre rapporteure visant à compléter l'article L. 312-9 du code de l'éducation **pour permettre d'informer les élèves**, notamment au collège, **des dangers du téléchargement illicite et du piratage des œuvres**[2].

En outre, le 23 mars 2010, il avait adopté en première lecture une **proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique**, notamment en promouvant de la part des élèves « *un comportement responsable dans l'utilisation des outils interactifs, lors de leur usage des services de communication au public en ligne* »[3].

Cette proposition de loi n'ayant jamais été inscrite à l'ordre du jour de l'Assemblée nationale, cette disposition a été introduite, par amendement de votre rapporteure[4], dans la loi n° 2011-302 du 22 mars 2011 portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière de santé, de travail et de communications électroniques. L'article L. 312-15 du code de l'éducation, relatif à l'éducation civique, a ainsi été complété par

---

[1] *Devenu la loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur Internet.*

[2] *Voir à ce sujet le rapport de la commission des affaires culturelles du Sénat (n° 53, 2008-2009) http://www.senat.fr/rap/l08-053/l08-053.html*
ainsi que les amendements n° 48 et 62 déposés en première lecture sur ce projet de loi respectivement par le rapporteur de la commission des affaires culturelles et par Mme Catherine Morin-Desailly.
http://www.senat.fr/amendements/2007-2008/405/Amdt_48.html
http://www.senat.fr/amendements/2007-2008/405/Amdt_62.html

[3] *Article 1er de la proposition de loi adoptée le 23 mars 2010 : http://www.senat.fr/leg/tas09-081.html*
Voir à ce sujet le rapport pour avis fait au nom de la commission des affaires culturelles du Sénat par Mme Catherine Morin-Desailly (n° 317, 2009-2010)
http://www.senat.fr/rap/a09-317/a09-317.html

[4] *Voir à ce sujet le rapport pour avis fait au nom de la commission des affaires culturelles du Sénat par Mme Catherine Morin-Desailly (n° 275, 2010-2011)*
http://www.senat.fr/rap/a10-275/a10-275.html

l'alinéa suivant : « *Dans le cadre de l'enseignement d'éducation civique,* ***les élèves sont formés afin de développer une attitude critique et réfléchie vis-à-vis de l'information disponible et d'acquérir un comportement responsable dans l'utilisation des outils interactifs lors de leur usage des services de communication au public en ligne****. Ils sont informés des moyens de maîtriser leur image publique, des dangers de l'exposition de soi et d'autrui, des droits d'opposition, de suppression, d'accès et de rectification prévus par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ainsi que des missions de la Commission nationale de l'informatique et des libertés.* »

c) Renforcer les dispositifs existants

Des dispositifs ont déjà été instaurés. **Le brevet informatique et Internet (B2i) a été créé en 2001, avant d'être généralisé en 2006**. Il ne s'agit pas à proprement parler d'un examen mais d'**une attestation des connaissances** acquises successivement à l'école, au collège puis au lycée. Pour chacun de ces trois niveaux, les enseignements s'articulent autour des cinq domaines mentionnés en annexes de l'arrêté du 14 juin 2006 relatif aux référentiels de connaissances et capacités exigibles pour le brevet informatique et Internet. Un arrêté pris le 24 juillet 2013, après la promulgation de la loi n° 2013-595 du 8 juillet 2013 d'orientation et de programmation pour la refondation de l'école de la République, a redéfini ces domaines en ce qui concerne le lycée. Les élèves doivent savoir : travailler dans un environnement numérique évolutif ; être responsables ; produire, traiter, exploiter et diffuser des documents numériques ; organiser la recherche d'informations ; communiquer, travailler en réseau et collaborer[1].

La loi n° 2013-595 du 8 juillet 2013 précitée a modifié l'article L. 312-9 du code de l'éducation, qui dispose désormais que : « *La formation à l'utilisation des outils et des ressources numériques est dispensée dans les écoles et les établissements d'enseignement ainsi que dans les unités d'enseignement des établissements et services médico-sociaux et des établissements de santé. Elle comporte une sensibilisation aux droits et aux devoirs liés à l'usage de l'Internet et des réseaux, dont la protection de la vie privée et le respect de la propriété intellectuelle*. »

Il est encore trop tôt pour mesurer les effets de cette réforme, susceptible de répondre en partie aux critiques généralement adressées à un brevet qui « *n'évalue pas la capacité de chacun à créer des contenus ni à travailler de façon collaborative sur Internet, deux compétences qui devraient pourtant être au cœur de la pédagogie numérique* », pour reprendre les termes du rapporteur du projet de loi d'orientation et de programmation pour la refondation de l'école de la République au Sénat[2]. Le député Jean-Michel Fourgous, qui s'était vu confier une mission sur

---

[1] *Arrêté du 24 juillet 2013 modifiant l'arrêté du 14 juin 2006*
http://www.legifrance.gouv.fr/affichTexte.do?categorieLien=id&cidTexte=JORFTEXT000027811513&dateTexte=

[2] *Rapport n° 568 (2012-2013) de Mme Françoise Cartron fait au nom de la commission de la culture, de l'éducation et de la communication du Sénat.*
http://www.senat.fr/rap/l12-568/l12-568.html

ce thème en 2011, avait été plus sévère encore, décrivant un enseignement qui « *se contente essentiellement de combattre les mésusages* »[1].

Outre le brevet informatique et Internet, les élèves qui le souhaitent peuvent suivre des enseignements du numérique à titre d'option, comme par exemple en classe de terminale scientifique.

Des progrès ont donc été accomplis récemment vers une meilleure prise en compte de l'ensemble des dimensions liées au numérique. Ils doivent être poursuivis pour que le numérique soit pleinement reconnu au sein des programmes scolaires. M. Pierre Léna, président de la fondation de coopération scientifique pour l'éducation à la science « La main à la pâte », présent lors de l'audition publique de l'OPECST organisée le 16 avril 2014, estimait qu'à terme il serait judicieux d'intégrer les connaissances en matière numérique au socle commun des compétences. **Cela supposerait toutefois de procéder par étapes pour former progressivement l'ensemble des 800 000 professeurs en fonction et pas seulement les nouveaux, ni même développer un enseignement ambitieux du numérique en garantissant sa place au cœur du socle commun des connaissances et des compétences et en formant progressivement l'ensemble des professeurs en fonction, des professeurs *ad hoc* qui contribueraient à maintenir le numérique en marge des disciplines traditionnelles.**

Proposition n° 48 : développer un enseignement ambitieux du numérique en garantissant sa place au cœur du socle commun des connaissances et des compétences et en formant progressivement l'ensemble des professeurs en fonction.

2. Renforcer l'encadrement légal des activités de renseignement et en améliorer le contrôle politique

a) Un double contrôle administratif et politique

Le contrôle des activités de renseignement est actuellement assuré en France par deux organes : une entité administrative, la Commission nationale de contrôle des interceptions de sécurité (CNCIS), et une entité politique, la Délégation parlementaire au renseignement (DPR).

Composée de trois membres – un magistrat qui la préside et deux parlementaires désignés par chacune des assemblées –, assistés de deux magistrats de l'ordre judiciaire, **la CNCIS est une autorité administrative indépendante qui a pour mission de garantir le secret des correspondances en s'assurant de la légalité des interceptions de sécurité mises en œuvre par les autorités administratives pour prévenir les atteintes aux intérêts fondamentaux**

[1] Apprendre autrement à l'ère numérique - *Rapport de la mission confiée à M. Jean-Michel Fourgous, député, sur l'innovation des pratiques pédagogiques par le numérique et la formation des enseignants, février 2012.*
http://www.missionfourgous-tice.fr/missionfourgous2/IMG/pdf/Rapport_Mission_Fourgous_2_V2.pdf

de la nation. Sont donc exclues de son champ d'intervention les interceptions effectuées par les services judiciaires pour constater des infractions et en rechercher les auteurs.

La triple mission de la CNCIS

La loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques a tout d'abord confié à la CNCIS le **contrôle de l'interception des correspondances émises par voie de communications électroniques**. À ce titre, la CNCIS émet un **avis** sur la légalité de l'interception autorisée au regard des cinq motifs légalement admis : la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous.

La procédure est la suivante : sur demande écrite et motivée des ministres de la défense, de l'intérieur, ou des douanes (ou d'une des deux personnes que chacun aura spécialement déléguées), le Premier ministre (ou l'une des deux personnes qu'il aura spécialement déléguées) prend une décision écrite et motivée d'autorisation pour une durée maximale de 4 mois, qui est communiquée à la CNCIS dans les 48 heures. Si la CNCIS juge que l'autorisation d'interception de sécurité n'est pas légale, elle recommande au Premier ministre d'y mettre fin et en informe le ministre demandeur et celui chargé des communications électroniques. Le Premier ministre informe sans délai la CNCIS des suites données à ses recommandations.

Dans le cadre de cette mission, la CNCIS procède à des contrôles et des enquêtes, de sa propre initiative ou sur réclamation de particuliers. Elle effectue ainsi des visites programmées ou inopinées des services utilisateurs d'interceptions.

À cette première mission, la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme a ajouté le **contrôle des demandes de communication des données de connexion conservées et traitées par les opérateurs, fournisseurs d'accès ou hébergeurs** (y compris les données relatives à la localisation des équipements terminaux utilisés). Initialement cantonnée aux agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales à la seule fin de prévention des actes de terrorisme, cette faculté a été étendue par la loi de programmation militaire du 18 décembre 2013[1], aux agents des services relevant des ministres chargés de la sécurité intérieure, de la défense, de l'économie et du budget pour des motifs et selon une procédure alignés sur ceux des interceptions de sécurité.

Enfin, la CNCIS est membre permanent de la Commission consultative dite « R 226 », créée par le décret n° 97-757 du 10 juillet 1997 et chargée d'émettre des **avis sur les demandes de commercialisation, d'importation, d'acquisition, de détention ou d'emploi des matériels susceptibles de porter atteinte au secret des correspondances**, autorisées par le Premier ministre.

[1] *Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.*

Créée par la loi du 9 octobre 2007[1], **la DPR est un organe commun à l'Assemblée nationale et au Sénat**, composé de huit membres, quatre députés et quatre sénateurs : les présidents des commissions des lois et de la défense de chacune des chambres sont membres de droit, les quatre autres membres étant désignés par les présidents des assemblées de manière à assurer la représentation du principal groupe de l'opposition. **La DPR assure un contrôle de nature très différente de celui exercé par la CNCIS : politique, ce contrôle ne porte pas sur l'opérationnel**, la communication de tout élément relatif aux opérations en cours ou aux procédures et méthodes opérationnelles étant expressément interdite par la loi. Depuis sa modification par la loi de programmation militaire du 18 décembre 2013, celle-ci lui confère la mission d'exercer « *le contrôle parlementaire de l'action du Gouvernement en matière de renseignement* » et d'évaluer « *la politique publique en ce domaine* ». À cet effet, la DPR est destinataire d'un certain nombre de documents, dont la partie confidentielle de la stratégie nationale du renseignement, mais ne peut être informée d'éléments portant sur « *les échanges avec des services étrangers ou avec des organismes internationaux compétents dans le domaine du renseignement* ».

b) Un cadre juridique dépassé

Le cadre juridique dans lequel s'inscrit l'intervention de la CNCIS, à savoir la loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques – désormais codifiée au sein du code de la sécurité intérieure –, **apparaît désormais inadapté face aux évolutions induites par l'Internet s'agissant de la nature des communications, des acteurs et des techniques**.

En premier lieu, le principe même de l'Internet, qui repose sur un protocole faisant fi du support matériel, conduit à ce qu'une même communication puisse emprunter différents types de canaux de diffusion – câbles, voies hertziennes ou satellitaires – qui obéissent chacun à des régimes juridiques distincts, lorsqu'il en existe un. Ainsi, 80 % des communications transitent actuellement par des câbles sous-marins ; les conventions internationales, telles celle de Montego Bay, ne précisent pourtant pas le régime juridique applicable à l'interception de ces communications.

Par ailleurs, la loi du 10 juillet 1991 avait été conçue pour encadrer l'interception du contenu des communications. Or, avec l'accès mobile à l'Internet, les données de connexion elles-mêmes, comme la géolocalisation de l'émetteur de la communication par exemple, sont devenues pertinentes, si bien que la loi du 23 janvier 2006 relative à la prévention du terrorisme a autorisé l'accès des services à ces données, à titre provisoire et à la seule fin de lutte contre le terrorisme. L'article 20 de la loi de programmation militaire du 18 décembre 2013 a pérennisé ce dispositif tout en alignant le régime du recueil des données techniques de communication sur celui des interceptions de sécurité tel que prévu par la loi du 10 juillet 1991.

[1] *Loi n° 2007-1443 du 9 octobre 2007 portant création d'une délégation parlementaire au renseignement.*

En deuxième lieu, la diversification et l'internationalisation des acteurs de l'Internet viennent bouleverser le schéma sur lequel repose le régime juridique en vigueur.

Afin de préserver au mieux les libertés, le régime juridique mis en place par la loi du 10 juillet 1991 a cloisonné les phases de l'interception en les confiant à des acteurs différents : les opérateurs privés de communication fournissent sur réquisition les données à un service de l'État qui en assure le traitement exclusivement administratif et technique, avant qu'elles ne soient transmises pour analyse aux services responsables de l'exploitation du renseignement. Ce régime reposant sur le principe de la réquisition aux opérateurs de communication exclut ainsi que les services de l'État effectuent eux-mêmes des interceptions de communication.

Certains opérateurs échappent néanmoins à ce cadre juridique. Les uns, pour des motifs historiques : apparus avec l'Internet à l'instar des fournisseurs d'accès et des hébergeurs, ils n'étaient pas visés par loi du 10 juillet 1991 qui leur est antérieure ; l'article 20 de la loi de programmation militaire du 18 décembre 2013 permet de remédier à cette situation à compter du 1er janvier 2015. Les autres, pour des motifs géographiques : la compétence de la norme étant territorialement circonscrite, il existe une incertitude sur les obligations légales auxquelles sont soumis les opérateurs étrangers.

En outre, certains outils – « chevaux de Troie », captation d'images informatiques, sonorisation, infiltration – permettent désormais de pratiquer des interceptions sans qu'il soit besoin de recourir aux opérateurs et services dédiés. Ces technologies recèlent donc de nouveaux risques d'atteinte au secret des communications, rendant nécessaire la définition de nouvelles modalités de contrôle.

En dernier lieu, l'évolution des techniques rend plus complexe l'identification des personnes et partant, du contrôle par la CNCIS de la pertinence des interceptions mises en place. L'Internet facilite l'anonymisation des émetteurs car il est plus difficile qu'en matière de téléphonie de connaître l'identité de la personne qui se trouve derrière une adresse IP, qui peut en outre être commune à plusieurs utilisateurs, comme les membres d'une même famille par exemple. À ce premier niveau de complexité s'ajoutent les différentes techniques d'anonymisation qui peuvent être mises en œuvre : recours à des « proxys anonymes » et autres WPA, utilisation du réseau TOR… La généralisation du chiffrement des communications, encouragée pour renforcer la confidentialité de celles-ci, pose en outre un nouveau défi aux services de renseignement.

c) Vers un renforcement du contrôle des activités de renseignement

Au-delà de l'ajustement opéré par la loi de programmation militaire du 18 décembre 2013, le besoin d'actualisation du cadre juridique des interceptions de sécurité est donc bien réel. Votre mission estime essentiel que les activités de

renseignements soient effectivement encadrées par une loi actualisée. Ainsi qu'il le rappelait dans l'avant-propos du 21ème rapport annuel de la Commission Nationale de Contrôle des Interceptions de Sécurité (CNCIS), son président, M. Hervé Pelletier, a, à plusieurs reprises, appelé de ses vœux une refonte des dispositions de la loi du 10 juillet 1991 ; il a d'ailleurs renouvelé cette demande lors de son audition devant votre mission d'information.

La première modification législative souhaitable serait d'aligner le droit sur le fait. Si la loi du 10 juillet 1991 prévoit que la CNCIS n'exerce qu'un contrôle *a posteriori* des autorisations d'interception, la pratique du contrôle préalable à la décision d'autorisation a été instaurée avec l'accord du Premier ministre dès les premiers mois de fonctionnement de la Commission. Ce contrôle *a priori* renforce indéniablement sa portée, en permettant en particulier un échange utile entre la Commission et les services et une meilleure prise en compte par ceux-ci des préconisations de la Commission. On observe d'ailleurs que l'avis de la CNCIS est suivi dans 99 % des cas. Cette pratique pourrait en outre être étendue au recueil des données de connexion.

Proposition n° 49 : inscrire dans la loi que l'avis de la Commission nationale de contrôle des interceptions de sécurité (CNCIS) est recueilli préalablement à la délivrance de toute autorisation d'interception de sécurité ou d'accès administratif aux données de connexion.

Déjà étendu au recueil des données de connexion par l'article 20 de la loi de programmation militaire du 18 décembre 2013, le contrôle de la CNCIS pourrait l'être également à de nouvelles techniques d'investigation si les services de renseignement obtenaient à l'avenir d'en être dotés : infiltration, sonorisation, captation d'images ou de données informatiques. Étant donné le risque d'atteinte aux libertés publiques et aux droits individuels que ces techniques spéciales d'enquête recèlent, un contrôle de la légalité de leur utilisation serait en effet indispensable.

À ce contrôle de légalité devrait en outre être ajouté explicitement un contrôle de la proportionnalité des moyens mis en œuvre eu égard aux objectifs poursuivis. Telle est la conclusion que votre mission tire de la décision de la Cour de justice de l'Union européenne invalidant la directive du 15 mars 2006 prévoyant l'obligation pour les fournisseurs de services de communications téléphoniques de conserver des données personnelles sans limitation, sans information et pour une durée maximum de deux ans (*cf. supra*). Selon votre mission en effet, en dépit des effets juridiques limités de l'invalidation de cette directive, cette décision de la CJUE invite chacun des États à une réflexion sur les pratiques de ses services de renseignement concernant la collecte et la conservation des données personnelles. Si, comme on l'a vu précédemment, les moyens techniques permettent désormais de stocker des quantités astronomiques de données, et si grande la tentation de les conserver le plus longtemps possible en vue d'un usage ultérieur soit-elle, **le droit au respect de la vie privée et familiale et le droit à la protection des données à caractère personnel doivent**

primer toute autre considération. **Il importe donc que le Parlement affirme solennellement son opposition à la surveillance de masse et mette la CNCIS en capacité de faire obstacle à une telle dérive.**

Si la CNCIS opère effectivement un contrôle de proportionnalité à l'occasion de son contrôle de légalité, il paraît donc nécessaire de le formaliser dans les textes.

Propositions n° 50 et 51 :

– prévoir automatiquement la consultation de la CNCIS préalablement à la mise en œuvre de tout moyen technique de collecte d'informations dont les services seraient dotés ;

– étendre explicitement le contrôle de la CNCIS à la proportionnalité des moyens mis en œuvre par les services de renseignement afin d'empêcher une dérive des activités de renseignement vers une surveillance de masse.

Cependant, **un tel accroissement des compétences de la CNCIS conduit à un renforcement indispensable des moyens à sa disposition, voire à sa transformation**.

À la suite de son déplacement à Berlin et de sa rencontre avec le député Hans-Christian Ströbele, la mission d'information s'est interrogée sur l'opportunité de la transposition en France du dispositif en vigueur en Allemagne qui confie à un organe du Bundestag – l'Organe de contrôle parlementaire – la surveillance des activités des services de renseignement, y compris opérationnelle. Ainsi, cet organe constitue pour la durée de la législature la « commission G 10 », dont les membres ne sont pas nécessairement des députés[1]. Cette commission est chargée de veiller au respect des dispositions de la loi relative au secret de la correspondance, de la poste et des télécommunications, garanti par l'article 10 de la Loi fondamentale : une interception de sécurité ne peut être décidée par le ministre de l'intérieur à la demande d'un service de renseignement sans l'approbation préalable de cette commission. La législation sur la lutte contre le terrorisme en vigueur de 2002 à 2012 avait en outre conféré à cette commission des pouvoirs décisionnels en matière de recueil de données de connexion par les services de renseignement.

Il n'a cependant pas semblé souhaitable à votre mission de fondre en une seule instance rattachée au Parlement les missions de contrôle opérationnel préalable des interceptions de sécurité, qui porte sur la légalité et la proportionnalité de celles-ci, et de contrôle politique de l'utilisation faite par le Gouvernement des services de renseignement, susceptible de déboucher sur une mise en cause de la responsabilité de l'exécutif. D'autant qu'instaurer un contrôle des activités opérationnelles par le Parlement risquerait de porter atteinte au principe de séparation des pouvoirs. Votre mission rejoint donc les conclusions de

[1] *À titre d'exemple, l'actuelle « commission G 10 » comprend quatre membres titulaires et quatre membres suppléants, dont deux sont des députés.*

la mission d'information de la commission des lois de l'Assemblée nationale sur l'évaluation du cadre juridique du renseignement, qui préconisait le maintien de deux entités, l'une administrative et l'autre politique.

Votre mission fait donc sienne la proposition de nos collègues députés visant à **la création, à partir de la CNCIS, d'une nouvelle autorité administrative indépendante, dont le champ de compétence serait élargi à l'ensemble des moyens de collecte d'informations utilisés par les services de renseignement** et baptisée « Commission de contrôle des activités du renseignement » (CCAR)[1]. Conformément à la recommandation de nos collègues députés, cette commission ne serait plus consultative mais décisionnelle : dans les cas où la mise en œuvre de moyens de recueil de renseignements serait soumise à autorisation, celle-ci serait accordée par le président de la CCAR sur demande écrite et motivée du Premier ministre, à l'initiative des ministres chargés de la sécurité intérieure, de la défense, de l'économie et du budget. Son contrôle porterait tant sur la légalité que sur la proportionnalité de leur mise en œuvre.

En revanche, votre mission s'interroge sur la composition proposée par nos collègues députés pour cette nouvelle autorité, qui ne comprendrait plus de parlementaires mais uniquement des magistrats administratifs et financiers, alors même que, comme le notait M. Hervé Pelletier lors de son audition, la présence en son sein de deux parlementaires, l'un de la majorité, l'autre de l'opposition, a pu apporter légitimité et autorité à la CNCIS. De même, l'absence de magistrats de l'ordre judiciaire parmi les personnels mis à disposition de l'autorité lui semblerait regrettable.

Proposition n° 52 : créer, à partir de la CNCIS, une nouvelle autorité administrative indépendante – la Commission de contrôle des activités du renseignement -, chargée de délivrer les autorisations de mise en œuvre des moyens de collecte d'informations après examen de leur légalité et de leur proportionnalité.

Parallèlement, les pouvoirs de la DPR seraient encore renforcés. Si la loi de programmation militaire du 18 décembre 2013 a d'ores et déjà intégré dans le droit positif une partie des recommandations formulées par nos collègues députés dans leur rapport de 2013, votre mission estime que d'autres propositions issues de ce rapport pourraient également l'être. En premier lieu, à l'instar de l'Organe parlementaire de contrôle du Bundestag, la DPR pourrait être dotée d'un pouvoir de contrôle sur pièces et sur place. En second lieu, la loi prévoirait que la DPR pourrait recourir en tant que de besoin aux services d'enquête de la CCAR.

Proposition n° 53 : renforcer les pouvoirs d'investigation de la Délégation parlementaire au renseignement (DPR) en la dotant d'un pouvoir de

[1] Cf. *le rapport d'information présenté par MM. Jean-Jacques Urvoas et Patrice Verchère au nom de la mission d'information de la commission des lois de l'Assemblée nationale sur l'évaluation du cadre juridique applicable aux services de renseignement (n° 1022, XIVe législature), 14 mai 2013.*

contrôle sur pièces et sur place et en prévoyant l'assistance des services de la Commission de contrôle des activités de renseignement.

Enfin, les fichiers des services de renseignement pourraient être soumis au contrôle de la Commission nationale de l'informatique et des libertés. À l'instar du contrôle qu'elle exerce sur les fichiers de police, la CNIL s'intéresserait uniquement aux fichiers en eux-mêmes, à leur sécurité, à leur durée de conservation ou aux conditions d'accès.

Proposition n° 54 : soumettre au contrôle de la Commission nationale de l'informatique et des libertés les fichiers du renseignement.

Un tel schéma combinant à la fois supervision du Parlement, intervention d'une autorité indépendante dotée de prérogatives effectives, et contrôle des données collectées par l'autorité de protection des données, correspond aux recommandations émises par le « G 29 »[1].

Un contrôle démocratique au niveau national ne suffit cependant pas. Comme l'expliquait M. Francesco Ragazzi à votre mission d'information, « *il s'agit bien plutôt d'un problème de contrôle démocratique sur un réseau transnational* ». En effet, si l'**échange de données entre services de renseignement** est justifié par la lutte contre de nouvelles formes de terrorisme et de criminalité, il permet de manière plus critiquable « *de contourner la loi quand elle interdit sur le territoire une surveillance de la population nationale* ». M. Jan Philipp Albrecht, député européen rapporteur pour la Commission LIBE de la proposition de règlement sur la protection des données personnelles, a également indiqué à votre mission d'information qu'il était nécessaire d'adopter des règles communes dans ce domaine. Cela permettrait de mettre un terme à la situation actuelle dans laquelle chaque État membre de l'Union européenne s'interdit d'espionner sa propre population mais obtient des renseignements sur celle-ci auprès de ses voisins, ce qu'Edward Snowden qualifiait de « bazar européen » lors de son audition par le Parlement européen.

Proposition n° 55 : établir un cadre européen de contrôle des échanges d'informations entre services de renseignement.

[1] "In order to ensure that intelligence services indeed do respect the limits imposed on surveillance programmes, meaningful oversight mechanisms need to be implemented in the laws of all Member States. This should include fully independent checks on data processing operations by an independent body as well as effective enforcement powers. Next to effective and robust parliamentary scrutiny, this could be done by a data protection authority or another suitable independent body […] If the oversight were to be carried out by another body, the Working Party encourages regular contacts between this body and the national data protection authority to ensure a coherent and consistent application of the data protection principles." *(Article 29 Data Protection Working Party,* Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes*, adopted on 10 April 2014, p. 8).*

3. Structurer la gouvernance des questions numériques aux niveaux national et européen

L'Internet n'est pas un secteur à proprement parler dans la mesure où il concerne tous les secteurs et pose des questions politiques au pouvoir en général. Aussi apparaît-il nécessaire d'instituer, à tous les niveaux, des structures qui lui sont dédiées afin de se saisir pleinement de cette problématique et de se l'approprier plutôt que de continuer à ne l'envisager que sur un mode défensif.

a) Créer des instances dédiées au sein des organes exécutifs et législatifs nationaux et européens

En confiant à Mme Neelie Kroes le portefeuille « Stratégie numérique » lors de sa nomination en 2009, la Commission européenne a acté le caractère transversal de la politique numérique. Cependant, comme le constatait votre rapporteure à l'issue de précédents travaux menés sur la question du numérique[1], cette initiative n'a pas trouvé d'écho au sein du Conseil de l'Union européenne, avec pour conséquence un **manque de vision politique de long terme** et un **traitement morcelé du défi numérique**.

Cette instance, qui partage avec le Parlement européen la fonction de législateur, siège en différentes formations réunissant les ministres des États membres compétents selon les sujets abordés. Or, à défaut de formation dédiée à la question numérique, plusieurs formations du Conseil se trouvent à traiter de sujets ayant trait à celle-ci sans en avoir jamais une vision globale : le Conseil Transports, Télécommunications et Énergie (TTE) pour les sujets liés aux réseaux numériques et à la société de l'information, le Conseil Affaires économiques et financières (ECOFIN) pour les questions de fiscalité, le Conseil Justice et Affaires intérieures (JAI) pour la protection des données, le Conseil Compétitivité (COMPET) pour les questions relevant du marché intérieur, de l'industrie, ou de la recherche, le Conseil Éducation, Jeunesse, Culture et Sport (EJCS) pour la dimension culturelle et éducative, le Conseil des Affaires étrangères (CAE) pour la sécurité de l'Union européenne et sa politique commerciale... La commissaire en charge du numérique n'a donc face à elle aucun pendant représentant les États membres, à même de recevoir la synthèse des travaux effectués dans le cadre de l'agenda numérique de l'Union européenne.

Les auditions conduites par votre mission d'information ont achevé de convaincre votre rapporteure de la pertinence de la première proposition qu'elle avait formulée dans son précédent rapport. Aussi souhaite-t-elle ici renouveler son **plaidoyer en faveur de la création d'une formation Numérique au Conseil de l'Union européenne**.

---

[1] Cf. L'Union européenne, colonie du monde numérique ?, *rapport d'information de Mme Catherine Morin-Desailly, fait au nom de la commission des affaires européennes du Sénat (n° 443, 2012-2013) (disponible à l'adresse suivante : http://www.senat.fr/notice-rapport/2012/r12-443-notice.html).*

Proposition n° 56 : créer au sein du Conseil de l'Union européenne une formation dédiée au numérique pour dépasser les cloisonnements administratifs au service d'une ambition politique partagée.

Le Parlement européen n'est cependant pas mieux structuré à cet égard que le Conseil de l'Union européenne. Pour ne prendre que l'exemple de la proposition de règlement sur les données personnelles, pas moins de cinq commissions ont travaillé sur le texte, une sixième ayant finalement décidé de ne pas rendre d'avis : la commission Libertés civiles, justice et affaires intérieures est saisie au fond tandis que sont saisies pour avis la commission Emploi et affaires sociales, la commission Industrie, recherche et énergie, la commission Marché intérieur et protection des consommateurs, ainsi que la commission Affaires juridiques.

Lors de son audition par votre mission d'information, Mme Catherine Trautmann a brossé un état des lieux des discussions sur les différents textes et indiqué : « *la gouvernance couvre un champ très large de politiques, et c'est pourquoi j'avais proposé, en 2005, la constitution d'une commission spéciale sur le numérique. Je n'ai hélas pas été suivie et l'on voit à présent s'élever, entre commissions, une querelle de* leadership. *Si c'est à la commission de l'industrie que revient ce rôle de tête, car l'approche technologique prévaut, se posent aussi des questions relatives à la protection des données et à l'impact sur la culture ou bien encore au droit des consommateurs, sur lesquelles interviennent d'autres commissions. D'où un risque de parcellisation de l'approche* ».

Particulièrement sensible à cette **problématique de concurrence entre commissions aux centres d'intérêt divergents**, votre mission d'information recommande la **création au sein du Parlement européen de commissions spéciales dédiées au numérique pour l'examen des textes traitant de ce sujet, à même de dialoguer avec le commissaire à la stratégie numérique et la formation numérique du Conseil de l'Union européenne**.

Proposition n° 57 : recommander la création au sein du Parlement européen de commissions spéciales pour examiner les textes relatifs à l'Internet.

Ce même constat peut également être dressé au niveau national, tant au Gouvernement qu'au Parlement.

Le portefeuille numérique n'a jusqu'à présent jamais fait l'objet d'un ministère dédié ; il est systématiquement rattaché au pôle économique et industriel ou bien il n'envisage le numérique que sous l'angle de son développement économique. La conséquence en est, comme au niveau du Conseil de l'Union européenne, un défaut de vision transversale et les risques que cela emporte lorsqu'on légifère. Si la création d'un ministère dédié risquerait de ne répondre que de manière insatisfaisante à la difficulté soulevée, du fait des doublons au sein des administrations que cela pourrait créer, une solution

pourrait être la **création d'un comité interministériel du numérique**, s'inspirant du comité interministériel de la société de l'information existant de 1998 à 2006. **Placé directement sous l'autorité du Premier ministre, ce comité serait à même de développer au niveau du Gouvernement une expertise transversale et d'obtenir les arbitrages nécessaires à une stratégie globale**. Il pourrait au surplus assister le Premier ministre dans la préparation des formations Numérique du Conseil de l'Union européenne auquel lui-même participerait, attestant d'une prise en considération à la hauteur de l'enjeu que le numérique représente désormais dans nos sociétés. Ce comité aurait à sa tête une personne incarnant l'ambition numérique de notre pays et orchestrant l'action gouvernementale en ce domaine, sur le modèle du *Chief Technology Officer* qui assiste le président Obama.

Proposition n° 58 : créer un comité interministériel du numérique auprès du Premier ministre pour conduire une stratégie d'ensemble cohérente.

Quant au Parlement, votre mission d'information a pris connaissance avec intérêt de **la création, pour la première fois sous l'actuelle législature, d'une commission permanente « Agenda numérique » au Bundestag**.

La nouvelle commission « Agenda numérique » du Bundestag

L'organisation des commissions permanentes du Bundestag est usuellement le reflet de celle du gouvernement fédéral, chaque commission étant chargée d'examiner les projets de loi émanant du ministère lui correspondant et en assurant le contrôle. La nouvelle commission « Agenda numérique » échappe cependant à ce schéma.

Créée à l'initiative de l'ensemble des quatre groupes politiques (CDU/CSU, SPD, Die Linke et Bündnis 90/Die Grünen) par un vote du Bundestag le 13 février 2014, cette commission s'est constituée le 19 février et compte seize membres. Elle est la **traduction de l'une des principales recommandations de la commission d'étude *ad hoc* « Internet et société numérique »** qui a conduit ses travaux au cours de la précédente législature.

Cette commission d'étude *ad hoc* avait été créée en mars 2010 et était composée de dix-sept députés et d'autant d'experts. Elle s'est penchée sur les conséquences de l'introduction du numérique dans tous les aspects de la vie économique, politique et sociale. Ses travaux ont donné lieu à la parution, entre octobre 2011 et mars 2013, de douze rapports d'étape thématiques[1], le rapport conclusif de mai 2013 insistant plus particulièrement sur les méthodes de travail innovantes mises en place par la commission : ouverture la plus transparente possible des travaux, utilisation d'instruments de travail collaboratifs – Etherpad, visioconférences, forum en ligne – participation des citoyens *via* l'Internet. En effet, cette commission s'était également donné comme objectif la modernisation des méthodes de travail du Bundestag grâce au numérique.

Dressant le constat d'un manque de coordination et d'une perte subséquente d'expertise sur le sujet de l'Internet tant au niveau parlementaire que gouvernemental, la commission

[1] *Ces rapports portaient sur : la compétence des médias ; les droits d'auteur ; la neutralité du réseau ; la protection des données et les droits de la personne ; démocratie et État ; économie, travail, Internet et télécommunications « verts » ; culture, médias, publication ; formation et recherche ; accès, structure et sécurité du réseau ; interopérabilité, standards, logiciels libres ; affaires internationales et gouvernance ; protection du consommateur.*

d'étude *ad hoc* avait recommandé, dans son septième rapport d'étape, la création d'une nouvelle commission permanente « Internet et société numérique » et d'une structure-miroir au sein du Gouvernement.[1]

La commission « Agenda numérique » prend donc le relais de cette commission d'étude *ad hoc* ; elle a pour mission de poursuivre la mise en œuvre de ses préconisations.

Lors de son déplacement à Berlin, une délégation de votre mission d'information a pu rencontrer neuf membres de cette nouvelle commission, dont son président, M. Jens Koeppen, avant même sa première réunion. Elle a ainsi pu échanger sur les raisons qui ont conduit à la création de cette commission et les difficultés que cela a soulevées.

Cette commission « Agenda numérique » s'est fixé pour objectif de **développer au sein du Parlement une expertise et un savoir-faire sur les enjeux du numérique afin de mieux contrôler l'action du Gouvernement en la matière**. En effet, bien que cela ait fait l'objet de nombreux débats, cette commission n'est pas législative car elle ne se veut pas concurrente mais complémentaire des autres commissions permanentes. À ce titre, elle se pose en **aiguillon des autres commissions afin d'éviter que des sujets numériques ne soient traités que partiellement en raison d'un manque de transversalité ou qu'au contraire ils se retrouvent orphelins**, aucune commission ne s'en saisissant. Modestes, ses membres estiment que la plus-value de cette nouvelle commission réside davantage dans sa capacité à faire inscrire les sujets numériques à l'ordre du jour et à lancer le débat plutôt que de prétendre mieux traiter au fond les différents sujets sous les divers angles nécessaires. Ses membres l'ont ainsi comparée à la commission des affaires européennes pour son caractère transversal. Enfin, la création de cette commission représente un signal pour l'opinion publique témoignant de l'intérêt du politique pour l'agenda numérique.

---

[1] *Extrait du septième rapport d'étape « Démocratie et État » de la commission d'étude* ad hoc *paru le 6 février 2013 :*
« Création d'une nouvelle commission permanente "Internet et société numérique"
Les délibérations au sein de la commission *ad hoc* au cours des années passées ont montré combien la politique de l'Internet est un thème transversal qui touche à différents domaines de la vie quotidienne. Elles ont également mis en évidence que le mouvement qui s'est enclenché avec le numérique dans tous les domaines est loin d'être achevé.
C'est pourquoi la commission *ad hoc* recommande au Bundestag la création dans les plus brefs délais d'une commission permanente dédiée à l'Internet.
En outre, la commission *ad hoc* recommande que cette nouvelle commission continue d'utiliser et de développer les moyens de participation en ligne des citoyennes et des citoyens.
Au surplus, la commission *ad hoc* recommande qu'eu égard à la complexité de la problématique, le Bundestag étudie les voies et moyens pour garantir à cette nouvelle commission une assistance scientifique dans son travail.
Parallèlement, la commission *ad hoc* recommande que le sujet de l'Internet et de la société numérique se voie accorder sa juste place au sein de l'exécutif par la création d'une structure à même de faire pendant à la nouvelle commission afin d'assurer une meilleure coordination dans le domaine transversal de l'Internet. »

Constatant que les préoccupations ainsi exprimées par ses homologues rejoignaient celles qui ont présidé à la création de la présente mission commune d'information, votre mission recommande **la création au sein du Sénat d'une commission dédiée au numérique sur le modèle de la commission des affaires européennes**, dont les membres seraient parallèlement membres d'une commission permanente thématique. Cela permettrait de garantir une **cohérence du traitement des différents sujets numériques**, tout en conservant également une **cohérence du traitement des sujets *offline* et *online***.

Proposition n° 59 : créer au Sénat une commission du numérique dont les membres seraient également membres d'une commission permanente législative.

b) Associer la société civile à la réflexion des politiques

Comme le soulignait la commission d'étude *ad hoc* du Bundestag dans son rapport de 2013, **il est nécessaire que le politique s'entoure de conseils, notamment techniques mais pas uniquement. Sur un sujet tel que l'Internet, l'association de la société civile à sa réflexion s'avère en effet indispensable**. C'est pourquoi votre rapporteure, lors de ses précédents travaux, avait recommandé la **création auprès de l'exécutif européen d'un organisme consultatif sur le modèle du Conseil national du numérique français**. Cette enceinte, indiquait-elle à l'époque, pourrait réunir des philosophes, des juristes, des chercheurs, des entrepreneurs, des financeurs de cette nouvelle économie, des créateurs de contenus... Elle pourrait ainsi également permettre de fédérer les énergies européennes et de resserrer les liens entre les Européens les plus au fait des évolutions permanentes de ce qu'il est désormais convenu de désigner comme l'écosystème numérique. À ce propos, elle relevait la déception des sociétés européennes constatant que les réunions des industriels du numérique organisées par la Commission européenne n'étaient pas réservées aux seuls acteurs européens mais également ouvertes à leurs concurrents.

De semblables initiatives semblent d'ailleurs se multiplier en Europe et au-delà du continent européen. Après la France et son Conseil national du numérique, le Royaume-Uni s'est doté au début de l'année 2013 d'un groupe consultatif multipartite sur la gouvernance de l'Internet, le MAGIG (pour *Multistakeholder Advisory Group on Internet Gouvernance*), pour l'assister dans la définition des positions gouvernementales sur ce sujet. Présidé par le ministère de la culture, des médias et des sports en charge de la politique en matière de télécommunications et d'Internet, qui associe des représentants des autres ministères concernés, ce MAGIG regroupe une trentaine de membres de la société civile : le régulateur Ofcom, l'association professionnelle du secteur technologique Tech UK, des entreprises du secteur des télécommunications (BT, Vodafone, Yahoo UK, Microsoft, Skype, ARM Holdings, Virgin Media, Google UK, Facebook, GSMA, Intel UK ...), le *London Stock Exchange*, un représentant de l'ICANN et des membres du *Third Sector* (*Taxpayers Alliance, London School of Economics, Oxford Internet Institute, Trade Union Congress, Childnet, Global Partner*

Digital, ...). Dans sa communication sur la gouvernance de l'Internet[1], la Commission européenne cite également l'exemple du *Comitê Gestor da Internet* brésilien.

Notant que la Commission européenne elle-même envisage, dans cette même communication, d'instaurer un processus de consultation préalable à l'élaboration des politiques relatives à l'Internet, votre rapporteure juge à propos de réitérer sa proposition d'un Conseil consultatif européen du numérique.

Proposition n° 60 : impulser la création d'un Conseil consultatif européen du numérique, véritable *task force* pour éclairer l'exécutif européen et fédérer l'écosystème européen dans un esprit d'équipe.

4. Promouvoir le modèle européen de l'Internet par une véritable diplomatie numérique associée à une politique industrielle

Comme le notaient plusieurs des personnes entendues par votre mission d'information, l'**Internet a pris une place telle dans nos sociétés qu'il est devenu un enjeu majeur des relations internationales**. Les États-Unis et les pays émergents, au premier rang desquels la Chine et la Russie mais également le Brésil et l'Inde, l'ont bien compris et ont d'ores et déjà commencé de mener une véritable diplomatie numérique, ainsi que M. Julien Nocetti l'expliquait à votre mission d'information. Mais la France et l'Europe en sont encore loin.

Certes, la France a, par le passé, été à l'origine d'initiatives en la matière : l'organisation par M. Bernard Kouchner, alors ministre des affaires étrangères, d'une conférence mondiale sur la liberté d'expression sur l'Internet, qui aurait dû se tenir en octobre 2010 mais fut annulée au dernier moment, ou encore l'inscription par le président Nicolas Sarkozy du numérique à l'ordre du jour du G8 lorsqu'il s'est tenu en France en mai 2011. La réunion des chefs d'État et de gouvernement avait ainsi été précédée la veille d'un « e-G8 » réunissant, à l'invitation du Président de la République, les grands acteurs de l'Internet, notamment les dirigeants de Google, Facebook, Wikipédia, Alibaba, PriceMinister, eBay… À l'heure actuelle toutefois, la diplomatie numérique de la France se résume à un diplomate, assisté d'une cellule de quelques personnes : M. David Martinon, nommé le 3 mai 2013 « représentant spécial de la France pour les négociations internationales sur la société de l'information et l'économie numérique ». Cependant, ainsi que le remarquait devant votre mission d'information M. Maurice Ronai, **cette diplomatie numérique française n'en est qu'au stade de l'esquisse : on n'en connaît pas la doctrine et ses moyens semblent fort limités**. Selon les dernières informations recueillies par votre rapporteure, le Ministère des affaires étrangères vient de décider d'alléger les

[1] *Communication du 12 février 2014 de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions – « Politique et gouvernance de l'Internet : le rôle de l'Europe à l'avenir » (COM(2014)72 final).*

maigres moyens qu'il y consacre à ce jour. La cellule de cinq personnes consacrée à ces sujets serait démantelée, laissant M. David Martinon porter seul nos positions en matière de gouvernance de l'Internet, avec l'unique appui d'un chargé de mission à la Direction générale de la compétitivité, de l'industrie et des services (DGCIS)[1]. **Votre rapporteure est particulièrement préoccupée par cet affaiblissement annoncé de nos moyens, à l'heure où de grands rendez-vous mondiaux s'annoncent pour redessiner la gouvernance de l'Internet et alors même que la diplomatie américaine se met en ordre de bataille.**

Si ce défaut de doctrine française peut être imputé au manque de structuration du traitement des questions du numérique au sein du Gouvernement (*cf. supra*), le même argument ne peut être avancé concernant la Commission européenne dont on a vu qu'elle était la seule institution européenne à avoir apparemment pris la mesure de l'enjeu numérique. Pourtant, nombreux sont ceux qui, à l'instar du Conseil national du numérique (CNNum), regrettent que la France et l'Europe ne soient pas mieux armées face à des équipes américaines solidement soutenues par les « géants du net » dans le cadre des négociations actuelles sur le Partenariat transatlantique de commerce et d'investissement (TTIP).

Dans son avis remis à Mme Fleur Pellerin, secrétaire d'État en charge du commerce extérieur, de la promotion du tourisme et des Français de l'étranger, le 7 mai dernier, le CNNum, entre autres recommandations, va en effet jusqu'à préconiser « *de temporiser les négociations, d'accélérer la construction de la stratégie numérique européenne, et de renforcer les capacités de négociation de l'Union européenne* », de crainte qu'un traité mal négocié faute de préparation suffisante du côté européen n'entrave durablement l'essor du marché numérique. Ce délai devrait être mis à profit pour rééquilibrer **l'« *asymétrie d'ambition et de stratégie* » entre l'Europe et les États-Unis**, dont l'organisation dans la négociation pourrait servir de modèle. À l'heure où l'opacité des négociations et en particulier du mandat européen est dénoncée, il apparaît en effet nécessaire, comme le suggère le CNNum, d'officialiser le rôle d'un négociateur européen spécifiquement chargé des questions numériques, s'appuyant sur un réseau d'experts et sur une consultation de la société civile et des acteurs économiques.

Au-delà de l'enjeu présent de la négociation du TTIP, ces recommandations pourraient servir de feuille de route pour l'**élaboration d'une doctrine européenne de diplomatie du numérique dont le Service européen pour l'action extérieure serait le fer de lance**. Cette doctrine pourrait également s'appuyer sur le projet d'Observatoire mondial de la politique de l'Internet, développé par la Commission européenne en partenariat avec le Brésil, l'Afrique du Sud, la Suisse et des organisations non gouvernementales. Cette plateforme accessible en ligne serait « *chargée du suivi de l'élaboration de la politique et de la réglementation de l'Internet et de la veille technologique dans ce domaine afin de mettre en évidence les relations entre différentes enceintes et discussions, de manière à éviter le*

[1] *La DGCIS est une direction du Ministère de l'économie, du redressement Productif et du numérique.*

cloisonnement des politiques et à aider à contextualiser les informations », selon la communication de la Commission[1].

Votre mission d'information observe par ailleurs qu'une recommandation similaire a été formulée par le groupe de travail sur le renseignement et les technologies de communication dans le rapport remis en décembre 2013 au Président Obama[2]. La recommandation n° 32 préconise ainsi la création au sein du Département d'État d'un bureau de l'Internet et des affaires du cyberespace dont la direction serait confiée à un diplomate confirmé et élevé au rang de secrétaire d'État adjoint. Sa mission serait non seulement de coordonner les activités des bureaux régionaux et thématiques sur les questions du numérique, mais également de promouvoir l'agenda diplomatique des États-Unis sur ces enjeux. Cet agenda consisterait en la promotion de la liberté de l'Internet, la protection de la propriété intellectuelle dans le cyberespace, l'évolution de la gouvernance de l'Internet et la mise en œuvre de la stratégie en matière de cybersécurité.

Proposition n° 61 : élaborer une véritable doctrine de diplomatie du numérique dotée de réels moyens, en s'appuyant sur un réseau d'expertise et sur une consultation de la société civile et des acteurs économiques.

Dans son avis précité, le CNNum met également en garde contre une approche trop centrée sur la relation transatlantique. Il rappelle ainsi que de nombreux pays se développent dans le numérique, en Afrique et en Asie notamment. **Ces pays émergents ne sont donc pas à négliger**, ce que d'autres États ont fort bien intégré dans leur stratégie diplomatique. Au cours de son audition, M. Maurice Ronai indiquait à votre mission d'information comment les États-Unis, notamment sous le mandat d'Hillary Clinton, ont su donner ses lettres de noblesse à la diplomatie numérique : « *elle regroupait alors des initiatives en faveur du développement des systèmes numériques en Afrique, des actions de soutien au cryptage pour permettre aux participants de communiquer, et aux développeurs des pays du Tiers-monde de travailler sur des applications mobiles* ».

Dans la guerre d'influence entre espaces juridiques concurrents présentée par Mme Isabelle Falque-Pierrotin (*cf. supra*), **cette diplomatie numérique est indispensable non seulement pour gagner des marchés** – on ne peut que se féliciter qu'Alcatel ait remporté le contrat du *cloud* du Burkina Faso, comme l'indiquait Mme Gabrielle Gauthey –, **mais également, et surtout, pour promouvoir les valeurs européennes, y compris en matière de protection des données personnelles**. À cet égard, votre mission ne peut que renouveler son souhait de voir adopter rapidement la proposition de règlement européen sur les données personnelles afin que la Commission européenne dispose d'un mandat clair sur la question pour négocier à l'international.

[1] *Communication (COM(2014)72 final).*

[2] Cf. Liberty and Security in a Changing World, *Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies, 12 décembre 2013.*

Dans cette perspective, **l'Europe dispose d'instruments à même de venir en appui à la diplomatique numérique**. L'Union européenne pourrait ainsi utilement mettre à profit la **politique européenne de voisinage**. Mise en place à partir de 2004 dans le but de promouvoir prospérité, stabilité et sécurité dans les pays limitrophes de l'Union, cette politique de voisinage ne se résume pas en effet à de simples accords de coopération et de commerce : elle comprend la conclusion de plans d'action bilatéraux prévoyant réformes politiques et économiques en vue d'asseoir les valeurs de démocratie, les droits de l'homme, l'État de droit. Dans ce cadre, l'Union pourrait par exemple diffuser son modèle de protection des personnes à l'égard du traitement automatisé des données à caractère personnel en assurant la promotion de la **Convention 108 du Conseil de l'Europe** qui est ouverte à l'adhésion d'États non membres (*cf. supra*).

La France pourrait, pour sa part, valoriser la **francophonie numérique** non seulement pour promouvoir la diversité linguistique sur Internet, mais également diffuser son modèle numérique, ainsi que le suggérait M. Vincent Champain lors de son audition. L'Association francophone des autorités de protection des données personnelles, dont Mme Jessica Eynard faisait mention, peut utilement être mobilisée à cet effet. Créée en 2007, cette association regroupe les seize autorités indépendantes chargées de la protection des données personnelles et de la vie privée des pays et gouvernements ayant en partage le français[1]. Elle associe également les représentants des États et gouvernements francophones ayant adopté une législation sans avoir encore installé d'autorité indépendante, ainsi que les représentants des autres États et gouvernements francophones qui sont intéressés à développer des règles de la protection des données personnelles, à titre d'observateurs. Quarante et un pays francophones sur les soixante-dix-sept membres et observateurs que compte l'Organisation internationale de la Francophonie disposent en effet d'une loi de protection des données personnelles. Il existe donc encore une marge de progrès en ce domaine.

Proposition n° 62 : appuyer la diplomatie numérique sur les instruments préexistants tels la politique européenne de voisinage ou la francophonie, afin de promouvoir à travers le monde le respect des valeurs européennes en ligne.

[1] *Sont ainsi membres adhérents de l'association les autorités indépendantes des États et gouvernements suivants : l'Albanie, Andorre, la Belgique, le Bénin, le Burkina Faso, le Canada, le Québec, la France, le Gabon, le Luxembourg, le Maroc, Maurice, Monaco, le Sénégal, la Suisse et la Tunisie.*

CONCLUSION

Votre mission commune d'information est plus que jamais convaincue que l'Union européenne a un rôle, et même une mission à assumer aujourd'hui : proposer un nouveau modèle de gouvernance de l'Internet, capable de fédérer de nombreux États autour de valeurs qui trouvent leur source en Europe mais qui sont universelles, articulées autour de la liberté et du respect des droits de l'homme et de l'État de droit. Ceci implique de consigner dans un traité, d'abord négocié entre les deux rives de l'Atlantique mais ouvert à tous, les principes de gouvernance dégagés par l'ensemble des parties prenantes réunies pour le NETmundial le 24 avril 2014 à São Paulo. Pour assurer la mise en œuvre de ces principes de gouvernance distribuée, transparente et responsable, votre mission propose de formaliser les relations entre les diverses instances de gouvernance et de mettre en place des mécanismes amenant ces instances à rendre compte de leur action devant l'ensemble des parties prenantes qui seraient représentées dans un Conseil mondial de l'Internet, issu de l'*Internet governance forum* rénové. Pour restaurer durablement la confiance, une refonte de l'ICANN est également indispensable : il s'agit d'en assurer la supervision par la communauté mondiale, de prévoir un vrai droit de recours à l'égard de ses décisions et de mettre fin aux conflits d'intérêts. De telles perspectives, seules à même d'asseoir une gouvernance légitime à long terme, impliquent de rendre la parole à l'ensemble des acteurs dans le débat ouvert par l'administration Obama et confié à la seule ICANN.

Pour être audible dans ce débat décisif, l'Europe doit parallèlement entreprendre de renforcer son assise industrielle numérique : une telle stratégie de construction économique prend du temps et doit devenir sans délai une priorité politique à haut niveau, ce que devrait soutenir M. Jean-Claude Juncker qui a annoncé vouloir « *travailler sur ce projet dès le premier jour de son accession à la présidence de la Commission* »[1]. Les données sont la ressource de demain, et sont donc au cœur de la stratégie de tous les grands pays du monde qui se projettent comme puissance : est-ce le cas de l'Union européenne ? C'est cette question essentielle que soulève finalement l'avènement de l'ère numérique.

Les prochains mois, qui devraient voir se succéder d'importantes réunions internationales, dans le cadre de l'UIT, de l'ICANN ou de l'IGF, seront cruciaux. Le dixième anniversaire du SMSI, que votre mission recommande de célébrer l'an prochain sur le sol européen, peut offrir l'occasion de témoigner en acte de l'implication de l'Europe dans la gouvernance de l'Internet.

L'Internet appelle à repenser les relations entre le droit et la technique, pour les faire dialoguer en continu grâce au juge, afin d'éviter que les évolutions

[1] Cf. *http://juncker.epp.eu/node/152*

techniques de plus en plus rapides ne précipitent l'obsolescence de la règle de droit et la décrédibilisent. Il invite aussi à repenser la souveraineté sous une forme dynamique, non pas autour d'un territoire mais autour de communautés de valeurs. C'est un effort auquel travaille précisément l'Europe pour sa propre construction.

L'Internet conduit finalement à la mondialisation de la politique, comme le souligne le géographe M. Boris Beaude. L'espace national dans lequel s'inscrit le politique n'est plus à l'échelle des pratiques humaines qui se font de plus en plus en ligne. C'est la communauté mondiale qui doit se projeter dans l'avenir pour le transformer. Et l'Union européenne est bien placée pour contribuer à ce mouvement, voire même y imprimer sa marque, à condition de le vouloir.

EXAMEN DU RAPPORT PAR LA MISSION

La mission s'est réunie le mardi 8 juillet 2014 pour l'examen du présent rapport.

M. Gaëtan Gorce, président. – Nous entendrons les questions de Mme Laborde, en réaction au projet de rapport mis en consultation la semaine passée, avant la présentation générale du rapport.

Mme Françoise Laborde. – Il semble que l'ICANN, sous dépendance de l'administration américaine, privilégie les intérêts des sociétés privées américaines qui cherchent à faire du business. Le rapport fait un certain nombre de propositions pour aider les entreprises européennes. Quels partenaires européens seraient prêts à soutenir la France sur ce projet ? D'une manière plus générale, quelle est la stratégie de l'Europe sur la gouvernance mondiale de l'Internet ? Par ailleurs, les pratiques du streaming ou du téléchargement ont un coût pour l'économie culturelle. Comment éviter que les acteurs de la création ne voient leur rémunération diminuer ? Vous préconisez la création d'un système d'exploitation européen. C'est tout à fait souhaitable. Mais comment pourrait-il s'imposer alors que les *smartphones* sont déjà équipés par défaut d'un OS - Android, IOS ou autres ? Enfin, l'enseignement du numérique est une question qui me tient à cœur. Le rapport s'inscrit dans la lignée du projet d'Axelle Lemaire, en proposant que la programmation informatique soit enseignée à l'école. Sous quelle forme se ferait cet enseignement ? Qui pourrait l'assurer ? Un dernier point m'intéresserait : votre analyse de l'autorisation donnée par l'ICANN à l'ouverture de noms de domaine en « .vin » et « .wine » sans tenir compte de certains enjeux de politique publique de l'Union européenne.

Mme Catherine Morin-Desailly, rapporteure. – C'est là tout le problème de l'ICANN.

Mme Françoise Laborde. – Les propositions du rapport, si on les applique, suffiront-elles à contrecarrer la puissance de cette organisation ? Je vous remercie pour ce rapport, remarquable par sa qualité d'information.

Mme Catherine Morin-Desailly, rapporteure. – Je tiens à remercier le président pour l'atmosphère conviviale qui a présidé à notre travail, favorisant sa rigueur et sa précision. L'Internet est né aux États-Unis dans les années 60. Il a connu un succès croissant à partir de 1989, date à laquelle le Cern a ouvert au public l'application du *World wide web*, souvent confondu avec l'Internet lui-même, qui est une interconnexion de réseaux. Un quart de siècle plus tard, 40 % de la population mondiale se connecte à l'Internet pour toutes sortes d'activités. Si l'Internet a pris racine sur les deux rives de l'Atlantique, celui que nous « consommons » est largement américain, car l'Europe n'a pas su prendre la mesure des enjeux. Cette technologie jeune constitue un potentiel de transformation exceptionnel dans les pays en développement et va prochainement s'étendre aux objets. Les enjeux politiques de l'Internet ne sont plus un secret depuis les

révélations d'Edward Snowden, en 2013, sur l'étendue de la surveillance en ligne. Au vu de l'actualité, je n'ai pu que me féliciter d'avoir convaincu mon groupe politique de lancer cette mission commune d'information, fin 2013. Nous avons ainsi travaillé plus de six mois pour analyser, dans le contexte post-Snowden, le nouveau rôle et la nouvelle stratégie que l'Union européenne pourrait avoir dans la gouvernance mondiale de l'Internet.

L'*Internet governance* est une notion ambivalente qui recouvre aussi bien la gouvernance de l'Internet, entendue comme la gestion technique de ce réseau de réseaux, que la gouvernance sur l'Internet, à savoir les moyens de faire respecter certaines règles en ligne, malgré le caractère transnational du réseau. Lors du sommet mondial sur la société de l'information (SMSI), qui s'est tenu sous l'égide des Nations unies en 2005, la gouvernance de l'Internet a été définie comme « l'élaboration et l'application par les États, le secteur privé et la société civile, dans le cadre de leur rôle respectif, de principes, normes, règles, procédures de prise de décisions et programmes communs, propres à modeler l'évolution et l'utilisation de l'Internet, évolution dans le sens technologique, utilisation au sens des pratiques». Cette définition reflète l'ambivalence de l'Internet dont le fonctionnement repose sur une imbrication de normes issues de la technique comme de la loi, sans organisme de tutelle centralisé. Quel ordonnancement peut-on y donner, dans quelles instances, avec quels instruments ? Comment concilier liberté de navigation et lutte contre la cybercriminalité, protection de la vie privée, encadrement de la marchandisation des données personnelles, protection de la diversité culturelle et de la propriété intellectuelle, protection de l'ordre public et de la sécurité des États ? Comment prévenir le risque d'une fragmentation de l'Internet en blocs régionaux voire nationaux ? Car, si l'Internet bouleverse les souverainetés, c'est aussi cela – le fait qu'il soit un espace partagé – qui fait sa richesse.

Au terme de nos travaux, il nous apparaît, dans un premier temps, que la gouvernance de l'Internet est devenue un nouveau terrain d'affrontement mondial. L'affaire Snowden a fait tomber le mythe originel de l'Internet et révélé sa nature hybride, puisqu'il est aussi un instrument de puissance et le support d'un monde d'hypersurveillance et de vulnérabilité. Le soupçon qui en résulte frappe le système de gouvernance de l'Internet. Notre mission a tenté de décrypter ce système de gouvernance, ce qui constitue une contribution inédite et importante pour le débat public. Elle a constaté que cette gouvernance était encore sous domination américaine, mais que le *statu quo* était devenu impossible. Une opportunité historique s'offre à l'Europe de garantir un avenir de l'Internet conforme à ses valeurs. Nous avançons 62 propositions pour tenter de saisir cette chance. Elles concernent à la fois le niveau national et européen, et ne sont pas toutes du même ordre, certaines pouvant se traduire dans la loi, d'autres en résolutions, d'autres encore n'étant que de simples recommandations.

Porté par le monde de la recherche avant d'être accaparé par les intérêts militaires et commerciaux américains, l'Internet s'est d'emblée caractérisé par ses dimensions d'horizontalité et d'ouverture. Il est ainsi devenu un instrument

technologique accessible par et pour tous. Grâce à l'architecture décentralisée de ce réseau de réseaux, tout utilisateur peut développer des innovations susceptibles de rencontrer un succès mondial. Cela promet des progrès immenses en matière de santé, d'énergie, d'éducation, de transport... Innovation de rupture, l'Internet révolutionne les modèles économiques, mais aussi les relations humaines et la relation de l'être au monde.

Au-delà de ce mythe originel, l'Internet est un prolongement de la puissance par le droit et l'économie. Avant la généralisation du web, au début des années 90, les États-Unis ont pris des dispositions législatives et fiscales pour acquérir le *leadership* sur cette technologie. Si bien que, sur les 50 premières entreprises de médias numériques, 36 sont américaines. Dans les années 2000, la Chine a bâti un écosystème d'entreprises numériques importantes, la Russie a suivi. Faute de volonté politique, l'Europe vit sous la domination commerciale des acteurs américains du net. Or, cette domination commerciale est le socle d'une domination juridique : de nombreux noms de domaine ressortent des juridictions américaines, tout comme un certain nombre de litiges relatifs aux conditions générales d'utilisation des plus grandes plateformes. L'Internet évolue également vers une hypercentralisation au profit de grands acteurs privés ; se constituent ainsi des silos verticaux, par exemple dans le mobile, où le terminal, le système d'exploitation et les applications sont vendus d'un seul bloc. Ces grands acteurs défient les États : ils sapent les moyens de l'action publique par l'optimisation fiscale, ils rivalisent avec leurs services publics, ils menacent leurs modèles économique et culturel, ils frappent même monnaie virtuelle – tel le Bitcoin.

L'Europe se trouve largement distancée dans cette redistribution des pouvoirs. Sa place est même en recul : seuls 8 groupes européens figurent dans les 100 premiers groupes high-tech mondiaux, contre 12 il y a deux ans. Quoique dotée d'opérateurs télécoms solides, l'Europe se trouve dépourvue d'acteurs de premier plan aux deux bouts de la chaîne de valeur numérique : les équipementiers d'une part, les fournisseurs de contenus et d'applications, également appelés *over the top* (OTT), de l'autre. Elle est ainsi menacée de ne plus avoir accès au savoir et à la connaissance que par la médiation d'acteurs non européens.

L'évolution des technologies et des mentalités a transformé la promesse de liberté que constituait l'Internet, en un fantastique outil de surveillance. En facilitant le stockage et le traitement, le *big data* a incité à une collecte exponentielle de données, notamment personnelles, qui peuvent être exploitées aussi bien par les géants du net que par les services de renseignement. Le système par défaut est devenu la collecte généralisée de données : que devient la présomption d'innocence ? Parallèlement, la dépendance croissante de nos sociétés à l'Internet est devenue facteur de vulnérabilité. Le réseau est le théâtre de véritables attaques qui peuvent provenir d'États, d'organisations ou simplement d'individus : espionnage économique, déstabilisation, sabotage d'infrastructures critiques… Le *hacking* est une arme et les vulnérabilités informatiques font l'objet d'un marché.

À la veille de l'affaire Snowden, Madeleine Albright confiait à François Delattre, ambassadeur de France à Washington, que la gouvernance de l'Internet était une priorité de la diplomatie américaine. C'est dire combien cette gouvernance constitue un enjeu géopolitique mondial. Aucune autorité centrale ne gouverne l'Internet aujourd'hui. En revanche, une pléthore d'enceintes participe à une forme d'autorégulation du réseau : l'ICANN, organisme de droit californien, mais aussi l'IETF qui s'occupe des standards et de la spécification des protocoles, l'ISOC, le W3C, etc. Si ce système informel a fait la preuve de son efficacité, il est parvenu au terme de l'exploitation qu'on peut en faire.

Cette gouvernance de l'Internet est américaine, de fait. Les géants américains de l'Internet ont naturellement intérêt à être présents dans ces diverses enceintes, qui sont souvent liées aux universités américaines. Aussi, 10 des 13 serveurs racine sont aux États-Unis. Surtout, l'ICANN gère le fichier racine du système des noms de domaine - forme d'annuaire central de l'Internet - en collaboration avec la société américaine VeriSign, sous la supervision du Département du commerce américain, qui doit valider tout changement au fichier. La gestion des noms de domaine, et notamment la création de nouvelles extensions génériques, a d'importantes conséquences économiques, voire politiques, comme en témoigne le cas du «.vin » et du « .wine ». En proie aux conflits d'intérêt, l'ICANN fonctionne de manière trop opaque. Elle n'offre pas de droit de recours satisfaisant et ne rend compte qu'au gouvernement américain. Les États ne sont représentés à son conseil d'administration que par une voix consultative, celle du *Governmental Advisory Committee*. Depuis la création de l'ICANN en 1998, le gouvernement des États-Unis a donc joué le rôle de pourvoyeur de confiance ou de garant du système.

Cette domination américaine sur la gouvernance de l'Internet a été de plus en plus contestée. En 2005, le sommet mondial de la société de l'information (SMSI), sous les auspices de l'ONU, s'est conclu par l'Agenda de Tunis, qui appelle à la coopération renforcée de tous les acteurs – États, secteur privé, société civile – dans la gouvernance de l'Internet. C'est dans cette perspective qu'a été fondé l'*Internet governance forum* (IGF), un forum multi-parties prenantes – *multistakeholder* dans le jargon américain-, qui est onusien mais pas interétatique. Doté d'un rôle consultatif, ce forum affiche un bilan médiocre et se trouve concurrencé par une multitude d'événements traitant de la gouvernance de l'Internet. C'est finalement à l'occasion de la conférence organisée par l'Union internationale des télécoms, à Dubaï, en décembre 2012, que l'opposition s'est cristallisée entre les tenants d'une reprise en main étatique de la gouvernance de l'Internet, et ceux d'une gouvernance multi-acteurs. Dans ce contexte, la parole européenne reste peu audible. Elle souffre d'être seulement portée par la direction générale compétente de la Commission européenne - la DG Connect - sans être assumée par le Conseil européen. Naturellement, tous ceux qui interrogent le *statu quo* sont présentés par les États-Unis comme des ennemis de la liberté. L'Union européenne, espace de liberté, n'est-elle pas attendue pour explorer une

troisième voie, celle de la gouvernance d'un Internet bâti sur des valeurs démocratiques mais reconnaissant le rôle légitime des États ?

À partir de juin 2013, les révélations d'Edward Snowden dévoilent la surveillance de masse exercée en ligne et attestent que les États-Unis ont volontairement affaibli la sécurité sur le net. La confiance dans l'Internet est ébranlée. Les géants du net, qui ont contribué à faire élire Obama, se retournent contre leur gouvernement, car leurs résultats s'en ressentent. Pour Éric Schmidt, le PDG de Google, Snowden est « un traître sur la côte Est, un héros sur la côte Ouest ». À Montevideo, en octobre 2013, les enceintes de gouvernance de l'Internet appellent à une mondialisation de la supervision du fichier racine de l'Internet. Dilma Rousseff, la présidente du Brésil, convoque une conférence mondiale sur la gouvernance de l'Internet pour avril 2014. En novembre 2013, le Brésil et l'Allemagne font adopter à l'ONU une résolution réaffirmant le droit à la vie privée à l'ère numérique. Les États-Unis, garants de la liberté en ligne, ont perdu leur magistère moral sur l'Internet.

Cette ère de soupçon à l'égard des États-Unis vient accélérer une tendance à la fragmentation de l'Internet, qui est déjà à l'œuvre par stratégie souveraine, surtout dans les États autoritaires, ou par stratégie commerciale des grands acteurs qui évoluent vers des silos. Un Internet fracturé donnerait des moyens de censure supplémentaires à ceux qui contrôleront ces blocs fermés : comment rétablir la confiance des internautes et la sécurité en ligne tout en maintenant l'unicité du réseau ? Le président Obama, dans son discours de janvier 2014 sur l'état de l'Union, n'a pas su répondre. La chancelière allemande a appelé en février 2014 à un Internet européen. Un mois plus tard, le Parlement européen a adopté un rapport très offensif en réaction aux pratiques de surveillance en ligne. C'est finalement le 14 mars, avant la conférence NETmundial au Brésil, que l'administration américaine a fait un pas significatif, en annonçant son intention de lâcher du lest sur la supervision du fichier racine du système des noms de domaine. La conférence NETmundial a rassemblé tous les acteurs les 23 et 24 avril à São Paulo. Elle représente une avancée décisive, en consacrant certains principes et valeurs fondamentaux pour l'Internet et sa gouvernance. Elle condamne la surveillance en ligne, sans renoncer à l'unicité et l'ouverture de l'Internet. Mais le rôle des États doit encore être précisé ; la réforme de la gouvernance de l'Internet reste à faire, à commencer par celle de l'ICANN.

Pour garantir un avenir de l'Internet conforme à ses valeurs l'Union européenne devra se poser en médiateur. Elle ne sera crédible dans ce rôle que si elle reprend en main son propre destin numérique. L'Internet est un bien commun, d'un genre inédit, ni public, ni privé. Pour que cette ressource profite à tous, sa gouvernance ne devrait pas être complètement privatisée. Elle doit reposer sur un dialogue entre technique et politique, car l'architecture de l'Internet est en fait politique. Il serait bon que les États membres de l'Union Européenne s'entendent sur un traité international consacrant les principes fondateurs du NETmundial. Ce traité serait ouvert à la signature de tous les États, et pourrait être soumis à une forme de ratification en ligne par les internautes. Sur

cette base, nous pourrions faire émerger un réseau d'enceintes pour une gouvernance de l'Internet distribuée et transparente. Il conviendrait aussi de transformer le Forum pour la Gouvernance de l'Internet en Conseil mondial de l'Internet, doté d'un financement propre, et en charge de contrôler la conformité des décisions des enceintes de gouvernance aux principes dégagés au NETmundial. Toutes les enceintes devraient rendre des comptes devant ce Conseil, selon le principe de l'*accountability*.

Quant à l'ICANN, elle doit être refondée pour restaurer la confiance. Il s'agirait d'en faire une WICANN (World ICANN), qui serait de droit international ou, de préférence, de droit suisse, sur le modèle du Comité international de la Croix Rouge. Serait mise en place une supervision internationale du fichier racine des noms de domaine en substitution de la supervision américaine. Elle serait assurée par un comité, au sein du Conseil mondial de l'Internet. La WICANN devra également être responsable devant ce Conseil ou, à défaut, devant une assemblée générale interne, qui aurait le pouvoir d'approuver les nominations au conseil d'administration de la WICANN et d'approuver ses comptes. Les États pourraient conserver un rôle consultatif au sein de la WICANN, à condition que soit mis en place un mécanisme de recours indépendant et accessible, permettant la révision d'une décision de la WICANN, voire sa réparation. Une séparation devrait être établie pour distinguer ceux qui élaborent les politiques relatives aux noms de domaine, de ceux qui les attribuent individuellement. Des critères d'indépendance seront à définir pour l'essentiel des membres du *board* de la WICANN, afin de réduire les possibilités de conflits d'intérêts. Avant tout, nous devrons exiger que le groupe directeur prévu par l'ICANN pour organiser la transition soit composé de membres désignés selon des modalités transparentes et démocratiques. Il devra inclure des représentants de tous les gouvernements et de la communauté académique.

La régulation des acteurs qui font partie de l'écosystème européen du numérique doit se faire offensive pour améliorer la répartition de la valeur au bénéfice des acteurs européens. Le principe de neutralité du net devrait s'appliquer non seulement aux réseaux mais aussi aux services. Parallèlement, la fiscalité européenne doit évoluer pour faire contribuer les fournisseurs de services en ligne aux charges publiques des États européens. Enfin, nous devons inventer de nouvelles modalités pour faire vivre la culture européenne sur l'Internet ; un premier pas serait déjà d'aligner les taux de TVA des biens et services culturels numériques et physiques.

L'Union européenne doit par ailleurs se doter d'un régime exigeant et réaliste de protection des données, à l'ère du *cloud* et du *big data*. Nous rentrons des États-Unis avec la conviction que l'approche européenne, qui est assise sur l'affirmation d'un droit fondamental à la protection des données personnelles, est valide. Elle peut donner un avantage comparatif à notre industrie, incitée à être plus innovante. Notre régime de protection des données doit être modernisé, notamment par l'adoption rapide de la proposition de règlement européen en cours de négociation. Cela implique aussi d'instaurer un régime de responsabilité

pour les responsables de traitement de données. Cette approche européenne doit être promue à l'international. La renégociation du *Safe Harbor* y contribuera, ce système par lequel les entreprises américaines s'auto-certifient pour assurer leur conformité aux règles européennes de protection des données. Cette négociation devra rester distincte de celle du traité transatlantique, afin que la question fondamentale des données personnelles ne soit pas utilisée comme une monnaie d'échange.

L'Union européenne doit également catalyser son industrie numérique autour d'une ambition affichée. Cela implique de faciliter l'accès au financement des entreprises européennes ; cela appelle aussi à développer des clusters européens du numérique. En matière commerciale, il importe de rendre plus équitables les règles du jeu international au bénéfice des entreprises européennes du numérique. L'Union européenne doit aussi défendre ses valeurs dans la négociation du traité transatlantique : promouvoir son système d'indications géographiques mais aussi veiller à assortir toute libéralisation transatlantique de la circulation des données, d'exceptions au titre de la protection de la vie privée et de la sécurité publique.

Cette ambition industrielle doit permettre à l'Union européenne d'exploiter ses propres données au service du bien commun : le *big data* doit être promu comme un véritable enjeu industriel. Le développement de l'open data doit être poursuivi, tout en respectant les principes d'anonymat et de non-discrimination. La France et l'Allemagne doivent prendre l'initiative de deux projets industriels concrets et stratégiques pour notre avenir numérique: un système d'exploitation pour mobiles européen et un service de *cloud* européen sécurisé mais ouvert. Ce *cloud* se distinguerait par sa fiabilité et sa transparence attestées par un label. Le potentiel européen en matière de sécurité doit par ailleurs être exploité, grâce au développement des compétences en matière de chiffrement. Les extensions en «.fr» et « .eu », qui ressortent des juridictions française et européenne, doivent être promues au titre de la sécurité juridique. Enfin, comme le préconise Louis Pouzin, l'Europe doit préparer sa place dans l'Internet de demain, notamment en étant plus présente dans les grandes instances internationales de standardisation de l'Internet.

L'Union européenne doit promouvoir une appropriation citoyenne de l'Internet. L'Éducation nationale a un rôle à jouer en garantissant la place du numérique au cœur du socle commun des compétences et en formant progressivement l'ensemble des professeurs en fonction. Il faut également renforcer l'encadrement légal des activités de renseignement et en améliorer le contrôle politique : la loi doit étendre le contrôle de la Commission nationale de contrôle des interceptions de sécurité (CNCIS). À partir de la CNCIS, une nouvelle autorité administrative indépendante – la Commission de contrôle des activités du renseignement – pourrait même être créée, pour autoriser la mise en œuvre des moyens de collecte d'informations, après examen de leur légalité et de leur proportionnalité. Les pouvoirs d'investigation de la Délégation parlementaire au renseignement devraient aussi être renforcés. Enfin, un cadre européen de

contrôle des échanges d'informations entre services de renseignement devrait être établi.

En outre, la gouvernance des questions numériques doit être mieux structurée en France et en Europe: au sein du Conseil de l'Union européenne, grâce à une formation dédiée au numérique pour dépasser les cloisonnements administratifs; au sein du Parlement européen, grâce à des commissions spéciales pour examiner les textes relatifs à l'Internet ; en France, grâce à la création d'un comité interministériel du numérique auprès du Premier ministre et grâce à la création d'une commission du numérique au Sénat, dont les membres seraient également membres d'une commission permanente législative, comme le sont les membres de la commission des affaires européennes.

De surcroît, le modèle européen de l'Internet doit être promu par une véritable diplomatie numérique s'appuyant sur une doctrine claire et dotée de moyens. C'est précisément le mouvement inverse que je constate : j'ai appris que le Quai d'Orsay venait de décider d'alléger les maigres moyens consacrés à ce sujet. Nous devons dénoncer cet affaiblissement, d'autant que l'action diplomatique que j'appelle de mes vœux devrait s'accompagner d'une politique industrielle européenne ambitieuse et cohérente. Pour promouvoir à travers le monde le respect des valeurs européennes en ligne, cette action diplomatique devrait aussi mettre à profit les instruments préexistants - comme la politique européenne de voisinage, la francophonie, et la Convention 108 du Conseil de l'Europe sur la protection des données personnelles.

La question essentielle que soulève l'avènement de l'ère numérique est celle de l'ambition européenne. Les données sont la ressource de demain, et sont donc au cœur de la stratégie de tous les grands pays du monde qui se projettent comme puissance : est-ce le cas de l'Union européenne? Les prochains mois vont voir se succéder d'importantes réunions internationales, dans le cadre de l'IUT, de l'ICANN ou de l'IGF ; ils seront cruciaux. Le dixième anniversaire du SMSI, que je recommande de célébrer l'an prochain sur le sol européen, peut offrir l'occasion de témoigner en acte de l'implication de l'Europe dans la gouvernance de l'Internet. L'Internet appelle à repenser les relations entre le droit et la technique. Il invite aussi à repenser la souveraineté sous une forme dynamique, non pas autour d'un territoire mais autour de communautés de valeurs.

M. Gaëtan Gorce, président. – Merci pour cet exposé très complet.

Mme Françoise Laborde. – Nous avons évoqué Mme Lemaire, n'oublions pas Mme Fioraso ! Qu'en est-il de l'écart entre l'Europe et les États-Unis en matière d'enseignement supérieur ? Le président Obama a changé beaucoup de choses, notamment dans l'enseignement. En France et en Europe, nous sommes beaucoup plus frileux. J'ai par ailleurs participé à la journée d'information sur le renseignement français qui a été organisée récemment. J'en retiens que la plus grande vigilance s'impose contre l'espionnage économique, les attaques sur Internet… Je me réjouis donc que ce rapport présente des propositions ambitieuses !

Mme Catherine Morin-Desailly, rapporteure. – Formons-nous assez d'ingénieurs ? Un passage du rapport est consacré à cette question. Toutes les activités humaines sont désormais concernées par le numérique. Un réel effort de formation d'ingénieurs-programmateurs reste à faire. Il convient aussi de sensibiliser les citoyens dès leur plus jeune âge, à la fois pour protéger leurs données personnelles et pour leur donner des connaissances techniques.

Quel est le degré de prise de conscience en Europe ? Nous voulions enquêter dans les 28 États-membres. Finalement, nous nous sommes concentrés sur neuf pays, pour des raisons budgétaires. Un premier groupe de pays est très aligné sur les États-Unis : Royaume-Uni, Suède, Pays-Bas et Estonie. L'Italie semble encore peu mobilisée sur ce sujet. Quant à l'Allemagne, sa position n'est pas très claire, nous l'avons bien vu lors de notre rencontre avec le représentant du ministre des affaires étrangères. La Belgique, l'Espagne et la Pologne sont de plus en plus préoccupés par ces questions. Mais aucun État membre n'a pris d'initiative politique sur le rôle de l'Union européenne dans la gouvernance mondiale de l'Internet. J'ai participé récemment à Athènes à la Conférence des représentants des commissions des affaires européennes des parlements de l'Union européenne : j'ai bien vu que ces thèmes ne suscitaient que peu de réactions, sauf chez les Allemands, les Lituaniens et les Estoniens.

M. Jean Bizet. – Je commence par saluer la qualité de ce rapport d'information, qui fera date. Il ne pouvait en être autrement, étant donné la qualité de la rapporteure et celle du président ! Ces dossiers techniques réclamaient un travail de longue haleine.

Si la France est souvent en avance dans la recherche fondamentale, les applications sont développées par d'autres. Nous avons inventé le Minitel, et Bill Gates en a tiré parti. Il en a été de même des biotechnologies végétales… Le numérique pénètre tous les aspects de l'économie, il est à la source de nombreux gains de productivité et de compétitivité. La mainmise des États-Unis sur la sphère de l'Internet est donc inquiétante. L'Europe doit réagir, cela devra être une des priorités de la nouvelle Commission européenne. L'amende infligée à BNP Paribas montre bien qu'une loi américaine peut devenir mondiale. Veillons à ce qu'un Internet mondial ne devienne pas américain !

L'importance de la protection des données ne saurait être sous-estimée : sans elle, la méfiance qu'inspirera l'Internet empêchera que son formidable potentiel de diffusion de la connaissance et de création de lien social ne soit exploité. L'Europe est consciente de cet enjeu, comme en témoignent plusieurs rapports publiés récemment par la Commission européenne – même si nous avons tendance à être un peu naïfs face à l'espionnage industriel.

Ce rapport comporte nombre de recommandations intéressantes. Je soutiens en particulier celle qui préconise la création au Sénat d'une commission du numérique, si nécessaire en regroupant la commission des affaires économiques et celle du développement durable. Le Sénat a une culture d'avenir ! La prochaine Commission européenne devra prendre rapidement la dimension de ces questions.

Bref, ce rapport arrive à point nommé. Je n'ai qu'un regret : n'avoir pu participer à toutes les étapes de son élaboration.

M. Philippe Leroy. – Je n'ai pas été assidu, mais je lirai attentivement ce rapport fondateur. Étant plutôt un spécialiste des tuyaux, j'estime que les considérations techniques sont indissociables des réflexions sur l'éthique, la gouvernance ou la protection économique : sur Internet, la porosité des tuyaux rend presque impossible le contrôle des données qui y circulent. Lorsqu'il s'agit d'électricité ou d'eau, les techniciens savent régler ce genre de problème. Dans les centres de données, des centaines de personnes surveillent en permanence les variations de débit pour empêcher tout piratage. Des milliards de données bancaires circulent à travers le monde : il importe de veiller à ce que des pirates ne puissent pas s'en emparer. Il est en effet très simple, et très bon marché, de détourner un flux électronique au moyen d'une simple sonde. C'est aussi sans danger, contrairement au piratage de l'électricité ou de l'eau. Inutile de créer une police si l'on ne règle pas ce problème, face auquel même les Américains sont démunis… Il faudra en tous cas, si une commission du numérique est créée, lui adjoindre des spécialistes de la transmission de données.

Une gouvernance européenne est nécessaire. Les opérateurs n'y sont pas tous favorables, et ils sont nombreux : plusieurs milliers d'acteurs se sont taillé des parts de marché dans ce nouvel écosystème, qui ne sont guère demandeurs de régulation… Les propos de M. Montebourg sur la nécessité de réduire le nombre des opérateurs révèlent bien la grande fragmentation de cette économie, où prospèrent encore, comme dans une sorte de *Far West*, de nombreux aventuriers. Mme Lemaire m'a semblé très favorable à l'idée que la France a un message à porter à l'Europe et au monde dans ce domaine, où son action pourrait être plus décisive que pour le développement du numérique en France.

M. Gaëtan Gorce, président. – Je vous propose d'adopter le rapport sous le titre suivant : « *L'Europe au secours de l'Internet : démocratiser la gouvernance de l'Internet en s'appuyant sur une ambition politique et industrielle européenne.* »

Mme Catherine Morin-Desailly, rapporteure. – « L'Europe au secours de l'Internet » est un impératif qui nous est apparu aux États-Unis…

La mission adopte le rapport d'information ainsi intitulé.

Mme Catherine Morin-Desailly, rapporteure. – J'ai souhaité travailler sur ces questions car, face à un monde en transformation, le rôle des responsables politiques est de poser les questions pertinentes. La science est-elle source de progrès et de développement ? « Science sans conscience n'est que ruine de l'âme »… Les valeurs européennes, inspirées de la Charte des droits de l'Homme, nous imposent de soulever cette question, sans arrogance, afin d'entretenir une confiance raisonnable en les promesses de l'Internet.

M. Gaëtan Gorce, président. – Merci à tous.

ANNEXES

ANNEXE 1 : GLOSSAIRE

ADPIC : Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce, dans le cadre de l'Organisation mondiale du commerce

ADSL : *Asymmetric Digital Subscriber Line* (liaison numérique asymétrique)

AEPD : Autorité espagnole de protection des données (Espagne)

AFNIC : Agence française pour le nommage Internet en coopération (France)

AMP : Accord sur les marchés publics, dans le cadre de l'Organisation mondiale du commerce

ANR : Agence nationale de la recherche (France)

ANSSI : Agence nationale de la sécurité des systèmes d'information (France)

APEC : Forum de coopération économique de la région Asie-Pacifique

API : *Application programming interface* (communications entre interfaces de programmation)

APIE : Agence du patrimoine immatériel de l'État (France)

ARCEP : Autorité de régulation des communications électroniques et des postes (France)

ARP : Société civile des auteurs, réalisateurs et producteurs (France)

ASO : *Address supporting organization*, structure de l'ICANN représentant les cinq registres Internet régionaux qui gèrent les adresses IP (Etats-Unis)

ATM : Mode de transfert asynchrone

B2I : Brevet informatique et Internet (en France)

BCR : *Binding corporate rules* (règles internes d'entreprises), règles protégeant le transfert de données transférées de l'Union européenne vers un pays tiers au sein d'une même entreprise multinationale

BEPS : *Base erosion and profit shifting* (érosion des bases d'imposition et transfert de bénéfices), projet de l'Organisation de coopération et de développement économiques sur la fiscalité et le numérique

BGP : *Border Gateway Protocol*, protocole d'échange de route utilisé notamment sur le réseau, conçu pour prendre en charge de très grands volumes de données et disposant de possibilités étendues de choix de la meilleure route, afin d'échanger des informations d'accessibilité de réseaux entre systèmes autonomes.

CBPR : *Cross-Border Privacy Rules* (règles relatives au transfert international de données personnelles), système élaboré dans le cadre du Forum de coopération économique de la région Asie-Pacifique

CCAR : Commission de contrôle des activités de renseignement (France)

ccTLD : *Country code top level domains* (domaines géographiques de premier niveau)

ccNSO : *Country code names supporting organization*, structure de l'ICANN en charge des noms de domaine géographiques

CEN : comité européen de normalisation (pays de l'Union européenne et certains pays de l'Association européenne de libre-échange)

CENELEC : comité européen de normalisation en électronique et électrotechnique (pays de l'Union européenne et certains pays de l'Association européenne de libre-échange)

CENTR : *Council of European National Top Level Domain Registries* (association européenne des gérants d'extensions de domaines géographiques de premier niveau)

CEPS : *Centre for European policy studies* (centre d'études de la politique européenne, à Bruxelles)

CERN : Organisation européenne pour la recherche nucléaire

CGU : Conditions générales d'utilisation

CICS : Comité des industries de la confiance et de la sécurité (France)

CIMAP : Comité interministériel de modernisation de l'action publique (France)

CIR : Crédit d'impôt recherche (France)

CJUE : Cour de justice de l'Union européenne (Union européenne)

Cloud computing : infonuage ou accès *via* Internet, à la demande et en libre-service, à des services de stockage, d'utilisation et de traitement de données informatiques accessibles à distance

CNC : Centre national de la cinématographie et de l'image animée (France)

CNCIS : Commission nationale de contrôle des interceptions de sécurité (France)

CNIL : Commission nationale de l'informatique et des libertés (France)

CSFN : Comité stratégique de la filière numérique (France)

DARPA : *Defense Advanced Research Projects Agency*, agence du département de la défense des États-Unis chargée de la recherche et développement des nouvelles technologies destinées à un usage militaire

DGCIS : Direction générale de la compétitivité, de l'industrie et des services du ministère de l'économie (France)

DGCCRF : Direction générale de la concurrence, de la consommation et de la répression des fraudes (France)

DG Connect : Direction générale de la société de l'information et des médias de la Commission européenne (Union européenne)

DGMIC : Direction générale des médias et des industries culturelles du ministère de la culture et de la communication (France)

DISIC : Direction interministérielle des systèmes d'information et de communication (France)

DNS : *Domain Name System* (système de noms de domaine)

DPI : *Deep packet inspection* (inspection des paquets en profondeur)

DPR : Délégation parlementaire au renseignement (France)

ECP : *European cloud partnership* (partenariat européen de l'informatique en nuage) (Union européenne)

EEE : Espace économique européen

ENISA : Agence européenne chargée de la sécurité des réseaux et de l'information (European Network and Information Security Agency)

EPFL : École polytechnique fédérale de Lausanne

ERCIM : *European Research Consortium for Informatics and Mathematics* (consortium européen pour la recherche en informatique et en mathématiques)

ETI : Entreprises de taille intermédiaire

ETSI : *European telecommunications standards institute* (Institut européen des normes de télécommunications)

FAA : *FISA Amendment Act* (loi du 10 juillet 2008 modifiant le *Foreign Intelligence surveillance act*) (États-Unis)

FAI : Fournisseur d'accès à Internet

FCA : Fournisseurs de contenus et d'applications

FCC : *Federal Communications Commission* (commission fédérale des communications) (États-Unis)

FTC : *Federal Trade Commission* (commission fédérale du commerce) (États-Unis)

FEDER : Fonds européen de développement régional (Union européenne)

FGI : Forum sur la gouvernance de l'internet

FING : Fondation Internet nouvelle génération

FISA : *Foreign Intelligence Surveillance Act* (loi de 1978 sur le contrôle des services de renseignement extérieur) (États-Unis)

FISC : *Foreign Intelligence Surveillance Court* (cour de justice instituée dans le cadre de la loi de 1978 sur le contrôle des services de renseignement extérieur) (États-Unis)

FIT : *Future Internet of things* (Internet du futur des objets), projet français de recherche

FUN : France université numérique

GAC : *Governmental Advisory committee*, comité gouvernemental consultatif placé auprès de l'ICANN (États-Unis)

GAFA : Google, Apple, Facebook, Amazon

GESTE : Groupement des éditeurs de services en ligne (France)

GIC : *Global Internet council* (conseil mondial de l'Internet)

gTLD : *Generic top level domains* (domaines génériques de premier niveau)

GNSO : *Generic names supporting organization*, structure de l'ICANN en charge des noms de domaine génériques

HLGIG : *High level group on Internet governance* (groupe d'experts sur la gouvernance de l'Internet)

HTML : *Hypertext markup language*, langage informatique le plus courant pour décrire le contenu d'un document (titre, paragraphe, intégration de photos …)

HTTP : *HyperText Transfer Protocol*, nom du protocole de communication généralement utilisé pour échanger ou transférer les ressources du Web

IAB : *Internet architecture board*, comité chargé de la surveillance et du développement de l'Internet désigné par l'*Internet Society*.

IANA : *Internet Assigned Number Authority* (Autorité des adresses de l'Internet), assumée par l'*Internet Corporation for Assigned Names and Numbers*

IAP : *In-app purchases*, achats intégrés à partir de l'application

ICANN : *Internet Corporation for Assigned Names and Numbers* (Société pour l'attribution des noms de domaine et des numéros sur l'Internet) (États-Unis)

IEEE : *Institute of Electrical and Electronics Engineers* (Institut des ingénieurs électriciens et électroniciens), association professionnelle à vocation mondiale

IETF : *Internet Engineering Task Force* (Détachement de l'ingénierie de l'Internet), groupe international participant à l'élaboration de standards dans le domaine de l'Internet

IFRI : Institut français des relations internationales (France)

IGF : Inspection générale des finances (France)

INRIA : Institut national de recherche en informatique et en automatique (France)

IP : *Internet protocol* (protocole Internet)

IRILL : initiative pour la recherche et l'innovation sur le logiciel libre

IS : Impôt sur les sociétés

ISOC : *Internet Society* (Société de l'Internet)

ITIF : *Information Technology & Innovation Foundation* (Fondation pour les technologies de l'information et l'innovation) (États-Unis)

JAI : Conseil Justice et Affaires intérieures (Union européenne)

MAGIG : *Multistakeholder Advisory Group on Internet Gouvernance* (Groupe de conseil des parties prenantes sur la gouvernance de l'Internet) (Royaume-Uni)

mbps : Mégabits par seconde

MIT : *Massachusets Institute of Technology (*Institut de technologie du Massachusetts)

MOOCs : *Massive Open Online Courses,* ou cours en lignes ouverts et massifs

NCSA : *National center for supercomputing applications* (Centre national pour les applications des super-ordinateurs) (États-Unis)

NSA : *National security agency* (Agence nationale de sécurité) (États-Unis)

NSF : *National science foundation* (Fondation nationale pour la science) (États-Unis)

NTIA : *National Telecommunications and Information Administration* (Administration nationale des télécommunications et de l'information) (États-Unis)

OCDE : Organisation de coopération et de développement économiques

OGF : *Open grid forum* (Forum pour un réseau ouvert)

OGP : *Open government partnership (*Partenariat des gouvernements ouverts)

OMC : Organisation mondiale du commerce

OMPI : Organisation mondiale de la propriété intellectuelle

OPECST : Office parlementaire d'évaluation des choix scientifiques et technologiques (France)

OS : *Operating system* (système d'exploitation)

OTT : *Over the top* (au sommet), contenus ou services fournis par un distributeur utilisant les infrastructures existantes et non les siennes propres

PME : Petites et moyennes entreprises

P2P : *Peer to peer,* de pair à pair

R&D : Recherche et développement

RFID : Identification par radio-fréquence

RCP : Rémunération pour copie privée

RSSAC : *Root Server System Advisory Committee,* comité consultatif placé auprès de l'ICANN

RTI : Règlement des télécommunications internationales

SACD : Société des auteurs et compositeurs dramatiques (France)

SEAE : Service européen pour l'action extérieure (Union européenne)

SGMAP : Secrétariat général pour la modernisation de l'action publique (France)

SMSI : Sommet mondial sur la société de l'information

SRI : Sécurité des réseaux et de l'information

SSAC : *Security and stability advisory committee*, comité consultatif placé auprès de l'ICANN

TCP/IP : *Transmission Control Protocol/Internet Protocol* (protocole de contrôle des transmissions/protocole de l'Internet)

TIC : Technologies de l'information et de la communication

TPE : très petites entreprises

TTIP : *Transatlantic Trade and Investment Partnership*

UE : Union européenne

UIT : Union internationale des télécommunications

URL : *Uniform Ressource Locator*, chaîne de caractères décrivant la localisation d'une ressource sur le Web

VPN : *Virtual private network*, réseau privé virtuel

VTC : Véhicules de tourisme avec chauffeur

W3C : *World wide web consortium* (Organisation pour le réseau mondial)

WICANN : *World ICANN* (ICANN mondiale)

WWW : *World wide web* (réseau mondial)

ANNEXE 2 :

LISTE DES AUDITIONS EFFECTUÉES PAR LA MISSION

- **M. Vinton CERF**, vice-président de Google, le 10 décembre 2013 ;
- **Mme Valentine FERRÉOL**, présidente de l'Institut G9+ et du groupe informatique Arts et Métiers Paristech, le 14 janvier 2014 ;
- **M. Michel SERRES**, membre de l'Académie française, auteur de *Petite poucette* (2012), le 14 janvier 2014 ;
- **M. Pierre BELLANGER**, fondateur et président directeur-général de la radio Skyrock, le 14 janvier 2014 ;
- **MM. Bernard BENHAMOU**, ancien conseiller de la délégation française au sommet des Nations unies pour la société de l'information (2003-2006) et ancien délégué aux usages de l'Internet (2007-2013), et **Laurent SORBIER**, conseiller référendaire à la Cour des comptes, professeur associé à l'université Paris-Dauphine, le 21 janvier 2014 ;
- **Mme Françoise MASSIT-FOLLÉA**, chercheur et consultant senior sur les usages et la gouvernance de l'Internet, le 21 janvier 2014 ;
- **M. Louis POUZIN**, ingénieur, un des pères de l'Internet, inventeur du datagramme, le 21 janvier 2014 ;
- **M. David FAYON**, administrateur des postes et des télécoms, auteur de *Géopolitique d'Internet : qui gouverne le monde ?* (2013), le 28 janvier 2014 ;
- **M. Bernard STIEGLER**, directeur de l'institut de recherche et d'innovation du Centre Pompidou, le 28 janvier 2014 ;
- **M. Bertrand de LA CHAPELLE**, directeur du projet Internet et juridiction, ancien délégué spécial pour la société de l'information au ministère des affaires étrangères (2006-2010), ancien directeur au conseil d'administration de l'Internet corporation for assigned names and numbers (ICANN) (2010-2013), le 4 février 2014 ;
- **M. David MARTINON**, représentant spécial pour les négociations internationales concernant la société de l'information et l'économie numérique, le 4 février 2014 ;
- **M. Jérémie ZIMMERMANN**, porte-parole de l'association « La Quadrature du net », le 4 février 2014 ;
- **M. Mathieu WEILL**, directeur général de l'association française pour le nommage Internet en coopération (AFNIC), le 4 février 2014 ;

- **MM. Stéphane GRUMBACH**, directeur de recherche à l'Institut national de recherche en informatique et en automatique (INRIA), et **Julien NOCETTI**, chercheur à l'Institut français des relations internationales (IFRI), et **Mme Pauline TÜRK**, maître de conférences en droit public à l'Université de Lille II, le 11 février 2014 ;
- **M. Viktor MAYER-SCHÖNBERGER**, professeur à l'*Oxford Internet Institute*, spécialisé en gouvernance et régulation de l'Internet, le 11 février 2014 ;
- **M. Jean-François ABRAMATIC**, ancien président du W3C (*World Wide Web consortium*) de 1996 à 2001, le 11 février 2014 ;
- **M. Jean-Michel HUBERT**, ancien président de l'Autorité de régulation des télécommunications, ancien président délégué du comité stratégique pour le numérique, le 18 février 2014 ;
- **M. Gérard DANTEC**, président du chapitre français de l'*Internet society* (ISOC), le 18 février 2014 ;
- **M. Sébastien BACHOLLET**, président d'honneur du chapitre français de l'*Internet society*, le 18 février 2014 ;
- **M. Fadi CHEHADE**, président de l'*Internet corporation for assigned names and numbers* (ICANN), le 21 février 2014 ;
- **MM. Hervé PELLETIER**, président et **Olivier GUÉRIN**, délégué général, de la commission nationale de contrôle des interceptions de sécurité (CNCIS), le 25 février 2014 ;
- **M. Roberto di COSMO**, professeur d'informatique à l'Université Paris-VII, directeur de l''initiative pour la recherche et l'innovation sur le logiciel libre (IRILL), le 25 février 2014 ;
- **M. Jean-Claude MALLET**, conseiller auprès de M. le ministre de la défense, le 4 mars 2014 ;
- **MM. Nicolas COLIN et Henri VERDIER**, coauteurs de *L'Âge de la multitude. Entreprendre et gouverner après la révolution numérique* (2012), le 4 mars 2014 ;
- **Mme Nathalie CHICHE**, membre du Conseil économique, social et environnemental, rapporteure de l'étude *Internet : pour une gouvernance ouverte et équitable* (janvier 2014), le 4 mars 2014 ;
- **M. Hervé COLLIGNON**, associé d'A. T. Kearney, coauteur d'une étude sur le secteur de la haute technologie en Europe (février 2014), le 11 mars 2014 ;
- **MM. Benoît THIEULIN**, président, et **Jean-Baptiste SOUFRON**, secrétaire général, du Conseil national du numérique, le 11 mars 2014 ;
- **MM. Jean-Ludovic SILICANI**, président, et **Pierre-Jean BENGHOZI**, membre du collège, de l'Autorité de régulation des communications électroniques et des postes (ARCEP), le 11 mars 2014 ;

- **MM. Philippe BOUCHER**, conseiller d'État honoraire, et **Louis JOINET**, ancien directeur juridique de la Commission nationale d'informatique et des libertés (CNIL), le 18 mars 2014 ;
- **M. Bernard BAJOLET**, directeur général de la sécurité extérieure, le 18 mars 2014 ;
- **M. Maurice RONAI**, membre élu de la formation restreinte de la Commission nationale de l'informatique et des libertés (CNIL), coauteur du rapport *République 2.0 : vers une société de la connaissance ouverte* (avril 2007), le 18 mars 2014 ;
- **M. Philippe LEMOINE**, président directeur-général de LaSer, président de la Fondation pour l'Internet nouvelle génération, chargé par le Gouvernement en janvier 2014 d'une « mission pour la transformation numérique de notre économie », le 25 mars 2014 ;
- **M. Andrew WYCKOFF**, directeur de la science, de la technologie et de l'industrie à l'Organisation de coopération et de développement économiques (OCDE), le 25 mars 2014 ;
- **Mme Vanessa GOURET**, conseillère chargée de la politique commerciale et des règles du commerce international, **M. Yohann PETIOT**, chef de cabinet adjoint, conseiller chargé des relations avec le Parlement et les élus, auprès de Mme la ministre du commerce extérieur, et **M. Aymeric PONTVIANNE**, chef du bureau de la politique commerciale, de l'OMC et des accords commerciaux de l'Union européenne, à la direction générale du trésor, le 25 mars 2014 ;
- **Me Winston MAXWELL**, avocat, associé du cabinet Hogan Lovells, le 25 mars 2014 ;
- **Mme Gabrielle GAUTHEY**, vice-présidente d'Alcatel-Lucent, présidente de la commission innovation du Mouvement des entreprises de France (Medef), et **MM. Yves LE MOUËL**, directeur général de la Fédération française des télécoms (FFT), **Giuseppe de MARTINO**, secrétaire général de Dailymotion, président de l'Association des services Internet communautaires (ASIC), **Loïc RIVIÈRE**, vice-président du comité stratégique de la filière numérique (CSFN), et **Éric SCHERER**, directeur de la prospective à France télévisions, vice-président du groupement des éditeurs de services en ligne (GESTE), le 1er avril 2014 ;
- **Mme Catherine TRAUTMANN**, députée au Parlement européen, ancienne ministre de la culture et de la communication, le 1er avril 2014 ;
- **M. Jacques TOUBON**, ancien ministre, délégué de la France pour la fiscalité des biens et services culturels, le 1er avril 2014 ;
- **M. Thierry BRETON**, ancien ministre de l'économie, des finances et de l'industrie, président directeur-général d'Atos, chargé de deux missions sur le *cloud* par le Gouvernement et par la Commission européenne, le 8 avril 2014 ;

- **Maître Olivier ITEANU**, avocat à la Cour d'appel de Paris et président d'honneur de l'Internet Society France, le 8 avril 2014 ;
- **MM. Jacky RICHARD**, rapporteur général, et **Laurent CYTERMANN**, rapporteur général adjoint, du Conseil d'État, le 8 avril 2014 ;
- **M. Vincent CHAMPAIN**, directeur des opérations de General Electric France, le 10 avril 2014 ;
- **Mme Anne-Thida NORODOM**, professeur à l'université de Rouen, co-directrice du centre universitaire rouennais d'études juridiques, le 10 avril 2014 ;
- **Mmes Céline CASTETS-RENARD**, professeur à l'Université Toulouse I Capitole, co-directrice du master 2 « droit et informatique », **Jessica EYNARD**, docteur en droit, auteur de *Les données personnelles, quelle définition pour un régime de protection efficace ?* (2013), et **Valérie PEUGEOT**, vice-présidente du Conseil national du numérique, présidente de l'association Vecam et prospectiviste à Orange Labs, et **M. Francesco RAGAZZI**, chercheur associé au centre d'études et de recherches internationales (CERI) de Sciences Po Paris et maître de conférences à l'université de Leiden (Pays-Bas), le 15 avril 2014 ;
- **M. Philippe BOILLAT**, directeur général, et **Mme Sophie KWASNY**, chef de l'unité « protection des données » au sein du service de la société de l'information, de la direction générale des droits de l'Homme et de l'État de droit du Conseil de l'Europe, le 15 avril 2014 ;
- **Mme Isabelle FALQUE-PIERROTIN**, présidente de la Commission nationale de l'informatique et des libertés (CNIL), le 15 avril 2014 ;
- **M. Giacomo LUCHETTA**, chercheur au *Centre for European policy studies* (CEPS) de Bruxelles, le 22 avril 2014 ;
- **M. Boris BEAUDE**, géographe, chercheur au sein du laboratoire Chôros de l'École polytechnique fédérale de Lausanne (Epfl), le 22 avril 2014 ;
- **MM. Per STRÖMBÄCK**, responsable du forum Netopia, **Peter WARREN**, co-auteur du rapport *Can we make the digital world ethical ?* (février 2014), publié par cette organisation, et **Murray SHANAHAN**, professeur à *City University* à Londres, le 22 avril 2014 ;
- **M. Jan Philipp ALBRECHT**, député au Parlement européen, membre de la commission des libertés civiles, de la justice et des affaires intérieures, le 28 mai 2014 ;
- **M. David MARTINON**, représentant spécial pour les négociations internationales concernant la société de l'information et l'économie numérique, le 28 mai 2014 ;

- **Mme Axelle LEMAIRE**, secrétaire d'État chargée du numérique, auprès du ministre de l'économie, du redressement productif et du numérique, le 3 juin 2014.

ANNEXE 3 : LISTE DES DÉPLACEMENTS

BRUXELLES

LUNDI 3 FÉVRIER 2014

(1) Composition de la délégation

– M. Gaëtan GORCE, sénateur de la Nièvre, président de la mission commune d'information (MCI)

– Mme Catherine MORIN-DESAILLY, sénatrice de Seine-Maritime, rapporteure de la MCI

– M. Jean BIZET, sénateur de la Manche, membre de la MCI

(2) Programme

9h00 Entretien avec **M. Peter HUSTINX**, contrôleur européen de la protection des données

10h30 Entretien avec **M. Maciej POPOWSKI**, Secrétaire général adjoint du Service européen pour l'action extérieure (SEAE), et **Mme Joëlle JENNY**, directrice de la division K3 du SEAE, Politique de sécurité et sanctions

12h15 Déjeuner de travail avec **M. Luigi GAMBARDELLA**, président d'ETNO *(European Telecommunications Network Operators Associated)*

14h45 Entretien avec **Mme Corugedo STENEBERG**, Directrice générale de la DG Connect de la Commission européenne, et **M. Michael NIEBEL**, Conseiller pour l'Internet à la DG Connect

16h45 Entretien avec **Mme Françoise LE BAIL,** Directeur général de la DG Justice de la Commission européenne

18h00 Entretien avec **M. Jean-Youri MARTY**, directeur adjoint de la branche 4 (capacités, équipements et formation) à l'Agence européenne de défense (AED)

BERLIN

(1) Composition de la délégation

– M. Gaëtan GORCE, sénateur de la Nièvre, président de la MCI

– Mme Catherine MORIN-DESAILLY, sénatrice de Seine-Maritime, rapporteure de la MCI

– M. André GATTOLIN, sénateur des Hauts-de-Seine, vice-président de la MCI

(2) Programme

MERCREDI 12 MARS 2014

8h30 Entretien avec **M. Gerd BILLEN**, secrétaire d'État au Ministère fédéral de la Justice et de la Protection des consommateurs

9h45 Entretien avec **M. Martin FLEISCHER**, sous-directeur en charge de la coordination cybersécurité au Ministère fédéral des Affaires étrangères

11h00 Entretien avec **M. Detlef DAUKE**, directeur de la politique des technologies de l'information, au Ministère fédéral de l'Économie et de l'Énergie et avec **M. Winfried HORSTMANN**, directeur-adjoint à la Chancellerie fédérale en charge de la politique énergétique, de l'industrie et de l'innovation

13h00 Entretien avec la **nouvelle Commission pour le numérique du Bundestag**

Participants :
– **M. Jens KOEPPEN** (CDU/CSU), président de la Commission
– **M. Gerold REICHENBACH** (SPD), vice-président de la Commission
– **M. Maik BEERMANN** (CDU/CSU)
– **Mme Saskia ESKEN** (SPD)
– **M. Christian FLISEK** (SPD)
– **M. Thomas JARZOMBEK** (CDU/CSU)
– **M. Christina KAMPMANN** (SPD)
– **M. Marian WENDT** (CDU/CSU)
– **M. Jens ZIMMERMANN** (SPD)

14h30 Entretien avec **M. Hans-Christian STRÖBELE (**Bündnis 90/Die Grünen), député, membre de l'Organe de contrôle parlementaire, en charge du contrôle des services de renseignement

16h00 Entretien avec **Mme Dorothee BÄR**, députée (CDU/CSU), secrétaire d'État parlementaire au Ministère fédéral des transports et des infrastructures numériques

JEUDI 13 MARS 2014

9h00 Entretien avec **M. Dirk ARENDT** et **Mme Lena-Sophie MÜLLER**, membre du Präsidium de l'association « Initiative D 21 »

10h15 Entretien avec **M. Henning LESCH**, représentant de M. Harald SUMMA, président de l'association « Eco »

14h15 Entretien avec **Mme Anke DOMSCHEIT-BERG**, spécialiste E-Gvt au sein du Parti pirate

15h30 Entretien avec **M. Andy MÜLLER-MAGUHN**, ancien membre de l'ICANN, spécialiste de la gouvernance Internet

ÉTATS-UNIS

(1) Composition de la délégation

– M. Gaëtan GORCE, sénateur de la Nièvre, président de la MCI

– Mme Catherine MORIN-DESAILLY, sénatrice de Seine-Maritime, rapporteure de la MCI

– M. Jean BIZET, sénateur de la Manche, membre de la MCI

(2) Programme à Washington

LUNDI 28 AVRIL 2014

9h30 Entretien avec **M. Howard SHELANSKI**, *administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget, Executive Office of the President*

11h00 Entretien avec **l'Ambassadeur Daniel SEPULVEDA**, *deputy assistant Secretary of State* et *coordinator for International Communications and Information Policy, Bureau of Economic and Business Affairs, State Department*

12h15 Déjeuner de travail avec **M. Ken SALAETS**, *director, Global Policy, Information Technology Industry Council*

14h00 Entretien avec **Mme Julie BRILL**, *commissionner, Federal Trade Commission*

15h30 Entretien avec l'équipe *Public Policy* de Facebook (**Mme Marne LEVINE** et **M. Matt PERAULT**)

17h15 Entretien avec le représentant **John SHIMKUS** (Républicain, élu dans l'Illinois), *member of the House Energy & Commerce Subcommittee on Communications and Technology, Sponsor of H.R. 4342, the Domain Openness Through Continued Oversight Matters (DOTCOM) Act of 2014*

19h00 Dîner à la résidence de l'ambassadeur de France aux États-Unis, M. François DELATTRE, avec une délégation de l'Assemblée parlementaire de l'OTAN

MARDI 29 AVRIL 2014

10h00 Entretien au Congrès avec **M. Philip MURPHY**, assistant parlementaire du représentant démocrate Mike Doyle, élu de Pennsylvania

13h00 Entretien au Congrès avec le représentant **F. James SENSENBRENNER**, Jr. (Républicain, élu dans le Wisconsin), *senior member of the House Judiciary and Science, Space & Technology Committees*

14h00 Entretien à la ***Federal Comunications Commission*** (FCC) avec **M. Louis PERAERTZ**, *legal advisor for Wireless, International, and Public Safety* du **commissaire CLYBURN**, suivi de réunions de travail avec les services de la FCC

16h30 Entretien avec **M. Lawrence STRICKLING**, *assistant Secretary for Communications and Information* et administrateur de la *National Telecommunications and Information Administration (NTIA)*

17h45 Entretien avec **Mme Laura DeNARDIS**, professeur à l'American University, *Senior Fellow au centre for International Governance Innovation* et directrice de la recherche pour la Commission internationale sur la gouvernance de l'Internet

MERCREDI 30 AVRIL 2014

8h30 Entretien avec **M. Marc ROTENBERG**, président de *l'Electronic Privacy Information Center* (EPIC)

9h45 Entretien avec **M. Robert D. ATKINSON**, président de *l'Information Technology & Innovation Foundation*

11h00 Entretien avec l'équipe *Public Policy* de Google (**Mme Aparna SRIDHAR** et **Mme Sarah FALVEY**)

12h45 Déjeuner de travail avec **M. Milton L MUELLER**, professeur à la *Syracuse University, School of Information Studies*

(3) Programme à Boston

JEUDI 1ER MAI 2014

10h00 Entretien avec le **professeur Nazli CHOUCRI**, *Massachussetts Institude of Technology*

12h30 Déjeuner avec **M. Philippe LE HEGARET** du *World Wide Web Consortium* (W3C)

15h30 Entretien avec **Mme Cynthia LAROSE**, directrice du département *Privacy & Security Practice* au cabinet Mintz Levin

17h00 Panel sur l'éducation numérique (professeurs de Harvard et MIT) au *Cambridge Innovation Center*

19h00 Dîner chez le consul général de France à Boston, **M. Fabien FIESCHI**, avec des entrepreneurs du net :
– M. Clément CAZALOT, DocTrackr

– **M. François DUCROUX**, Winslows Evans & Crocker / president de la FSCCNE
– **M. Chris HOTE**, Digimind
– **M. Philippe TARTAVULL**, Comverse
– **M. Aymeric VIGNERAS**, Sharalike / Avincel Consulting
– **M. Yannick WITTNER**, Dassault Systèmes

(4) Programme à New York

VENDREDI 2 MAI 2014

10h30 Entretien avec **M. Adam SEGAL** du *Council on foreign affairs*

12h00 Entretien avec le **professeur E. NOAM** de *Columbia University*

ANNEXE 4 :
DÉCLARATION MULTIPARTITE À L'ISSUE DE LA CONFÉRENCE NETMUNDIAL DE SÃO PAULO (24 AVRIL 2014)

Global Multistakeholder Meeting on the Future of Internet Governance
NETmundial

Préambule

Cette déclaration non-contraignante résulte d'un processus participatif ascendant et ouvert impliquant des milliers de parties prenantes issues des gouvernements, du secteur privé, de la société civile, de la communauté technique, et des universitaires du monde entier. La conférence NETmundial était une première du genre. Elle devrait contribuer à l'évolution de l'écosystème de gouvernance d'Internet.

INTRODUCTION

La réunion multipartite mondiale sur l'avenir de la gouvernance de l'Internet, également connue sous le nom de NETmundial, s'emploie à considérer deux questions importantes quant à l'évolution future de l'Internet, de manière ouverte et multipartite :

1. Les principes de gouvernance de l'Internet
2. La feuille de route pour l'évolution future de l'écosystème de gouvernance de l'Internet

Les recommandations contenues dans ce document sont formulées dans le but de guider le NETmundial vers un consensus. Il s'agit d'un effort collaboratif regroupant des représentants de tous les groupes de parties prenantes.

Plus de 180 contributions ont été reçues des parties prenantes du monde entier. Ces contributions ont servi de base à l'élaboration des recommandations ci-dessous soumises aux participants de NETmundial ci-dessous pour parvenir à un consensus élargi.

Les recommandations de NETmundial pourront également constituer une contribution potentiellement importante pour d'autres forums et entités de gouvernance de l'Internet.

1. PRINCIPES DE GOUVERNANCE DE L'INTERNET

NETmundial a identifié une série de valeurs importantes et de principes communs qui contribuent à un cadre de gouvernance de l'Internet inclusif, multipartite, efficace, légitime et évolutif, et a reconnu que l'Internet était une ressource mondiale qui devait être gérée dans l'intérêt du public.

DROITS DE L'HOMME ET VALEURS COMMUNES

Les droits de l'homme, comme l'indique la Déclaration Universelle des Droits de l'Homme, sont universels, et doivent sous-tendre les principes de gouvernance de l'Internet. Les droits dont les individus jouissent **hors ligne** doivent également être protégés **en ligne**, en conformité avec les obligations juridiques internationales en matière de droits de l'homme, y compris les pactes internationaux sur les droits civils et politiques et les droits économiques, sociaux et culturels, ainsi que la Convention relative aux droits des personnes handicapées. Ces droits incluent, sans s'y limiter :

- **La liberté d'expression :** Tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répandre, sans considérations de frontières, les informations et les idées par quelque moyen d'expression que ce soit.

- **La liberté d'association :** Toute personne a droit à la liberté de réunion et d'association pacifiques en ligne, y compris à travers les réseaux sociaux et les plateformes.

- **La vie privée :** Le droit à la vie privée doit être protégé. Il consiste notamment à ne pas faire l'objet de surveillance, de collecte, de traitement et d'utilisation de données personnelles de manière arbitraire ou illégale. Le droit à la protection de la loi contre de telles immixtions ou de telles atteintes devrait être assuré.

    - Les procédures, les pratiques et la législation concernant la surveillance des communications, leur interception et la collecte de données personnelles, y compris la surveillance, l'interception et la collecte de masse devraient être revues en vue de protéger le droit à la vie privée en assurant la mise en œuvre pleine et efficace de toutes les obligations internationales en matière de droits de l'homme

- **L'accessibilité :** Les personnes handicapées doivent pouvoir jouir d'un accès complet aux ressources en ligne. Il faut promouvoir la conception, le développement, la production et la distribution d'informations, de technologies et de systèmes accessibles sur Internet.

- **La liberté d'information et l'accès à l'information :** Chacun devrait avoir le droit d'accéder, de partager, de créer et de distribuer l'information sur l'Internet, dans le respect des droits des auteurs et des créateurs tels qu'ils sont définis par la loi.

- **Le développement :** Tout individu a droit au développement, et l'Internet peut apporter une contribution vitale à la pleine réalisation des objectifs de développement durable convenus sur le plan international. C'est un outil essentiel pour permettre aux personnes en situation de pauvreté de participer au processus de développement.

PROTECTION DES PRESTATAIRES INTERMÉDIAIRES

Des limites de responsabilité des prestataires intermédiaires devraient être définies de manière à respecter et promouvoir la croissance économique, l'innovation, la créativité et la libre circulation de l'information. À cet égard, la coopération entre toutes les parties

prenantes devrait être encouragée afin de s'attaquer aux activités illicites et les décourager, selon un processus équitable.

DIVERSITÉ LINGUISTIQUE ET CULTURELLE

La gouvernance de l'Internet doit respecter, protéger et promouvoir la diversité culturelle et linguistique sous toutes ses formes.

UN ESPACE UNIFIÉ ET NON FRAGMENTÉ

L'Internet doit continuer à être un réseau de réseaux mondialement cohérent, interconnecté, stable, non fragmenté, évolutif et accessible, basé sur un ensemble commun d'identifiants uniques et permettant aux paquets de données et à l'information de circuler librement de bout en bout quel que soit le contenu licite.

SÉCURITÉ, STABILITÉ ET RÉSILIENCE DE L'INTERNET

La sécurité, la stabilité et la résilience de l'Internet devraient être des objectifs prioritaires pour toutes les parties prenantes de la gouvernance de l'Internet. En tant que ressource universelle mondiale, l'Internet se doit d'être un réseau sécurisé, stable, résilient, fiable et digne de confiance. L'efficacité face aux risques et aux menaces en matière de sécurité et de stabilité de l'Internet repose sur une forte collaboration entre les différentes parties prenantes.

ARCHITECTURE OUVERTE ET DISTRIBUÉE

L'Internet doit être préservé en tant qu'environnement fertile et innovant, basé sur une architecture système ouverte, une collaboration sur la base du volontariat, une gestion et une participation collective. La nature intrinsèquement ouverte de l'Internet de bout en bout se doit d'être défendue, et les experts techniques sollicités pour résoudre les problèmes techniques de manière appropriée et en accord avec cette approche ouverte et collaborative.

CRÉER UN ENVIRONNEMENT PROPICE À L'INNOVATION ET À LA CRÉATIVITÉ DURABLES

La capacité à créer et à innover est au cœur de la remarquable croissance de l'Internet et elle a enrichi la société dans son ensemble. Afin de préserver son dynamisme, la gouvernance de l'Internet doit continuer d'autoriser des innovations sans demande de permission, par le biais d'un environnement en ligne propice et en accord avec les autres principes de ce document. Les initiatives et les investissements dans l'infrastructure constituent des éléments essentiels d'un environnement favorable.

PRINCIPES DU PROCESSUS DE GOUVERNANCE DE L'INTERNET

- **Participation multipartite :** L a gouvernance de l'Internet devrait reposer sur des processus démocratiques et multipartites, garantissant la participation valable et responsable de toutes les parties prenantes, comprenant les gouvernements, le secteur privé, la société civile, la communauté technique et universitaire et les utilisateurs. Les responsabilités et rôles respectifs des parties prenantes devraient être interprétés avec un certain degré de flexibilité selon le sujet en discussion.

- **Gouvernance ouverte, participative et consensuelle :** Le développement de politiques publiques internationales relatives à l'Internet et le dispositif de gouvernance de l'Internet devraient permettre la participation entière et équilibrée de toutes les parties prenantes de par le monde, d'une manière consensuelle, dans la mesure du possible.

- **Transparence :** Les décisions prises doivent être simples à comprendre, les processus être clairement documentés et suivre les procédures convenues, et enfin, les procédures être élaborées et approuvées selon des processus multipartites.

- **Responsabilité :** Des mécanismes de contre-vérification indépendants ainsi qu'un système de révision et de recours devraient exister. Les gouvernements détiennent la responsabilité principale, juridique et politique en matière de protection des droits de l'homme.

- **Inclusion et équité** : Les institutions et les processus de gouvernance de l'Internet doivent être inclusifs et ouverts à toutes les parties prenantes intéressées. Les processus, y compris ceux de prises de décisions, devraient être ascendants pour permettre la pleine et entière participation de toutes les parties prenantes, de manière à ne désavantager aucune catégorie.

- **Distribution** : La gouvernance de l'Internet devrait se faire dans un écosystème distribué, décentralisé et multipartite.

- **Collaboration** : La gouvernance de l'Internet devrait être basée sur des approches collaboratives et coopératives qu'elle encourage et qui reflètent les contributions et les intérêts des parties prenantes.

- **Possibilité d'une participation significative :** Tout individu concerné par un processus de gouvernance de l'Internet devrait pouvoir y participer. Plus spécifiquement, les institutions et les processus de gouvernance de l'Internet devraient soutenir le renforcement de capacité pour les nouveaux arrivants, particulièrement les parties prenantes des pays en développement ou de groupes sous-représentés.

- **Accès et faibles obstacles :** La gouvernance de l'Internet doit promouvoir un accès universel, égalitaire, abordable et de bonne qualité, afin que l'Internet puisse être un outil efficace au service du développement humain et de l'inclusion sociale. Il ne devrait pas y avoir d'obstacles exagérés ou discriminatoires à l'entrée de nouveaux utilisateurs. L'accès public est un outil puissant pour fournir un accès à l'Internet.

- **Agilité :** Les politiques d'accès aux services Internet doivent être tournées vers le long-terme et être neutres sur le plan technologique afin de pouvoir s'adapter aux technologies qui évoluent rapidement et aux différents types d'usages.

STANDARDS OUVERTS

La gouvernance de l'Internet devrait promouvoir les standards ouverts, qui s'appuient sur l'expertise individuelle et collective et sur les décisions prises par consensus approximatif, permettant ainsi l'accès de tous à un réseau mondial, interopérable, résilient, stable, décentralisé, sécurisé et interconnecté. Les standards doivent être compatibles avec les droits de l'Homme et permettre le développement et l'innovation.

2. FEUILLE DE ROUTE POUR L'ÉVOLUTION FUTURE DE LA GOUVERNANCE DE l'INTERNET

L'objectif de la feuille de route proposée pour l'évolution future de la gouvernance de l'Internet est de souligner les possibles étapes dans le processus d'amélioration continue du cadre existant de gouvernance de l'Internet en s'assurant de l'entière implication de toutes les parties prenantes selon leurs rôles et responsabilités respectifs.

Le dispositif de gouvernance de l'Internet est un écosystème distribué et coordonné qui implique divers organisations et forums. Ce dispositif doit être inclusif, transparent et responsable, et ses structures et opérations doivent suivre une approche qui permet la participation de toutes les parties prenantes afin de répondre aux intérêts de tous ceux qui utilisent l'Internet comme de ceux qui ne sont pas encore connectés.

La mise en œuvre de l'Agenda de Tunis a démontré l'intérêt d'un modèle multipartite pour la gouvernance de l'Internet. Il faut reconnaître la précieuse contribution de toutes les parties prenantes dans la gouvernance de l'Internet. Grâce à toutes ces expériences fructueuses, ce modèle devrait être renforcé, amélioré et développé.

La gouvernance de l'Internet devrait inciter le développement durable et inclusif pour la promotion des droits de l'Homme. La participation devrait refléter la diversité géographique et inclure des parties prenantes de pays en développement, des pays les moins développés, ainsi que des états insulaires en développement.

I. Questions méritant l'attention particulière de toutes les parties prenantes dans l'évolution future de la gouvernance de l'Internet

1. Les décisions liées à la gouvernance de l'Internet sont parfois prises sans la réelle participation de toutes les parties prenantes. Il est essentiel d'améliorer la prise de décisions multipartite et l'élaboration de politiques afin d'assurer l'entière participation de toutes les parties intéressées, tout en reconnaissant les différents rôles joués par les diverses parties prenantes sur les multiples sujets.

2. Il faut mettre en œuvre, de manière prioritaire et consensuelle, la coopération renforcée mentionnée dans l'Agenda de Tunis pour s'attaquer aux questions internationales

de politique publique concernant l'Internet. Si l'on prend en compte les efforts du groupe de travail de la CSTD (*Commission on Science and Technology for Development*) sur la coopération renforcée, il est important que toutes les parties prenantes s'engagent à faire avancer cette discussion de manière multipartite.

3. Des processus ouverts, démocratiques et transparents doivent permettre de désigner des représentants des parties prenantes dans les processus multipartites de gouvernance de l'Internet. Les différents groupes de parties prenantes devraient gérer eux-mêmes leurs processus fondés sur des mécanismes inclusifs, connus du public, bien définis et responsables.

4. Il faut développer des mécanismes multipartites au niveau national car une large part des questions de gouvernance de l'Internet doit être traitée à ce niveau. Les mécanismes multipartites nationaux devraient servir de lien entre les discussions locales et les instances régionales et mondiales. Il est donc essentiel d'encourager une coordination et un dialogue fluides entre ces différentes entités.

5. Il faut une participation significative de toutes les parties intéressées aux discussions sur la gouvernance de l'Internet et à la prise de décision, en tenant compte de l'équilibre en termes géographique, de parties prenantes et de parité, afin d'éviter les asymétries.

6. Il est essentiel d'inciter au renforcement des capacités et à l'autonomisation au travers de mesures telles que la participation à distance, un financement approprié, et un accès en temps et en heure à des informations satisfaisantes, afin de promouvoir une gouvernance de l'Internet inclusive et efficace.

7. Toutes les parties prenantes devraient renouveler leur engagement à produire une Société de l'Information centrée sur l'humain, inclusive et orientée sur le développement, comme elle a été définie dans les documents issus du SMSI. Il ne faut donc pas perdre de vue le cap sur le développement quand on poursuivra l'amélioration de l'écosystème de gouvernance de l'Internet.

8. Les discussions sur la gouvernance de l'Internet pourraient tirer avantage d'une communication et d'une coordination améliorées entre les communautés techniques et non-techniques, en fournissant une meilleure compréhension des implications politiques des décisions techniques et des implications techniques dans l'élaboration de politiques.

II. Questions liées à l'amélioration institutionnelle

1. Toutes les organisations ayant des responsabilités dans l'écosystème de gouvernance de l'Internet devraient développer et mettre en œuvre des principes de transparence, de responsabilité et d'inclusion. Toutes ces organisations devraient préparer des rapports périodiques sur leur progression et leur état d'avancement concernant ces questions. Ces rapports devront être mis à la disposition du public.

2. Il faudra prendre en compte la possible nécessité de mécanismes pour aborder les nouveaux sujets et débats qui ne sont pas encore suffisamment traités par les dispositifs existants de gouvernance de l'Internet.

3. Le Forum de Gouvernance de l'Internet (FGI) devra être renforcé. Le groupe de travail de la Conférence des Nations Unies sur la science et la technique au service du développement (UNCSTD) sur les améliorations du FGI a formulé des recommandations

importantes en ce sens. Il est suggéré que ces recommandations soient mises en œuvre avant fin 2015.

Les améliorations devraient conduire, entre autres à :

a. Améliorer les résultats : des améliorations peuvent être introduites, passant par exemple par des modalités créatives pour émettre des conclusions/recommandations et l'analyse des options de politique ;

b. Allonger le mandat du FGI à plus de cinq ans;

c. Garantir au FGI un financement stable et prévisible, notamment grâce à une base élargie de donateurs ;

d. Doter le FGI de mécanismes pour promouvoir des discussions mondiales entre les réunions à travers des dialogues intersessions.

Un FGI renforcé pourrait mieux servir de plateforme de discussions des questions au long cours, ainsi que des nouveaux sujets dans le but d'aider à identifier de nouveaux moyens pour y répondre.

4. Il devrait y avoir une communication et une coordination adéquates entre les forums, les groupes de travail et les organisations existantes de l'écosystème de gouvernance de l'Internet. Des rapports périodiques, des discussions officielles et des retours d'expérience réactifs sont des exemples de mécanismes qui pourraient être mis en œuvre à cette fin. Il serait judicieux d'envisager des outils de coordination de la gouvernance de l'Internet pour effectuer des vérifications et des analyses continues, et pour partager l'information.

5. Suite à l'annonce récente et bien accueillie du gouvernement américain concernant son intention de transférer la supervision des fonctions IANA, la discussion sur les mécanismes garantissant la transparence et la responsabilité de ces fonctions, une fois le rôle du gouvernement américain terminé, devra se faire de manière ouverte avec le concours de toutes les parties prenantes au-delà de la communauté ICANN.

Plusieurs organisations et forums accueillent les dispositifs qui permettent de développer les politiques selon lesquelles sont actuellement exercées les fonctions IANA. Tout mécanisme adopté devrait protéger la nature ascendante, ouverte et participative de ces processus de développement de politiques et assurer la stabilité et la résilience de l'Internet. Une discussion sur la relation appropriée entre les aspects politiques et opérationnels devrait avoir lieu.

Cette transition devrait être mise en œuvre de manière réfléchie, en mettant l'accent sur le maintien de la sécurité et de la stabilité de l'Internet, en favorisant le principe de participation équitable de tous les groupes de parties prenantes, et en faisant l'effort de terminer la transition avant septembre 2015.

6. Le processus de mondialisation de ICANN est sensé s'accélérer et aboutir à une organisation vraiment internationale et globale au service de l'intérêt du public avec des mécanismes de transparence et de responsabilité vérifiables et faciles à mettre en œuvre, de manière à satisfaire les demandes des parties prenantes internes ainsi que de la communauté dans son ensemble.

La représentation active de toutes les parties prenantes dans la structure ICANN, en provenance de toutes les régions, est un des points clé de la réussite du processus de mondialisation.

III. Questions liées spécifiquement à la gouvernance de l'Internet

1. Sécurité et stabilité

a. Il faut renforcer la coopération internationale sur les sujets tels que les questions de juridiction et l'assistance à l'application des lois afin de promouvoir la cybersécurité et prévenir la cybercriminalité. Les discussions sur ces structures doivent faire l'objet de participation multipartite.

b. Les initiatives pour améliorer la cybersécurité et contrer les menaces sur la sécurité numérique devraient impliquer une collaboration appropriée entre gouvernements, secteur privé, société civile, universitaires et communauté technique. Certaines parties prenantes doivent encore s'engager davantage en matière de cybersécurité, comme par exemple les fournisseurs de réseaux et les développeurs de logiciels.

c. De nouveaux forums et de nouvelles initiatives devront trouver leur place. Toutefois, ils ne devront pas dupliquer, mais au contraire compléter les structures existantes. Toutes les parties prenantes devraient essayer de tirer parti de ces organisations de cybersécurité existantes et de les améliorer. L'expérience cumulée de plusieurs d'entre elles démontre que l'efficacité de toute initiative de cybersécurité dépend de la coopération entre les différentes parties prenantes, ce qui ne peut résulter d'une organisation ou structure unique.

2. La surveillance arbitraire de masse mine la confiance envers l'Internet et son écosystème de gouvernance. Le recueil et le traitement de données personnelles par des acteurs étatiques et non étatiques devraient être effectués dans le respect du droit international des droits de l'Homme. Il est nécessaire d'inciter à davantage de dialogue à ce sujet au niveau international par le biais de forums tels que le Conseil des droits de l'homme et le FGI afin de promouvoir une compréhension commune de tous les aspects de la question.

3. Le renforcement des capacités et le financement constituent des exigences essentielles pour s'assurer que les différentes parties prenantes aient l'opportunité d'une participation plus que symbolique, et qu'elles acquièrent le savoir-faire et les ressources nécessaires à une réelle participation. Le renforcement des capacités soutiendra l'émergence de véritables communautés de parties prenantes, surtout dans les régions où la participation de certains groupes d'acteurs doit encore être consolidée.

IV. Points à débattre au-delà de NETmundial :

Plusieurs contributions à NETmundial ont identifié ci-après une liste non-exhaustive de domaines qui nécessitent d'être mieux compris et débattus dans les forums appropriés:

- Les différents rôles et responsabilités des acteurs de la gouvernance de l'Internet, y compris le sens et l'application de l'expression « sur un pied d'égalité ».

- Les questions de juridiction et leurs liens avec la gouvernance de l'Internet.

- Les systèmes d'évaluation et d'indicateurs associés concernant l'application des principes de gouvernance de l'Internet.

- La neutralité du Net : Des discussions importantes et très productives ont eu lieu à NETmundial sur la question de la neutralité du Net, avec des points de vue différents concernant l'inclusion ou non de ce terme spécifique comme principe dans les conclusions. Les principes comprennent les concepts d'Internet ouvert et de droits

individuels à la liberté d'expression et d'information. La discussion sur l'Internet ouvert doit se poursuivre et prendre en compte la manière de favoriser la liberté d'expression, la concurrence, le choix du consommateur, la vraie transparence et la gestion appropriée du réseau, et nous préconisons que ces points soient débattus lors de forums tels que la prochaine réunion du FGI.

V. Marche à suivre

Toutes les organisations, les processus et tous les forums de l'écosystème de gouvernance de l'Internet sont invités à prendre en compte les conclusions de NETmundial.

Les constatations et les conclusions de NETmundial seront intégrées par d'autres processus et forums, tels que le Programme de Développement Post-2015, le SMSI +10, le FGI, et toutes les discussions sur la gouvernance de l'Internet des différentes organisations et instances à tous niveaux.

Les futurs débats et les discussions de suivi sur les sujets figurant dans ce document doivent servir de base de travail aux entités et aux instances existantes. Nous les invitons à présenter un rapport de leurs activités lors de grandes réunions sur la gouvernance de l'Internet.

ANNEXE 5 :
DOCUMENT DE SYNTHÈSE SUR L'INTERNET ÉLABORÉ PAR L'INRIA

DIRECTION DE LA RECHERCHE

Document de synthèse sur Internet

Editeur : Frédéric Desprez (Frederic.Desprez@inria.fr)

Contributeurs : Claude Castellucia (claude.castelluccia@inria.fr), Isabelle Chrisment (isabelle.chrisment@inria.fr), Walid Dabbous (walid.dabbous@inria.fr), Arnaud Legout (arnaud.legout@inria.fr), Jonathan Rouzaud-Cornabas (jonathan.rouzaud-cornabas@inria.fr), Luc Saccavini (luc.saccavini@inria.fr), Damien Saucez (Damien.Saucez@inria.fr)

Architecture et socle technologique d'Internet

L'Internet est bâti sur un modèle de réseau de réseaux où coopèrent des acteurs différents (fournisseurs d'infrastructures, de services, de contenus, utilisateurs, etc.) souvent concurrents. Le bon fonctionnement de cette tour de Babel planétaire est garanti par la mise en œuvre d'une base technologique commune dont l'objectif est de répondre à une fonction simple : la transmission de messages. Ces messages doivent pouvoir être transmis entre deux points quelconques du réseau Internet, leur taille pouvant varier de quelques octets à quelques milliards d'octets. Ces messages doivent être transmis de façon fiable, efficace, tout en partageant équitablement la capacité des liens (de quelques dizaines de Mbit/s à des centaines de Gbits/s). Ces messages doivent aussi pouvoir transiter par des supports de transmission variés comme les ondes hertziennes (wifi, téléphonie 2G, 3, 4G...) ou encore des supports physiques (fibre optique, paires torsadées cuivre) dont les caractéristiques techniques (fiabilité, débit, coûts) varient sur plusieurs ordres de grandeur. Une des bases d'Internet est d'avoir l'intelligence à la périphérie du réseau et un cœur de réseau simple.

Pour satisfaire ces contraintes en partie contradictoires, le modèle technologique repose sur deux principes : la communication de « bout en bout » pour la gestion des messages et le « meilleur effort » (*Best Effort*) pour leur acheminement. Le principe du « bout en bout » implique que les deux entités partenaires d'une communication (ex. smartphone / serveur) dialoguent directement pour garantir le bon échange des messages. Chaque message est découpé en paquets que les éléments intermédiaires des réseaux (les routeurs) sont chargés d'acheminer, sans intervenir dans le dialogue entre émetteur et récepteur des messages. Le protocole TCP (*Transmission Control Protocol*) est une implémentation de ce principe, tout objet qui veut se connecter à Internet doit être capable de « faire du TCP » (à de rares exceptions près). Une session TCP est principalement définie par 2 numéros ou ports : le port destination qui définit aussi la nature du service (web, messagerie, vidéo) que l'initiateur de la session veut utiliser et le port source qui permet d'identifier chacune des sessions TCP initiées par un objet donné. Les rôles de serveur et de client sont définis simplement : l'initiateur d'une session TCP est le client et le serveur est son correspondant qui accepte l'ouverture de la session.

Le principe du « meilleur effort » s'applique à la transmission des paquets constituant le message par l'infrastructure réseau. Ce principe implique que les équipements réseaux font ce qu'ils peuvent pour acheminer au mieux les paquets (qui peuvent ne pas arriver à destination, ou arriver dans le désordre). Cette non fiabilité, qui est compensée par TCP, permet de définir un protocole robuste et simple : le protocole IP. Son fonctionnement est basé sur l'algorithme du postier : chaque élément du réseau (ou routeur), choisit le routeur à qui il va transmettre le paquet IP en fonction de son adresse de destination. Cette simplicité du protocole IP permet aux opérateurs d'infrastructure réseau de coopérer sur la base de contrats de services relativement simples à instancier commercialement : l'échange de flux de paquets IP. Elle permet aussi à l'infrastructure d'évoluer dynamiquement (pertes de liens, évolutions topologiques) sans impact sur les communications (sessions TCP) en cours.

Le protocole IP est le véritable cœur technologique de l'Internet. On peut retenir que sa principale caractéristique est que chaque paquet possède une adresse source (qui caractérise l'émetteur) et une adresse destination (qui caractérise le récepteur à qui le paquet doit être remis). Ces adresses IP sont codées sur 32 bits ce qui définit un espace d'adressage de 2 milliards d'objets. Ces 32 bits sont présentés en 4 parties qui conduisent à un format du type « a.b.c.d » où a, b, c et d peuvent prendre des valeurs comprises entre 0 et 255

(exemple : 128.12.3.25). Compte tenu de la croissance d'Internet et en particulier de l'internet des objets (réseaux de capteurs, systèmes embarqués…), cet espace devient insuffisant et une nouvelle version de ce protocole (IPv6) est en cours de déploiement. En IPv6 les adresses sont codées sur 128 bits ce qui étend quasiment « à l'infini » cet espace d'adressage, puisqu'il autorise jusqu'à 7 x 10^{23} adresses IP par m^2 de la surface de la terre !

Du point de vue technologique, il n'y a pas d'autorité centrale, mais des acteurs qui interagissent économiquement, sur la base de protocoles éprouvés, définis dans des standards ouverts publiquement et collectivement élaborés et dont les spécifications sont librement disponibles.

En synthèse technique de cette description succincte des protocoles de base d'Internet, on peut retenir que chaque objet connecté à Internet doit posséder 1 adresse IP (au moins). Une session TCP/IP est ainsi identifiée de façon unique par 4 numéros : 2 adresses IP et 2 ports TCP (dits chacun source et destination) correspondants aux deux entités qui échangent des messages. L'identification de machines par des numéros IP n'est pas commode pour des utilisateurs, il faut donc pouvoir faire cette identification de façon plus ergonomique, c'est le rôle d'un autre composant clé d'Internet : le DNS.

Le DNS

Alors qu'au début de l'Internet le nombre de machines interconnectées était petit, il était facile pour un humain de retenir l'adresse IP de chaque machine et de s'y connecter directement en utilisant cette adresse. Cependant, la taille du réseau a rapidement augmenté et ce sont des milliers d'adresses que les utilisateurs devaient retenir. Pour pallier à cette complexité, un système d'indirection a été proposé. Le principe étant que chaque machine dispose d'un nom non ambigu et unique que les utilisateurs peuvent utiliser pour se connecter à la machine. Comme le protocole IP ne comprend pas les noms, mais uniquement les adresses, ces noms doivent être traduits en adresses. La première approche a été de construire un fichier commun, le fichier "hosts" qui est installé sur toutes les machines du réseau. A chaque changement, le fichier doit être corrigé et synchronisé entre toutes les machines du réseau. Le réseau prenant de l'ampleur, il devint rapidement ardu de garder le fichier "hosts" synchronisé sur toutes les machines et à cela s'ajoutait la complexité de nommer les machines de manière unique. Pour cette raison les concepts de noms de domaines et de DNS (*Domain Name System*) ont été proposés et déployés dès les années quatre-vingt.

Le DNS est donc un annuaire réparti qui permet de passer d'un espace de nommage humainement compréhensible pour désigner les machines connectées à Internet, aux informations techniques comme leurs adresses IP. Par exemple le site www.assemblee-nationale.fr a comme adresse IP 89.185.59.149. Quand un internaute écrit le texte suivant http://www.assemblee-nationale.fr/ dans son navigateur cette information provoque l'ouverture d'une session TCP sur le port destination 80 (service=web) vers la machine d'adresse IP destination 89.185.59.149.

L'espace de nommage du DNS est hiérarchique. Un arbre de nommage est ainsi créé par délégation de sous espaces en cascade. Chaque nœud représente une entité à nommer (ex., un domaine administratif, un serveur). Afin d'éviter toute ambiguïté, tous les fils d'un nœud reçoivent un nom différent et le nom global pour un nœud correspond à la concaténation du nom de chaque nœud suivant la hiérarchie entre lui et le sommet de l'arbre. Le premier niveau est constitué de deux ensembles : les domaines nationaux ou ccTLD (*country code Top Level Domain*) et les domaines génériques ou gTLD (*general Top Level Domain*). Les ccTLD réfèrent des pays (.fr pour la France, .es pour l'Espagne, etc) les gTLD des domaines généraux (.com pour commercial, .edu pour les sites académiques, .org pour les organisations). Le DNS comprend actuellement 320 TLD, 265 millions de domaines dont 105 dans le gTLD .com. L'ICANN (*Internet Corporation for Assigned Names and Numbers*), est une autorité de régulation qui a été mise en place pour gérer le sommet de la hiérarchie du système de nommage dans l'Internet. Le rôle de l'ICANN est d'une part de déterminer les règles de nommage et de s'assurer du bon fonctionnement des serveurs qui composent la racine du DNS. Le rôle de l'ICANN est aussi déterminant dans la création de nouveaux TLD ou même des alphabets pouvant être utilisés pour construire des noms.

La gestion des (13 systèmes) racines est l'une des 3 missions principales de l'ICANN. La gouvernance de l'ICANN est régie par un long document, initié en 1999 et dont la dernière mouture date de 2002[1]. Ce texte fait de nombreuses références à la loi californienne « CNPBCL » (*California Nonprofit Public Benefit Corporation Law*). Là où il est évident que pour maintenir de l'ordre dans un système de nommage de l'ampleur du DNS il est nécessaire de se référer à une autorité centrale, il y a une certaine controverse autour de l'ICANN et de ses liens plus ou moins proches avec le gouvernement américain du fait que l'ICANN est intrinsèquement lié au département du commerce des Etats-Unis. Par exemple, d'aucun pourrait voir une sur-représentativité d'organisations basées aux Etats-Unis dans l'attribution des serveurs racines du DNS[2]. Ceci dit, cela vient principalement de raisons historiques. Toutefois, comme l'attribution se fait de manière assez statique suivant des schémas administratifs complexes, il est assez ardu de pouvoir déployer une racine DNS officielle, ce qui pourrait mettre en péril la neutralité du système de nommage qui est le pilier de l'Internet tel que nous le connaissons aujourd'hui.

La possibilité de créer de nouveaux gTLD a été décidée en 2008 et a été lancée en 2012. Le nombre de gTLD va très probablement augmenter dans un avenir proche, avec l'arrivée de gTLD comme .paris, .banque, .sncf par exemple. Il y a eu 1800 demandes de nouveaux gTLD déposées auprès de l'ICANN, mais compte tenu des critères de sélection et du coût élevé (180k$ pour l'examen complet d'un dossier, puis 25k$/an), le nombre final de nouveaux gTLD est pour l'instant estimé à 1200.

Chaque gérant de TLD va déléguer la gestion d'une sous-zone à une entité qui en fait la demande légitime. Ainsi l'AFNIC qui gère le .fr va déléguer au prestataire qui gère le site web de l'Assemblée Nationale le domaine 'assemblee-nationale.fr', ce dernier pourra ensuite organiser l'espace de nommage 'assemblee-nationale.fr' à sa guise. Il peut nommer directement des machines, créer d'autres sous-domaines, etc.

La structure hiérarchique du nommage DNS crée une pseudo sémantique (.fr = France, .com = sté commerciale) qui peut être trompeuse. En effet, une machine sous .fr peut être située n'importe où sur la planète, et sur le territoire français il peut y avoir des machines de pratiquement n'importe quel TLD.

Une partie de la sécurité d'Internet repose sur le DNS, en particulier l'authentification des serveurs applicatifs. Comment être sûr que l'adresse IP 89.185.59.149 est bien celle du serveur www.assemblee-nationale.fr ? Un protocole complémentaire (DNSSEC) permet de garantir par signature numérique que les informations DNS sont correctes. Le déploiement de DNSSEC commencé en 2009 par la signature de la racine du DNS se poursuit doucement. Par exemple sur .fr 20 000 domaines étaient signés fin 2012 (sur 2,5 millions).

Quand un internaute connecte son terminal (*smartphone*, PC, tablette) à Internet, via un point d'accès privé (ADSL domestique), d'entreprise ou public, cette connexion est fonctionnelle quand le point d'accès a affecté à son terminal une adresse IP, l'adresse IP du routeur le plus proche et l'adresse IP du serveur DNS à utiliser.

Racines ouvertes

En alternative au système de racines officiel, la mouvance des racines ouvertes (*open roots* en anglais) est de plus en plus marquée. L'idée des racines ouvertes est de ne plus lier le devenir des racines DNS à une seule autorité, mais de déployer les racines de manière coopérative à la place. La majorité des racines ouvertes reprennent le schéma de l'ICANN avec la délégation des racines à des entités bien déterminées. Cependant d'autres approches se veulent complètement coopératives et reprennent le schéma bien connu des réseaux pair-à-pair où chaque utilisateur du système devient aussi contributeur. L'utilisation des racines ouvertes permet de casser l'aspect monopolistique qui règne actuellement dans la gestion du sommet de la hiérarchie DNS et offre de ce fait plus de flexibilité et de liberté dans la gestion des noms dans l'Internet, par exemple en autorisant l'utilisation des alphabets et langues locales. Les approches fortement décentralisées permettent aussi de lutter efficacement contre la censure et la répression et donc d'assurer un accès libre à l'Internet et

[1] www.icann.org/en/about/governance/bylaws

[2] Voir http://fr.wikipedia.org/wiki/Serveur_racine_du_DNS (tableau repris en **Annexe 1**)

d'empêcher les formes de répressions numériques qui sont de plus en plus nombreuses[3,4]. Cette liberté peut cependant compromettre la cohérence de l'ensemble car elle supprime l'unicité globale des noms dans l'Internet. Les racines ouvertes posent aussi des problèmes juridiques avec un contrôle difficile de l'attribution des noms aux différentes entités et donc le risque pour les marques de perdre le contrôle sur leur nom dans l'Internet.

Sur ce sujet de racines ouvertes, Julien Naillet, en charge de la communication de l'Afnic (Association française pour le nommage Internet en coopération) déclare : « *Nous accueillons avec intérêt toute initiative en faveur de l'innovation et de la concurrence. Néanmoins, il nous semble essentiel de garantir aux utilisateurs l'unicité des noms de domaine en usage. La multiplication des racines, bien que pouvant offrir de nouvelles fonctionnalités au cas par cas, est donc une voie sur laquelle nous ne souhaitons pas nous engager.* » Il est important de garder une autorité sur le sujet mais qu'elle soit sous contrôle indépendant et ouvert. Plus précisément, la participation dans l'autorité devrait être libre, gratuite, non-gouvernementale et non-commerciale afin de laisser la tribune à tout acteur du monde numérique, tant individuel qu'organisationnel. La raison pour laquelle il est important de maintenir une autorité est lié au besoin de conserver un système assurant l'unicité des noms à l'échelle globale, et sans ambiguïté, tout comme recommandé par l'Afnic. Un autre point qui nous semble important est de rendre complètement libre et décentralisé le déploiement de serveurs racines alors qu'aujourd'hui seules les entités approuvées par l'ICANN sont autorisées à déployer des serveurs racines officiels. L'aspect décentralisé étant à mettre en avant afin de réduire le risque de censure au maximum.

BGP: le protocole qui assure le fonctionnement global d'Internet

Comme cela a été expliqué précédemment, Internet est un réseau de réseaux. Chacun de ces réseaux est appelé *Autonomous System* (AS[5]), il en existe 45 000 (début 2014). Le protocole BGP (*Border Gateway Protocol*) permet à ces différents AS de communiquer, c'est-à-dire d'échanger du trafic de paquets IP. Pour cela, chaque AS va dire à ses voisins quels préfixes (ensembles d'adresses IP) il sait router. Soit parce que les machines correspondantes à ces préfixes sont dans son AS, soit parce qu'il a un voisin qui sait router ces préfixes. Ces informations de routage vont permettre aux AS de cœur de connaître toutes les routes de l'Internet (500000 actuellement) et d'acheminer n'importe quel paquet vers sa destination. Par exemple c'est l'AS CLARANET-AS N° 8426 de la sté ClaraNET Ltd qui possède le préfixe incluant l'adresse IP 89.185.59.149 et qui annonce à ses voisins qu'il sait router les paquets IP correspondants. BGP est, avec TCP/IP et DNS, une des briques essentielles d'Internet car c'est ce protocole qui permet aux différents AS qui forment Internet de communiquer. Tout comme ces deux derniers, il est basé sur des protocoles ouverts. De plus, BGP est construit sur une confiance absolue entre les différents AS. Comme un AS peut annoncer qu'il est capable de router des préfixes correspondant à des terminaux qui ne sont pas dans son réseau il a la possibilité de détourner par son système des données à destination d'un autre. Ces attaques ont été vues plusieurs fois ces dernières années[6]. Elles vont permettre de facilement espionner le trafic à destination ou en provenance d'une partie du réseau sans avoir à installer du matériel ou aller modifier les systèmes qui sont attaqués.

Pour transférer des données d'un AS à un autre, des opérateurs dits de transit IP (ou de cœur) vont fournir les liaisons qui permettent ce transfert. Certains de ces transits sont payants en fonction de la capacité du lien et du volume données qui vont y transiter. Un acteur majeur est Open Transit qui appartient à Orange mais aussi Cogent ou Level 3 qui sont des sociétés étrangères. Ces acteurs ne sont pas visibles par les utilisateurs mais disposent d'un grand pouvoir puisqu'ils sont en charge d'interconnecter les différents systèmes qui fondent Internet mais ils pourraient aussi surveiller le trafic de leurs clients passant dans leurs liaisons. Pour autant, afin de diminuer les coûts, il existe des accords dit de peering entre les différents acteurs d'Internet. Un accord de peering permet d'échanger gratuitement du trafic entre 2 systèmes (AS). De tels accords existent entre la plupart des fournisseurs de contenus et d'accès sur Internet. Cela se base sur un trafic symétrique (entrant et

[3] http://www.lefigaro.fr/secteur/high-tech/2011/01/26/01007-20110126ARTFIG00639-face-a-la-revolte-l-egypte-muscle-sa-censure-du-web.php
[4] http://www.lefigaro.fr/flash-actu/2011/10/29/97001-20111029FILWWW00423-la-syrie-a-censure-internet.php
[5] Internet est modélisé et organisé par un ensemble d'AS communicants entre eux.

[6] http://www.bortzmeyer.org/bgp-shunt.html

sortant). Mais de part les nouveaux modèles de consommation sur Internet, il y a eu une perte de symétrie. Par exemple, les clients de Free vont regarder plus de vidéos sur Youtube qu'ils vont en envoyer. L'excédent doit passer par des transits IP payants. Il est nécessaire de conserver ces accords de peering afin de conserver une bonne qualité du réseau. Des combats commerciaux existent pour savoir qui doit payer pour augmenter la capacité des liaisons de transit IP ainsi que ceux de peering. Un exemple concret est le ralentissement de Youtube pour les clients de Free de fait d'une bataille commerciale entre les 2 sociétés. Une des caractéristiques originales du protocole BGP est donc de prendre en compte (à travers son paramétrage) aussi bien des caractéristiques technologiques (optimisation du routage des paquets IP) que des éléments commerciaux (implémentation de l'accord de peering entre deux opérateurs d'AS).

Elaboration des standards

L'élaboration des standards de l'Internet est principalement portée par l'IETF (*Internet Engineering Task Force*). Il s'agit d'une organisation ouverte où les participations sont individuelles. Toute personne peut participer (il suffit que son employeur le paye pour cela), et son poids dans l'élaboration des standards sera directement lié à sa capacité à agir et à la qualité de ses propositions de protocoles. L'objectif premier de l'IETF est de produire des spécifications de protocoles appelées RFC les plus efficaces, les plus simples et les plus lisibles possibles afin de faciliter leur implémentation dans les systèmes. Pour cela, quelques règles simples sont mises en œuvre : les documents sont tous publics, et discutés publiquement. De plus un projet de spécification ne peut passer la première étape de validation que si deux implémentations en ont été faites de façon indépendante et coopèrent comme prévu. Ces points méthodologiques, garantissent d'être à l'état de l'art, l'efficacité des protocoles et la lisibilité des documents de référence.

A titre indicatif, l'IETF produit environ 250 RFC par an dont la moitié sont des propositions de standards. Au bout d'un processus qui peut durer plusieurs années, 2 à 3 de ces propositions deviennent chaque année des standards aboutis ayant un caractère obligatoire. L'implication de la France est notable dans ce processus et représente 4% de cette production à travers des auteurs issus du monde académique et industriels (France-Telecom, Orange, INRIA, AFNIC, Alcatel Lucent, Renater, SFR, Bouygues Telecom, Institut Telecom, ...). D'autres organismes participent à l'élaboration des standards de l'Internet, comme le W3C (web), l'IEEE et l'ETSI (liens physiques, hertziens, filaires), l'OGF (services répartis) et d'autres encore sur des domaines très spécifiques.

Indépendance numérique de la France

A côté de la gouvernance ISOC, la véritable gouvernance revient de plus en plus aux acteurs économiques. On observe un glissement historique depuis les équipementiers, telco jusqu'aux producteurs de contenus actuellement.

L'économie numérique est reconnue aujourd'hui comme une des premières économies mondiales, mais l'importance de l'indépendance numérique des états est largement sous-estimée ce qui peut conduire à moyen terme à une profonde modification des équilibres géopolitiques.

La France sur les 40 dernières années a fait le choix d'un protectionnisme d'anciens modèles économiques au détriment de nouveaux modèles innovants. Ce choix a conduit à une forte dépendance numérique envers notamment les États-Unis. Deux cas emblématiques illustrent ce choix : l'adoption d'Internet et le téléchargement pair-à-pair. L'Internet a longtemps été opposé au minitel en France, les responsables politiques et dirigeants de grands groupes considérant Internet comme étant un produit américain devant être freiné face au minitel. En effet, le minitel avait un modèle économique stable et bien maîtrisé : l'accès payant a tous les services avec une facturation sur la ligne téléphonique rattachée. Cette lutte contre Internet fut paradoxale puisque des chercheurs français jouèrent un rôle de premier plan dans sa conception, notamment Louis Pouzin et Christian Huitema, chercheurs visionnaires qui comprirent très tôt le potentiel énorme d'Internet, mais qui ne furent pas suivis par les dirigeants de l'époque.

Le deuxième cas emblématique est celui du téléchargement en pair-à-pair (utilisant majoritairement BitTorrent) qui fut stigmatisé. Cependant, ce soudain succès du téléchargement pair-à-pair montrait que les nouveaux modes de communication et les attentes du grand public ne correspondaient plus aux modes historiques de diffusion des contenus audiovisuels. Dans ce cas également, la France a été précurseur avec

Azureus/Vuze (le client BitTorrent le plus populaire créé par un français Olivier Chalouhi qui est parti en Californie pour développer sa société), Wizzgo (le premier magnétoscope numérique déporté condamné par décision de justice à arrêter ce service pourtant précurseur des actuels services de vidéos à la demande), et les succès relatifs que sont Dailymotion et Deezer (qui sont pourtant parfaitement compétitifs avec les leaders mondiaux Youtube et Spotify, mais qui manquent de contenus).

Bien que le contexte soit très différent dans ces deux cas, la même erreur fut reproduite : vouloir conserver un ancien modèle économique bien maîtrisé et refuser un nouveau modèle économique en rupture. Cette stratégie protectionniste n'est plus adaptée dans un contexte mondialisé tel que le permet Internet. En effet, n'importe qui peut accéder de manière totalement transparente à n'importe quel service opéré depuis n'importe quel pays. Lorsqu'un modèle économique alternatif apparait, la seule option valable est de le soutenir, puisqu'en cas d'absence de soutien, ce modèle sera développé à l'étranger sans aucun retour financier pour la France ni aucune possibilité de régulation.

Les conséquences d'une dépendance numérique sont nombreuses :

- perte d'emplois en France au profit de pays ayant développé les nouveaux modèles économiques ;
- difficulté à légiférer et réguler ces nouveaux modèles qui reposent sur de nouveaux services accessibles par Internet ;
- risques d'atteinte à la vie privée puisque les données ne sont pas hébergées en France est qu'il est très difficile d'influer sur un choix stratégique d'une société basée à l'étranger ;
- risque de pénurie numérique lorsqu'une seule société basée à l'étranger a le monopole de la fourniture d'un service à forte valeur ajoutée (Google, Facebook, Twitter, iTunes, Dropbox, Amazon, etc.)

L'identification des enjeux liés à l'indépendance numérique de la France et les choix stratégiques afférents relève de compétences scientifiques, technologiques et politiques de haut niveau. Aucun acteur isolé ne peut prendre de décisions éclairées, il est par conséquent fondamental de renforcer les discussions et collaboration entre les chercheurs, les entrepreneurs et les décideurs politiques.

Sécurité et chiffrement

Au niveau d'Internet, la plupart des services utilisent des mots de passe et le chiffrage des communications. Pour les mots de passe, il arrive trop souvent que les bases de données des sites web ne soit pas chiffrées (ou faiblement) et que des grands ensembles de mots de passe se retrouvent dans le domaine public. Comme il n'y a pas de loi forçant les entreprises et les sites web à divulguer ces attaques et mises à disposition de données, il n'est pas forcément simple de savoir si un mot de passe a été compromis. De plus, une grande partie du chiffrage des communications repose sur le protocole SSL (https par ex). Hors, tout comme les noms de domaines, les certificats SSL utilisés pour l'authentification du serveur reposent sur une structure stricte et très contrôlée par les USA. La corruption du système de certificat aurait des impacts encore plus grands en termes de sécurité que celles des serveurs DNS. En effet, il serait possible de se faire passer pour un site commercial ou gouvernemental et de lire les informations envoyées entre les utilisateurs et le site.

Il est possible de chiffrer les données avant de les envoyer sur un canal qui est sécurisé ou pas. On peut prendre l'exemple du site mega.co.nz (ou de cryptocat) qui place le chiffrement du côté de l'utilisateur. Par conséquent, même si les données sont lues lorsqu'elles circulent ou lorsqu'elles sont stockées, elles sont chiffrées. Cela permet de garantir une meilleure sécurité à un hébergeur car il ne peut pas savoir ce qu'il stocke et donc en être tenu responsable. Par contre, dans le cas du Cloud, on se retrouve avec des données chiffrées dans le Cloud et il faut les déchiffrer pour pouvoir les traiter. Ce problème au niveau du Cloud peut être réglé par la cryptographie homomorphique. En effet, en utilisant cette technologie, il est possible de faire des traitements directement sur les données chiffrées et donc faire ces traitements sur des plateformes dont on a moins confiance. Pour le moment, les systèmes de cryptographie homomorphique ont souvent un coût en termes de performance trop important pour être utilisables et/ou ne permettent que l'une des 2 opérations élémentaires (addition, multiplication).

Enfin, il est maintenant reconnu qu'aussi bien des cœurs de réseaux que des câbles sous-marins, bien qu'utilisant des fibres optiques comme support de transmission ont été espionnés[7]. Cela pose le problème de la sécurité physique de ces infrastructures qui sont pour le moment considérées comme étant de confiance. Pour éviter ces problèmes de communication et détecter les tentatives d'espionnage, certaines banques suisses ont installé un réseau basé sur le cryptage quantique qui rend les méthodes actuelles d'espionnage beaucoup plus complexes. Pour parer à l'espionnage des fibres optiques par écoute directe de la fibre optique, certains équipementiers de matériels optiques (dont Alcatel) proposent des solutions de chiffrement au niveau optique jusqu'à des débits de 10Gb/s par lambdas actuellement.

DataVeillance (Surveillance par les données)

Les révélations récentes sur les programmes d'espionnage de la NSA ont suscité l'émoi et l'inquiétude en France et un peu partout dans le monde. Ces révélations ont eu le mérite de susciter des discussions/débats et des prises de conscience des hommes politiques et des citoyens. Bien que la surveillance soit nécessaire dans certains cas, si elle est bien encadrée, la surveillance de masse est dangereuse pour la démocratie et peu efficace[8]. Un autre mode de surveillance qui fait moins parler de lui et qui a été un peu éclipsé par l'impact médiatique de l'affaire NSA, mais qui est au moins autant, voire plus, inquiétant (par son ampleur, par ses acteurs, par ses motivations, par sa furtivité, par son manque de transparence) est la *surveillance de masse sur Internet par des entités privées* (publicitaires, agrégateurs/courtiers de données, réseaux sociaux, fournisseurs de services etc.) qui collectent de plus en plus de données ou métadonnées sur les Internautes[9]. On peut distinguer deux types de collectes : les collectes involontaires et les collectes volontaires (entre autre par les réseaux sociaux).

Collectes passives et involontaires (online tracking). Il existe des centaines d'entreprises qui « tracent » les utilisateurs, souvent à leur insu, lorsqu'ils utilisent l'Internet. L'objectif de ces entreprises est d'identifier les sites visités par les utilisateurs, pour identifier leurs centres d'intérêts et construire des profils. Ces profils sont souvent complétés avec des informations recueillies sur diverses bases de données publiques ou privées. Ils incluent typiquement l'âge, la race, le sexe, le nombre d'enfants, le niveau d'éducation, les achats récents, etc. Ces courtiers en données (*data brokers*), tel qu'Acxiom.com, revendent souvent ces données à des banques, publicitaires, agences de crédits, assurances, partis politiques etc. Le marché est tellement juteux que certaines entreprises proposent même aux utilisateurs de racheter leurs données pour quelques dollars[10] ! Une étude récente effectuée dans le cadre du projet Cnil-Inria Mobilitics a montré que les téléphones mobiles sont eux-aussi largement ciblés et qu'une grande majorité des applications mobiles exfiltre des données privées vers des entités tierces. La plupart des applications mobiles étant « gratuites », les données personnelles deviennent une monnaie virtuelle. Ce phénomène est d'autant plus inquiétant que les mobiles possèdent et génèrent beaucoup d'informations personnelles (localisations, listes de contacts, ...). De plus il est très difficile, voire impossible, d'échapper à cette traque[11].

Collectes « volontaires ». Les données que les utilisateurs publient sur les divers réseaux sociaux (Facebook, Twitter,...) sont, bien entendu, aussi utilisées pour enrichir les profils construits par les divers « *Data Brokers* ». Le développement des gadgets connectés (Fitbit, Withings,...) et du mouvement « *Quantified Self* » qui permet à chacun de « se mesurer » (fréquence cardiaque, calories, sommeil, etc.) pour mieux se connaître est un progrès incontestable et aura probablement un impact positif sur la santé. Cependant les données collectées,

---

[7] **Les câbles sous-marins, clé de voûte de la cybersurveillance**
http://www.lemonde.fr/technologies/article/2013/08/23/les-cables-sous-marins-cle-de-voute-de-la-cybersurveillance_3465101_651865.html

[8] **Surveillance is necessary for security, but not mass-surveillance**
http://www.theguardian.com/commentisfree/2014/feb/11/surveillance-myths-nsa-reform-freedom-act?CMP=twt_gu

[9] **How your Data are being deeply mined** http://www.nybooks.com/articles/archives/2014/jan/09/how-your-data-are-being-deeply-mined/?pagination=false

[10] http://www.technologyreview.com/news/524621/sell-your-personal-data-for-8-a-month/ et http://stream.wsj.com/story/markets/SS-2-5/SS-2-453476/

[11] http://juliaangwin.com/privacy-tools-opting-out-from-data-brokers/

éminemment sensibles car liées à la santé, peuvent aussi être aussi très convoitées par les « *data brokers* ». En effet, imaginer la source d'information que ces données peuvent être pour vos assureurs ou banques (par exemple lors d'une demande de prêt)!

Les dangers. Il existe au moins trois conséquences de ces pratiques qui méritent d'être discutées :

Discrimination par les données : Ces profils peuvent être utilisés pour catégoriser les utilisateurs selon différents critères (par exemple « acheteurs impulsifs », « acheteurs influençables », etc.) afin de fournir des traitements différents. Cette catégorisation peut aboutir à des discriminations inacceptables. Par ailleurs, ces profils étant générés automatiquement, par des algorithmes, ils peuvent parfois être erronés et produire des aberrations.

Manipulation par les données : Les profils peuvent aussi être utilisés pour manipuler les gens en leur présentant les informations de façon à influencer leurs décisions.

Surveillance par les données : Finalement, comme les récentes révélations sur la NSA l'ont montré, ces données et profils peuvent être revendus à divers gouvernements à des fins de surveillance de masse.

Le développement de la collecte des données personnelles est préoccupant car il est aujourd'hui impossible d'y échapper. Cette collecte est omniprésente, à la fois sur l'Internet mais aussi dans le monde physique (vous êtes filmés en permanence dans les magasins, les rues. Vous laissez des traces lorsque vous payez avec votre carte bancaire, prenez les transports en commun, empruntez les autoroutes, utilisez votre téléphone mobile, etc.). Il y a ainsi une inversion entre ce qui est perçu par l'Internaute qui se sent consommateur de services (gratuits) alors qu'il est en fait producteur de données à forte valeur (son comportement, ses connaissances, ses opinions, ...). La technologie se développe beaucoup plus rapidement que la législation sur la protection des données personnelles et des citoyens. Bien que la technologie puisse apporter des solutions, elle ne peut malheureusement pas résoudre tous les problèmes. Il est important d'avoir plus de transparence et de contrôle sur la façon dont nos données sont collectées et utilisées. Il est aussi important de lancer un débat sur la question du « *Big Data* » comme vient de le faire la Maison Blanche[12].

Cloud, Internet of Things

Le Cloud Computing pose des problèmes encore plus complexes d'un point de vue de la sécurité. En effet, le matériel est maintenant virtualisé et ce matériel est disposé dans un lieu distant auquel le client n'a pas accès. Cela amène le concept de confiance sans contact. Il faut faire confiance envers la société qui fournit le service de ne pas espionner les données qui transitent et d'avoir une sécurité suffisante pour garantir sa sécurité et la nôtre. Les méthodes d'évaluation et de certification telles que ebios sont caduques dans ce cas. En effet, il faudrait évaluer la sécurité du système d'information de l'entreprise mais aussi celui de l'ensemble des systèmes d'information de ses fournisseurs (Cloud, etc.). En effet, en sécurité, le niveau de sécurité global est toujours celui du système le plus faible.

Pour autant, est-ce une bonne idée d'avoir un Internet/Cloud purement européen et/ou français comme par exemple l'Internet iranien ou Chinois qui ne sont pas « parfaits » mais permettent via un contrôle très fort de la totalité des infrastructures, services et points d'accès à Internet de limiter la propagation des données. Le Cloud souverain (Cloud spécifique à un pays) ne permet pas de s'affranchir des problèmes de sécurité inhérents aux piratages (par exemple, voir le piratage de Belgium Telecom par la NSA pour récupérer les méta-données sur tous les appels en Belgique). Il permet par contre de s'assurer que la loi nationale/régionale s'applique sur les données et les processus de ce Cloud. Pour autant, cette approche n'a pas tellement de sens car ce n'est pas uniquement le lieu géographique qui compte mais la totalité de la pile matérielle et logicielle qui doivent être souverains dans ce cas. Il faut donc pouvoir redévelopper et produire l'intégralité de la plate-forme Cloud depuis les puces électroniques jusqu'au service SaaS. Cela n'est clairement pas réaliste car équivalent au principe d'interdire tel ou tel fournisseur. Huawei (constructeur chinois d'équipements réseaux) a été interdit car les américains n'ont pas confiance dans le logiciel et les composants qui se trouvent dans ses routeurs. En

[12] Bring on the Big Data Debate, https://cdt.org/blogs/0202bring-big-data-debate

effet, ils pourraient contenir des logiciels permettant la surveillance par la Chine à l'insu des gens qui installent ce matériel. Pour autant, il faut se rappeler qu'en 2008, une agence fédérale américaine s'était rendu compte que certains des routeurs Cisco qu'ils utilisaient étaient des contrefaçons chinoises[13]. Sachant qu'il est possible d'introduire des mécanismes de surveillance cachés (chevaux de troie par exemple) aussi bien dans le logiciel et le matériel, cela aurait pu avoir l'impact que souhaitent éviter les américains en bannissant Huawei. Cela justifie un contrôle de bout en bout du développement à la production. Une entreprise américaine produisant en Chine n'est pas plus sûre qu'une entreprise Chinoise produisant aux USA.

Bien sur, il est possible de réguler les flux d'informations de l'ensemble d'un pays. Quelques sociétés disposent et vendent des équipements permettant à des gouvernements ou des entreprises de surveiller et interdire des flux réseau ciblés. Au niveau d'un pays, pour repérer un flux interdit pour par exemple essayer de contrer la fuite d'information industrielle suite à un pirate, il faudrait utiliser des méthodes fortement intrusives en marquant l'ensemble des documents avec des *watermark* ou DRM et inspecter l'ensemble des paquets/flux sortant de France pour voir si on repère ces documents. Un pays avec un budget conséquent comme la Chine ne réussit pas à imposer un tel contrôle qui a plus de chance de se retourner contre le citoyen que d'améliorer la sécurité des entreprises.

Après si le but est de contrôler les données au sein d'un Cloud, il est possible de pouvoir exprimer ce genre de problème comme une propriété de sécurité/privacy et ensuite d'avoir un (ou un ensemble de) mécanisme(s) qui va (vont) s'assurer que cette propriété est bien respectée. Ces mécanismes de contrôle peuvent être augmentés avec des mécanismes d'assurance qui permettent de fournir la preuve à l'utilisateur que ses demandes de sécurité ont été respectées (une sorte de log).

Pour autant, il faut se méfier des certifications de sécurité. Mettre en place des audits spécifiques au Cloud via une certification donnée par un tiers peut amener de la confiance. Pour autant, les certifications reconnues et utilisées par le secteur de la sécurité informatique tel qu'eBios, CC, ISO 27001, etc. ont montré la limite de ces approches et la décorrélation entre une sécurité effective et une sécurité sur le papier. De plus, il faut que les résultats d'un audit soient appliqués. Pouvoir fournir un Cloud sécurisé passe par un processus de R&D complexe visant à analyser, développer, évaluer chacun des composants (matériels et logiciels) du Cloud. Le but étant de construire progressivement une base de confiance suffisamment large pour fournir ce Cloud sécurisé.

Pour finir, les objets connectés sont de plus en plus nombreux. Mais comme les téléphones portables il y a quelques années, ils ne sont jamais mis à jour ou ont une sécurité approximative. On peut ainsi trouver des dizaines (centaines) de milliers de dispositifs connectés à Internet avec le login/mot de passe par défaut qui est de plus disponible dans la documentation. Enfin, les mécanismes de mise à jour automatique n'existent pas toujours. Pour le moment, les problèmes liés à ces objets connectés sont minimes de part leur faible déploiement et la faible sensibilité des données qu'ils traitent. Pour autant, il devient de plus en plus critique de s'intéresser à leur sécurité de part leur omniprésence de plus en plus forte dans des dispositifs critiques de la vie de tous les jours (domotique, *wearable computing*, etc.).

[13] http://it.slashdot.org/story/08/05/09/164201/fbi-says-military-had-counterfeit-cisco-routers

DIRECTION DE LA RECHERCHE

Annexe 1 : Les treize serveurs* racines du DNS

Lettre	adresse IPv4	adresse IPv6	Autonomous System	Ancien nom	Société	Localisation	Sites (global/local)	Logiciel
A	198.41.0.4	2001:503:ba3e::2:30	AS19836	ns.internic.net	VeriSign, USA	trafic distribué par anycast	6 (6/0)	BIND
B	192.228.79.201	2001:478:65::53 (pas encore dans la zone)	AS4	ns1.isi.edu	USC-ISI (en), USA	Marina Del Rey, Californie, États-Unis	1 (1/0)	BIND
C	192.33.4.12	2001:500:2::c (pas encore dans la zone)	AS2149	c.psi.net	Cogent Communications, USA	trafic distribué par anycast	6 (6/0)	BIND
D	199.7.91.13	2001:500:2d::d	AS27	terp.umd.edu	Université du Maryland, USA	College Park, Maryland, États-Unis	1 (1/0)	BIND
E	192.203.230.10		AS297	ns.nasa.gov	NASA, USA	Mountain View, Californie, États-Unis	1 (1/0)	BIND
F	192.5.5.241	2001:500:2f::f	AS3557	ns.isc.org	Internet Systems Consortium, USA	trafic distribué par anycast	49 (2/47)	BIND, ?
« G »	192.112.36.4		AS5927	ns.nic.ddn.mil	Defense Information Systems Agency (en), USA	trafic distribué par anycast	6 (6/0)	BIND
H	128.63.2.53	2001:500:1::803f:235	AS13	aos.arl.army.mil	United States Army Research Laboratory (en), USA	Aberdeen, Maryland, États-Unis	1 (1/0)	NSD
I	192.36.148.17	2001:7fe::53	AS29216	nic.nordu.net	Autonomica, Suède	trafic distribué par anycast	36	BIND
J	192.58.128.30	2001:503:c27::2:30	AS26415		VeriSign, USA	trafic distribué par anycast	70 (63/7)	BIND
K	193.0.14.129	2001:7fd::1	AS25152		RIPE NCC, Hollande	trafic distribué par anycast	18 (5/13)	NSD
L	199.7.83.42	2001:500:3::42	AS20144		ICANN, USA	trafic distribué par anycast	38 (37/1)	NSD
M	202.12.27.33	2001:dc3::35	AS7500		WIDE Project, Japon	trafic distribué par anycast	6 (5/1)	BIND

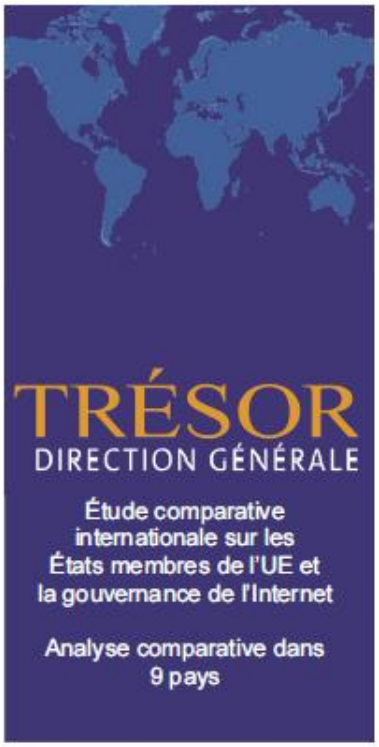
(*) Le terme serveur est à comprendre comme système, chacun de ces « systèmes racines » pouvant comporter un grand nombre de serveurs répartis sur tous les continents pour des questions de robustesse.

ANNEXE 6 :
NOTE DE LA DIRECTION GÉNÉRALE DU TRÉSOR – ÉTUDE COMPARATIVE INTERNATIONALE SUR LES ÉTATS MEMBRES DE L'UNION EUROPÉENNE ET LA GOUVERNANCE DE L'INTERNET

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DES FINANCES
ET DES COMPTES PUBLICS

MINISTÈRE DE L'ÉCONOMIE,
DU REDRESSEMENT PRODUCTIF ET DU NUMÉRIQUE



Contributions des Services économiques des pays suivants :
Allemagne, Belgique, Espagne, Estonie, Italie, Pays-Bas, Pologne, Royaume-Uni, Suède

Mai 2014

DG Trésor – Stratégie, études et pilotage

Ce document de travail, réalisé par le réseau international de la DG Trésor sur la base d'un cahier des charges et questionnaire précis fournis par le(s) commanditaire(s), permet de disposer d'un panorama de diverses situations à l'international. Toutefois, il ne constitue d'aucune manière une prise de position de la DG Trésor (et par extension celle des ministères économique et financier) sur le sujet donné.

La DG Trésor ne peut en aucun cas être tenue responsable de l'utilisation et de l'interprétation de l'information contenue dans ce document.

DG Trésor – Stratégie, études et pilotage

SOMMAIRE

INTRODUCTION

Ce dossier, réalisé pour le compte de la Mission commune d'information du Sénat « Nouveau rôle et nouvelle stratégie pour l'Union européenne dans la gouvernance mondiale de l'Internet » comprend 9 fiches pays analysant la gouvernance de l'Internet dans ces Etats.

I Contexte et objectif de la demande :

Le 6 Novembre 2013, le Sénat a créé une mission commune d'information « Nouveau rôle et nouvelle stratégie de l'UE dans la gouvernance mondiale de l'Internet », initiée par le groupe politique de l'UDI-UC. Elle comprend 33 sénateurs représentant tous les groupes politiques et toutes les commissions permanentes, y compris la commission des affaires européennes.

Cette mission fait suite aux récentes révélations sur l'ampleur du programme de surveillance d'Internet de la NSA, dans un contexte où le contrôle des organes de gouvernance de l'Internet par les Etats-Unis suscite des doutes croissants, entraînant un risque de fragmentation de l'Internet tant les États individuels réagissent.

Son objet est d'analyser la gouvernance de l'Internet d'aujourd'hui et de contribuer à une prise de conscience des enjeux stratégiques en jeu. La mission est convaincue que les Etats membres de l'UE ont un rôle à jouer pour donner lieu à une véritable gouvernance multilatérale de l'Internet afin de défendre leur conception d'un Web basé sur nos valeurs et nos principes démocratiques. Les sénateurs estiment que l'UE peut contribuer à contenir la menace d'une fragmentation de l'Internet.

À cette fin, la mission a procédé à de nombreuses auditions depuis décembre (Vint Cerf, vice-président de Google, Louis Pouzin, Fadi Chehadé, président de l'ICANN, des penseurs comme Michel Serres, des diplomates, des chercheurs, des représentants de la société civile, des entreprises ...). Certains de ses membres se sont rendus à Bruxelles et à Berlin. La mission devrait avoir terminé ses travaux d'ici la fin du premier semestre 2014.

Un voyage aux Etats-Unis est également prévu pour permettre aux membres de la mission de rencontrer certains membres du Congrès américain et des membres de l'administration Obama traitant des questions de l'Internet, les équipes de politique publique des principales entreprises de l'Internet, et les universitaires les plus pertinents.

L'objectif de la demande est, pour la mission sénatoriale, d'enrichir le rapport qu'elle doit publier en juin d'une forme de benchmark des diverses positions des Etats membres de l'UE les plus significatifs, permettant d'évaluer dans quelle mesure chacun de ces pays a identifié la gouvernance de l'internet comme un enjeu politique décisif aujourd'hui.

II Situation française – Réponse pour la France au questionnaire

1. Quelles sont les préoccupations majeures que soulève l'Internet en France ?

Les Français sollicitent activement le réseau Internet et les services qu'il offre en ligne : 8 sur 10 sont des internautes, et parmi eux 9 sur 10 effectuent des achats en ligne et consultent leurs comptes bancaires, 3 sur 10 stockent des documents en ligne et deux tiers possèdent un compte sur les réseaux sociaux.

Toutefois, cette importante activité numérique ne va pas sans des incertitudes notables sur la sécurisation du réseau et de ses services. Ainsi, selon une récente étude, 8 internautes sur 10 s'interrogent sur la protection des informations personnelles, sont inquiets du fait que l'on puisse accéder à leurs informations et ont le sentiment qu'elles ne leur « appartiennent plus réellement ». De la même façon, une étude de la Commission européenne de 2013 classait la France 9ème seulement dans la confiance apportée au commerce électronique parmi les Etats membres.
Outre son impact sur l'opinion publique, accréditant l'idée qu'Internet n'apportait pas à ses utilisateurs toutes garanties de sécurité et de confidentialité, l'affaire Snowden a recentré le débat politique et économique national sur Internet, qui auparavant portait surtout sur les moyens de bloquer l'accès aux contenus illicites en ligne, autour du rôle des Etats et de la protection des données privées.
La notion de « souveraineté numérique » – et ses implications dans un domaine dématérialisé où l'action territorialisée des pouvoirs publics est rendue délicate – est désormais interrogée, souvent pour conclure à son inadaptation aux réalités modernes. Le concept de « co-responsabilité », de « co-souveraineté » de « souveraineté partagée » est avancé comme substitut.
La fiscalité, et notamment l'adaptation des mécanismes d'imposition aux flux immatériels transfrontaliers, est désormais perçue comme un enjeu central, comme l'ont montré l'année dernière le rapport sur la fiscalité du secteur numérique de la mission d'expertise Colin – Collin ou les propositions formulées par le sénateur Philippe Marini, président de la commission des finances du Sénat. Dans un contexte de tension des finances publiques et de perte de compétitivité de nos entreprises, la non-soumission à l'impôt de grandes multinationales du secteur pour l'activité réalisée sur notre territoire, et l'avantage concurrentiel que cela représente par rapport aux entreprises nationales, est vivement ressenti.
L'adaptation aux nouveaux enjeux du cadre légal relatif à la protection des données, très novateur lors de son apparition en 1978 mais dont l'uniformité constitue désormais une limite, est par ailleurs remise en question. La difficulté est de concevoir un nouveau cadre qui soit protecteur sans empêcher la valorisation des données par l'initiative privée, source d'innovation, de croissance et d'emploi, par exemple via le Big Data et l'Open Data.
La question de la sécurisation de données contenues dans un « infonuage » situé dans un pays tiers ou traitées par des opérateurs non européens a été soulevée, et avec elle l'opportunité d'un rapatriement de ces données dans des serveurs situés sur le territoire européen. Une enveloppe a ainsi été mobilisée, au sein du programme des « Investissements d'avenir », pour promouvoir des solutions nationales en ce sens.

2. La place de l'Union européenne dans la gouvernance mondiale de l'internet est-elle un sujet de préoccupation importante en France, soit au niveau politique (exécutif/législatif), soit dans l'opinion publique ? Avez-vous connaissance d'initiatives politiques en ce domaine ?

Ces questions, perçues comme excessivement techniques, ne semblent pas être perçues comme des enjeux majeurs par le grand public, mises à part les associations spécialisées dans le domaine de l'Internet et du numérique (du type La quadrature du Net).
Le gouvernement français a lancé des consultations publiques sur le sujet – en 2009 sur l'Internet du futur, en 2012 sur la révision du Règlement des télécommunications internationales (RTI) en vue de la conférence de Dubaï – qui n'ont été que moyennement relayées.
De façon générale, l'exécutif est resté peu audible sur ces problématiques, y compris vis-à-vis des élus nationaux. La réponse à deux questions écrites posées en 2012 respectivement par les députés Fleur Pellerin et Patrice Martin-Lalande sur sa stratégie lors de ladite conférence a ainsi été publiée six mois plus tard, après le déroulement de cette conférence.
Une certaine sensibilisation du monde politique commence toutefois à se faire jour. Ainsi, les assemblées parlementaires et consultatives se sont saisies du sujet depuis quelques années.
En 2011, les députées Corinne Erhel et Laure de La Raudière ont publié un rapport sur la neutralité de l'internet et des réseaux, qui recommande de définir le concept dans la loi et de fixer sa promotion comme objectif aux autorités réglementaires.
Le rapport rédigé en 2013 par la sénatrice Catherine Morin-Desailly au nom de la commission des affaires européennes, intitulé « L'Union européenne, colonie du monde numérique ? », a mis l'accent

sur les risques d'une perte par l'Europe de son indépendance en matière numérique, et l'urgence de se saisir de la question.
Un rapport publié début 2014 par le Conseil économique, social et environnemental (Cese) intitulé « Internet, pour une gouvernance ouverte et équitable » et présenté par Mme Nathalie Chiche, soulignait que « jusqu'ici, la France et l'Europe ont été inaudibles sur ces questions » et qu'« il est grand temps que l'on s'empare du sujet ».
Dans le prolongement de ce rapport, le Cese a accueilli le 10 mars dernier le premier forum sur la gouvernance d'Internet en France (FGI France). Cette déclinaison nationale du forum international du même nom avait pour but de définir et de consolider une position française sur les grands enjeux du Net, dans la perspective du Netmundial qui aura lieu au Brésil fin avril.

3. Comment la France considère-t-elle le fonctionnement actuel de la gouvernance d'Internet?

La France est globalement attachée au modèle de gouvernance multipartite, qui a fait la preuve de son efficacité mais dont la légitimité pourrait être améliorée.
Elle rejoint ainsi la volonté européenne d'obtenir une universalisation de la convention 108 du Conseil de l'Europe, dont elle partage également les valeurs et que l'UE a invité les Etats-Unis à signer suite à l'affaire Snowden.
Elle questionne l'architecture générale de l'ICANN, dont elle remet en cause l'attachement au gouvernement américain et l'insuffisante représentativité des diverses catégories d'acteurs impliqués dans ces enjeux. Elle estime en effet que ses décisions, bien que formellement techniques, ont une portée politique et économique majeure.
Elle demande par conséquent que le poids des Etats au sein de cette instance soit accru et, dans cette perspective, que le comité consultatif des gouvernements soit professionnalisé et mieux associé au mécanisme de décision ; sont en particulier critiqués le fait que son président n'ait pas voix délibérative au sein du conseil d'administration de l'ICANN, et que ses avis – même consensuels - ne lient pas ce dernier.
Elle milite pour que le lien entre le département du commerce américain et l'ICANN pour la fonction d'enregistrement des noms et des nombres dans la racine soit supprimé, quand bien même aucun abus n'aurait été constaté de la part des Etats-Unis.
Elle plaide pour que la responsabilité de cette instance soit reconnue et institutionnalisée au moyen d'instruments adaptés, comme le respect d'une plus grande transparence dans son fonctionnement, la mise en œuvre du principe d'« accountability » ou l'instauration d'un droit de recours.

4. Quelle est la position des autorités françaises à l'égard du principe de la neutralité du net, et notamment à l'égard de la définition qu'en propose la Commission européenne dans la proposition de règlement « L'Europe, continent connecté » COM(2013) 627 final ?

Les autorités françaises soutiennent la position adoptée par la rapporteure du Parlement européen, Mme del Castillo Vera, en ce qu'elle garantit un service d'accès à l'Internet de qualité tout en permettant le développement d'offres commerciales innovantes (« services spécialisés »). Elles jugent que le rapport de la commission ITRE améliore la proposition de la Commission européenne sur ce thème.

5. Quelles sont les relations entre les pouvoirs publics de la France et l'Association française pour le nommage Internet en coopération (AFNIC) ? Comment cette association se coordonne-t-elle avec l'ICANN et quel est son degré d'autonomie par rapport à ce dernier ? Est-il jugé suffisant pour permettre une stratégie nationale de fixation des noms de domaine ?

L'AFNIC, association de loi 1901, se présente comme un *trustee* chargé, dans l'intérêt général, de gérer une ressource commune, le .fr, point d'appui de la juridiction française. La base de données associée à la gestion des noms de domaine en .fr n'est pas publique : ces données sont communiquées aux autorités françaises si elles en font la demande sur une base légale.

Les relations entre l'AFNIC et l'ICANN sont fondées sur un échange de courriers reconnaissant le bien-fondé de leur action respective. Lors de son audition par la mission sénatoriale, le directeur général de l'AFNIC a indiqué que l'AFNIC demandait à l'ICANN le respect de ses compétences et une internationalisation effective de l'ICANN.

6. Quelle est la position des autorités du pays où vous représentez la France à l'égard de la proposition de règlement européen relatif à la protection des données personnelles en cours de négociation ? Quel avenir envisagent-elles pour l'accord Safe Harbor qui constitue depuis 2001, dans le domaine civil et commercial, le cadre juridique, pour permettre l'échange de données entre entreprises de l'Union européenne et entreprises américaines respectant un certain niveau de protection des données et qui repose donc sur l'auto-certification des entreprises? Quelle est leur position à l'égard de la communication de la Commission européenne publiée le 29 novembre 2013 et appelant au renforcement du « Safe Harbor » ?

La France est favorable aux objectifs poursuivis par la proposition de règlement -assurer un niveau élevé et homogène de protection des données partout sur le territoire de l'Union-, même si elle considère que plusieurs points de cette proposition nécessitent encore d'être travaillés. Elle soutient que la protection offerte par le règlement aux résidents de l'Union doit être la même quel que soit le responsable de traitement collectant et traitant leurs données personnelles. La France souhaite que l'encadrement des transferts de données hors de l'Union européenne soit plus efficace.

En matière de protection des données, au-delà du dossier PRISM, la France reste attentive dans les travaux à venir suite au paquet de communications de la Commission européenne du 29 novembre 2013, tant concernant la volonté de la Commission européenne d'aboutir avant l'été 2014 à la négociation de l'accord parapluie qu'au sujet des propositions de la Commission relatives au renforcement du Safe Harbor.

Service économique régional de Berlin
Chancellerie de l'Ambassade de France

ALLEMAGNE

Éléments locaux de contexte :

Trois sénateurs membres de la mission sénatoriale se sont rendus à Berlin du 11 au 13 mars derniers et ont pu rencontrer les interlocuteurs allemands pertinents sur le sujet. Du fait de la tenue de cette mission, des précisions ne seront apportées que pour les questions 4 à 6. Les réponses aux questions 1 à 3 ont été fournies à la délégation sénatoriale.

Q1/ Quelles sont les préoccupations majeures que soulève l'Internet dans le pays où vous représentez la France ?

Q2/- La place de l'Union européenne dans la gouvernance mondiale de l'internet est-elle un sujet de préoccupation importante dans le pays où vous représentez la France, soit au niveau politique (exécutif/législatif), soit dans l'opinion publique ? Avez-vous connaissance d'initiatives politiques en ce domaine ?

Q3/- Comment le pays où vous représentez la France considère-t-il le fonctionnement actuel de la gouvernance d'internet? Quelle est sa position à l'égard de la communication de la Commission européenne sur la gouvernance de l'internet publiée en février 2014 ?

Q4/- Quelle est la position des autorités du pays où vous représentez la France à l'égard du principe de la neutralité du net, et notamment à l'égard de la définition qu'en propose la Commission européenne dans la proposition de règlement « L'Europe, continent connecté » COM(2013) 627 final ?

Le gouvernement allemand défend la neutralité du net et mise sur la concurrence et la transparence pour garantir un transfert de données sans discrimination et neutre. Les dispositions européennes ont été transposées dans la loi sur les télécommunications (TKG), afin d'imposer des obligations de transparence, des règles claires en cas de changement de fournisseur et des critères de base de protection de neutralité du net. Aux termes de l'article 41a de la loi TKG, le gouvernement peut prendre des dispositions afin de garantir la neutralité du net. L'agence fédérale des réseaux est également compétente pour fixer des critères de base et exiger des fournisseurs des informations.

Une proposition de règlement portant garantie de la neutralité du net avait été élaborée en juin 2013 par le ministère fédéral de l'économie. L'ancien Ministre de l'économie (Philip Rösler, FDP) avait en effet fortement critiqué les projets alors annoncés par Deutsche Telekom de limiter la vitesse de circulation des données sur internet. Cette proposition a été discutée et travaillée par des groupes de travail en aout et en septembre 2013. Le contrat de coalition gouvernementale fixe comme objectif d'insérer la neutralité du net dans la loi sur les télécommunications.

Il existe par ailleurs, depuis 2011, un dialogue d'experts sur la neutralité du net, regroupant des universitaires, des économistes, des politiques et des représentants de la société civile. Il s'est réuni à quatre reprises examinant notamment les aspects juridiques, économiques et internationaux de la neutralité du net.

Selon nos interlocuteurs du Ministère fédéral de l'économie et de l'énergie, leader sur le sujet, les discussions entre les ministères sont en cours sur les possibles propositions de modification à apporter à la proposition de règlement. Ces discussions se poursuivent également sur la suite à donner à la proposition de règlement élaborée sous l'impulsion de l'ancien Ministre. Elles se basent notamment sur les réflexions et discussions du groupe de travail du Conseil sur la proposition de règlement. Par conséquent, les autorités allemandes attendent l'issue des discussions avant d'avancer en interne.

Q5/- Quelles sont les relations entre les pouvoirs publics du pays où vous représentez la France et l'association gérant le nommage sur Internet dans ce pays, équivalent de l'Association française pour le nommage Internet en coopération (AFNIC) ? Comment cette association se coordonne-t-elle avec l'ICANN et quel est son degré d'autonomie par rapport à ce dernier ? Est-il jugé suffisant pour permettre une stratégie nationale de fixation des noms de domaine ?

L'équivalent allemand de l'AFNIC est la DENIC eG, société coopérative créée en 1996 et basée à Francfort. Ses membres (près de 300) sont les entreprises faisant appel à ses services pour la gestion de leurs domaines. Elle gère plus de 15 730 000 domaines en .de. http://www.denic.de/home.html

Le ministère fédéral de l'économie n'a pas de relation formelle et juridique avec la DENIC. Les échanges existent bien sûr, mais de manière informelle. Le ministère souligne par ailleurs qu'il n'aurait pas besoin de mettre en place ou d'avoir un droit de regard sur la gestion des domaines, la DENIC étant soumise au respect du droit allemand et des décisions des tribunaux, qui peuvent exiger la fermeture d'un domaine. La DENIC a, selon le ministère, adopté d'elle-même une politique de surveillance et de gestion efficace, qui ne rend pas nécessaire l'adoption d'une stratégie nationale de fixation des noms de domaine.

La DENIC a les mêmes relations avec l'ICANN que l'AFNIC. Notre interlocuteur au ministère a tenu à souligner les prérogatives de souveraineté nationale dans la gestion des domaines nationaux (.de et .fr).

Q6/- Quelle est la position des autorités du pays où vous représentez la France à l'égard de la proposition de règlement européen relatif à la protection des données personnelles en cours de négociation ? Quel avenir envisagent-elles pour l'accord Safe Harbor qui constitue depuis 2001, dans le domaine civil et commercial, le cadre juridique, pour permettre l'échange de données entre entreprises de l'Union européenne et entreprises américaines respectant un certain niveau de protection des données et qui repose donc sur l'auto-certification des entreprises? Quelle est leur position à l'égard de la communication de la Commission européenne publiée le 29 novembre 2013 et appelant au renforcement du « Safe Harbor » ?

Selon les termes de l'accord de coalition du 27 novembre 2013, la principale préoccupation de l'Allemagne, dans les discussions en cours et à venir, sera de garantir un niveau de protection au moins équivalent à celui déjà élevé qui existe en Allemagne : « nous voulons garantir les standards rigoureux de l'Allemagne en matière de protection des données (…). Les principes de finalité, d'usage restreint et minimal, la condition du consentement, le droit à l'effacement et le droit à la portabilité doivent être inscrits dans le règlement. Les normes de l'UE sur l'entraide judiciaire et policière doivent garantir que le niveau allemand de protection des données soit respecté lorsqu'a lieu un transfert de données vers d'autres Etats de l'UE »[1].

Des consultations franco-allemandes menées à Berlin le 15 janvier 2014 ont permis d'identifier certains points essentiels restant à clarifier dans les négociations ultérieures. Ainsi :

-le champ d'application du règlement, et notamment la distinction entre le secteur privé et le secteur public. Cette distinction structurelle dans la législation allemande a été introduite par la loi fédérale du 20 décembre 1990 de protection des données (Bundesdatenschutzgesetz, texte profondément révisé en 2001).

[1] Accord de coalition CDU, CSU et SPD, *Façonner l'avenir de l'Allemagne*, p.104.

Pour l'Allemagne, des règles distinctes doivent continuer à s'appliquer : non seulement la relation entre l'Etat et les citoyens posent des problèmes juridiques d'une tout autre nature que celle entre les citoyens et les entreprises, mais en outre, le besoin d'harmonisation est bien plus grand dans la sphère économique. La question se pose donc de savoir si le secteur public doit être sorti du champ d'application du règlement (telle est la position allemande), ce qui rendrait nécessaire l'élaboration d'une directive spécifique au cas du secteur public.

-le transfert des données dans les Etats tiers : la loi allemande actuellement en vigueur définit les conditions de transfert de données à caractère personnelle vers un pays tiers. Le §4b de la loi fédérale de protection des données fait notamment obligation aux établissements responsables du transfert de vérifier le niveau de protection des pays tiers[2].

La révélation du programme PRISM ayant montré que les assurances fournies par les pays tiers (au premier chef par les Etats-Unis) pouvaient être largement théoriques, l'Allemagne a fait part de son souhait de renégocier l'accord Safe Harbor, dont les garanties, en termes de contrôle et de protection juridique, sont jugées insuffisantes.

Malgré certaines voix qui s'étaient exprimées en ce sens (cf. la lettre ouverte à la Chancelière et à la Commission de la Conférence des Chargés de la protection des données du 24 Juillet 2014), l'Allemagne n'est pas favorable à la suppression pure et simple de l'accord Safe Harbor. Elle souhaite en revanche le renforcement de cet accord et considère que le règlement européen doit devenir la base juridique solide à partir de laquelle il pourra être approfondi et amélioré.

L'Allemagne milite ainsi pour inscrire dans le règlement européen les règles renforcées de la transmission des données aux Etats tiers. Dans un document conjoint publié le 14 août 2013[3], le ministère fédéral de l'intérieur et celui de l'économie ont proposé un système de déclaration et de demande d'autorisation préalable de transmission des données, de la part des entreprises, auprès des autorités de contrôles. Cette proposition transmise à la Commission a été reprise le 24 janvier dernier par M. Ole Schröder, Secrétaire d'Etat parlementaire au ministère de l'intérieur, qui a suggéré d'insérer en ce sens un article 42a dans le projet de règlement, sans rencontrer toutefois beaucoup d'écho du côté de la Commission.

La position allemande est désormais de s'assurer que le texte du prochain règlement permette d'écarter une éventuelle argumentation des Etats-Unis selon laquelle la protection des données serait un obstacle aux échanges commerciaux. C'est la primauté du principe de protection des données qui doit être réaffirmée.

-le guichet unique : l'Allemagne n'est pas favorable à la proposition de la Commission européenne qui donne la possibilité à une autorité nationale de prendre des décisions valant pour l'ensemble de l'UE[4]. Non seulement cela conduirait à un éloignement géographique considérable de l'instance de recours pouvant être saisie par les citoyens, mais en outre, un tel système risquerait d'entraîner un abaissement du niveau des normes.

C'est pourquoi l'Allemagne est favorable soit à un mécanisme de codécision, soit à un mécanisme d'accord tacite entre autorités de contrôle. Rainer Stentzel, qui dirige le projet « Protection des données » du ministère de l'intérieur, projet chef de file pour la réforme de l'UE sur la protection des données, estime par ailleurs que l'autorité européenne de contrôle prévue par le futur règlement ne saurait être une instance supérieure aux autorités nationales : pour les consommateurs, les entreprises ou les institutions, les autorités nationales respectives en matière de protection des données doivent rester l'organe de surveillance de référence.

[2] A cette fin, l'établissement responsable doit recueillir différentes informations relatives au transfert des données, en particulier : l'origine des données ; l'objectif défini ; la durée du traitement envisagé ; le pays d'origine et le pays destinataire ; les prescriptions, les règles déontologiques et les mesures de sécurité auxquelles le destinataire en question est soumis. Le §4c de la BDSG prévoit les exceptions à ce principe.
[3] *Maßnahmen für einen besseren Schutz der Privatsphäre, Fortschrittsbericht vom 14. August 2013.*
[4] Article §51-2 de la proposition de règlement.

Service économique régional de Bruxelles

BELGIQUE

Éléments locaux de contexte :

Les sujets principaux de préoccupation de l'opinion belge concernant l'internet sont la protection des données personnelles et la cybersécurité, notamment suite aux affaires révélées par Snowden et la NSA et Heartbleed (faille de sécurité des sites web). Belgacom, opérateur historique des télécommunications détenu à 53% par l'État belge, a été victime d'attaques en septembre 2013. Le ministère belge des Affaires Étrangères a subi l'intrusion d'un virus dans son système informatique, en mai 2014. En février 2014, les parlementaires belges ont appelé le gouvernement Di Rupo à renforcer la cybersécurité qu'ils estiment peu performante en Belgique.

Plus généralement, les pouvoirs publics conduisent leurs actions principalement dans le cadre de l'Agenda numérique, à l'horizon 2020, en se focalisant sur la couverture nationale du réseau haut et très haut débit, la transparence de l'offre d'internet, les changements de fournisseurs d'accès à internet (FAI), et la qualité du service.

Pour l'année 2014, l'enveloppe budgétaire pour la cybersécurité s'élève à 10 millions d'euros. La Belgique opte pour une diversification et un renforcement des moyens existants plutôt qu'une concentration des moyens au sein d'un grand service unique. L'enveloppe est répartie entre le CCB (centre belge pour la cybersécurité), le Cert (l'équipe d'intervention urgente en informatique), la FCCU (Federal Computer Crime Unit), la Sûreté de l'État et les Renseignements militaires. Cependant, un plan transversal de sécurisation des télécommunications est envisagé, afin de permettre au SPF Économie (équivalent du ministère de l'Économie) d'exercer un rôle de coordination en matière de planification et de gestion des situations d'urgence dans le secteur des télécommunications.

Q1/ Quelles sont les préoccupations majeures que soulève l'Internet en Belgique ?

Selon le responsable des Télécommunications à la direction générale des Télécommunications et de la Société de l'Information, la cybersécurité est l'une des préoccupations majeures concernant l'Internet en Belgique. Pour y faire face, les pouvoirs publics belges proposent de :

- développer une offre européenne de composants informatiques et d'entreprises du secteur, afin d'assurer l'indépendance de l'Union européenne dans ce domaine. NDRL Belgacom fait appel à du matériel chinois (Huawei) pour l'intégralité de ses équipements ;
- renforcer l'offre européenne de cloud computing pour assurer une meilleure protection des données et de la vie privée;
- promouvoir le recours aux marchés publics européens, moyen efficace pour assurer la fourniture de matériels d'origine européenne.

La réduction de la fracture numérique est également un sujet de préoccupation pour la partie belge. Les organismes compétents mènent des actions de formation auprès des publics exclus de l'internet. En 2012, 15% des particuliers en Belgique n'avait jamais utilisé internet ;

Service économique régional de Bruxelles

Q2/- La place de l'Union européenne dans la gouvernance mondiale de l'internet est-elle un sujet de préoccupation importante en Belgique ?

Selon notre interlocuteur, les pouvoirs publics belges estiment que l'Union européenne devrait être plus présente dans la gouvernance mondiale de l'Internet. Ils préconisent notamment l'adoption de principes communs aux États membres, au niveau du conseil des ministres, la mise en place rapide de l'Observatoire mondial de la politique de l'internet (GIPO), plateforme en ligne qui favorisera la transparence des politiques liées à l'internet ainsi que le renforcement du dialogue stratégique avec les pays émergents, notamment l'Afrique et le Brésil.

Q3/- Comment la Belgique considère-t-elle le fonctionnement actuel de la gouvernance d'internet?

Ci-après dans son intégralité, le document, daté du 26 février 2014, transmis par la délégation belge au groupe télécoms du Conseil.

"Working Party on Telecommunications and Information Society

BE comments - Internet Policy and Governance communication

La Belgique se félicite de la communication de la Commission européenne. Les discussions menées en matière de gouvernance d'internet devraient constituer une priorité de l'Union européenne.

En ce qui concerne les débats relatifs au Sommet mondial sur la Société de l'Information, la Belgique qui réaffirme son attachement au modèle pluri-acteurs, tout en reconnaissant que le modèle actuel doit être amélioré (pt.3). La valeur de l'IGF doit être soulignée, tout en reconnaissant la nécessité de renforcer la procédure de « coopération renforcée », au sein des entités existantes. Cet objectif peut être atteint par l'amélioration des compétences et de la représentativité du comité consultatif gouvernemental de l'ICANN (pt.4). La Belgique est favorable à la mise en place, à court terme et selon un calendrier précis, d'un secrétariat du GAC permanent et doté d'une structure pleinement indépendante. L'ICANN ne doit s'écarter des avis du GAC que de façon exceptionnelle.

L'internationalisation de l'ICANN doit se poursuivre. La participation des États émergents doit être renforcée, notamment par l'amélioration du programme de traduction des principaux documents et l'affectation des bénéfices résultant de la procédure d'attribution des gTLD à des mesures de sensibilisation et à la prise en charge des coûts de participation. La Belgique est favorable aux propositions relatives à la participation inclusive des acteurs concernés et à la mise en œuvre de « l'Observatoire mondial de la politique de l'internet » (GIPO) de la Commission européenne (pt.5). Un dialogue devrait être entamé avec les pays émergents, notamment les États africains, afin d'éviter que ceux-ci n'optent pour un modèle purement intergouvernemental. Certains de ces pays pourraient devenir des partenaires économiques importants pour l'Union européenne. Les discussions devraient être menées, en priorité, avec le Brésil qui semble constituer un interlocuteur fiable et modéré.

La Belgique se félicite que l'accent soit mis sur l'adoption rapide de la proposition de directive « cybersécurité » (pt.7). Une recommandation devrait être adoptée pour encourager l'utilisation des logiciels « open source » qui permettent aux utilisateurs d'en contrôler le contenu.

En ce qui concerne la question des conflits de loi (pt.8), la Belgique propose que la question du lien territorial des noms de domaine nationaux ccTLD devrait être évoquée au niveau européen afin de consacrer une règle comparable au principe territorial applicable aux marques de commerce. Enfin, une offre européenne de produits « cloud computing » doit être développée, afin de garantir le respect de la règlementation européenne applicable en matière de vie privée.

Il est nécessaire de renforcer la coopération au niveau européen, voire de porter cette discussion au Conseil des ministres, afin de permettre l'adoption de principes communs aux États membres. »

Service économique régional de Bruxelles

Q4/- Quelle est la position des autorités belges à l'égard du principe de la neutralité du net, et notamment à l'égard de la définition qu'en propose la Commission européenne dans la proposition de règlement « L'Europe, continent connecté » COM (2013) 627 final ?

Selon « l'Étude portant sur la neutralité du réseau (Internet) et les mesures de gestion du trafic », commandée par le SPF Économie, la Belgique est en avance sur les prérogatives européennes en matière de neutralité du réseau dont la définition est en accord avec celle proposée dans le règlement « L'Europe, continent connecté ». Les pouvoirs publics sont déjà engagés dans cette voie en concentrant leur action dans les domaines suivants :

- transparence : obligation des fournisseurs d'accès à internet – FAI – de donner toutes les informations sur la vitesse et les volumes de téléchargement sans toutefois être tenus d'expliciter les priorités des flux sur leur réseau ;
- changement d'opérateur de réseau et de FAI : les pouvoirs fédéraux limitent la possibilité des opérateurs de réclamer des indemnités lors de la résiliation d'un contrat ;
- le rapport entre les services d'accès à Internet (public lane) et les services gérés (managed lane) : fournir un accès à capacité suffisante pour l'ensemble des utilisateurs finaux mais possibilité de mettre en place des services gérés plus performants pour l'industrie ou l'innovation sans compromettre l'accès Internet sur la public lane.

Ces mesures sont censées ouvrir la voie vers une plus grande neutralité du net qui ne doit pas être un principe restrictif au risque de compromettre l'accès à l'information des usagers finaux (notamment si la gestion des flux est trop rapidement libéralisée par rapport aux capacités matérielles du réseau).

http://economie.fgov.be/fr/modules/publications/analyses_etudes/etude_net_neutrality.jsp

Selon le responsable des Télécommunications à la direction générale des Télécommunications, concernant le support juridique, les pouvoirs publics belges ne sont pas favorables à des priorités fixées dans le règlement télécom du paquet Single Market. Ils préfèrent le recours à une recommandation. Ils ne sont pas favorables à la possibilité de conclure des accords préférentiels entre les fournisseurs d'accès et les fournisseurs de services. Ces accords pourraient porter préjudice à la neutralité du réseau et à la libre concurrence entre les différents fournisseurs de service.

Q5/- Quelles sont les relations entre les pouvoirs publics belges et l'association gérant le nommage sur Internet dans ce pays, équivalent de l'Association française pour le nommage Internet en coopération (AFNIC) ?

La DNS Belgium, équivalent belge de l'AFNIC, n'a pas de lien formel avec les pouvoirs publics belges puisque ses membres ne sont pas été nommés par ces derniers. Il faut cependant noter la présence d'un représentant du régulateur des télécoms (IBPT – Institut belge des services postaux et des télécommunications) au sein du conseil de gestion de la DNS Belgium ainsi qu'un représentant du SPF Economie au comité stratégique de l'extension .be. Ils ont donc un rôle consultatif, renforcé récemment par la nouvelle loi sur les télécommunications de 2012 (transposition de la directive) dont deux articles concernent l'extension .be : le premier stipule que la gestion du .be doit être faite par une association sans but lucratif, basée en Belgique et dont les opérations techniques se situent en Belgique ; le second permet une intervention de l'IBPT au cas où l'un des critères du premier article ne serait pas rempli et lui donne le droit de désigner un autre opérateur.

La DNS Belgium et l'ICANN ont confirmé leur coopération, la DNS Belgium faisant notamment partie du ccNSO (country codes Names Supporting Organisation) mais elle reste totalement indépendante de l'organisation internationale en ce qui concerne l'attribution de noms de domaines.

Finalement, ni les pouvoirs fédéraux, ni l'ICANN ne peuvent donner des instructions à la DNS Belgium concernant l'attribution des noms de domaines, les services à offrir et leur tarification. Elle doit cependant prouver que les augmentations de prix d'enregistrement sont bien liées à des coûts réels.

Service économique régional de Bruxelles

La Belgique est l'un des rares pays où l'État n'a de pouvoir de contrôle ni de décision (modèle quasi-similaire au Pays-Bas). La Belgique souhaite conserver ce modèle, adopté pour des raisons historiques et résultant d'une volonté politique, modèle qui, à ses yeux, fonctionne bien.

Q6/- Quelle est la position des autorités belges à l'égard de la proposition de règlement européen relatif à la protection des données personnelles en cours de négociation ? Quel avenir envisagent-elles pour l'accord « Safe Harbor » ?

La protection des données personnelles est de la compétence de la CPVP (Commission de protection de la vie privée), entité fédérale composée de seize membres et dirigée par un magistrat.

La CPVP, chargée d'émettre un avis sur ce règlement européen, fait part de ses doutes quant aux réelles avancées de ce dernier dans le renforcement des droits des personnes par rapport à l'acquis de la directive 95/46/CE qui fait toujours foi aujourd'hui. Une protection sûre passe par un renforcement du droit mais aussi par sa mise en œuvre effective et par les moyens mis à disposition pour les faire valoir (cf. Annexe – Avis du 5 février 2014 (10/2014) de la CPVP concernant ce règlement).

Concernant le renforcement du Safe Harbor (ou tout autre accord international de transmission de données entre entreprises), la CPVP rappelle qu'une « surveillance générale, massive et systématique des citoyens belges et européens n'est pas acceptable dans une société démocratique » et elle accueille donc favorablement les dispositions de la Commission LIBE (Libertés civiles, justice et affaires intérieures) du Parlement européen de tenter de trouver des réponses adéquates et pratiques pour la protection de la vie privée et des données à caractère personnel. Passé ce constat, elle estime que l'article 43a. proposé entraîne une certaine confusion dans les rôles respectifs des autorités de protection des données et de la Commission européenne et se demande si les autorités de protection des données sont véritablement armées pour évaluer la compatibilité avec le règlement de la demande de transmission de données vers un pays tiers. Elle considère donc que l'entité chargée d'évaluer les demandes devrait être désignée par l'accord international concerné (tel Safe Harbor).

Service économique régional de Bruxelles

ANNEXE

Avis n° 10/2014 du 5 février 2014

Annexe - Avis d'initiative portant sur la proposition de Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, tel que voté par la Commission LIBE du Parlement européen le 17 octobre 2013 (CO-A-2014-001)

La Commission de la protection de la vie privée (CPVP) ;
Vu la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (ci-après LVP), en particulier l'article 29 ;
Vu le rapport de Monsieur Willem Debeuckelaere, Président, et Monsieur Stefan Verschuere, Vice-président;
Émet, le 5 février 2014, l'avis suivant :

Résumé de l'avis que l'on retrouve à l'adresse suivante :
http://www.privacycommission.be/sites/privacycommission/files/documents/avis_10_2014.pdf

Le 21 novembre 2012, la CPVP rendait d'initiative un avis critique sur la proposition de Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après « le projet de Règlement ») déposé par la Commission européenne.
Dans la lignée des objections et commentaires exprimés aux termes de cet avis 35/2012, la CPVP formule ci-dessous son point de vue au regard du projet de texte voté par la Commission chef de file « Libertés civiles, justice et affaires intérieures » (LIBE) du Parlement européen le 17 octobre 2013.
La CPVP souhaite attirer l'attention tant des parlementaires européens que des responsables politiques (belges) compétents - aujourd'hui et au lendemain des élections à venir – sur les implications des orientations prises par la Commission chef de file. Une attention toute particulière est apportée à certains concepts qui ne figurent pas dans le projet déposé par la Commission européenne (les données pseudonymes), qui revêtent une autre dimension aux yeux des parlementaires de la Commission LIBE (certification, BCR sous-traitants) ou qui font très largement débat au(x) niveau(x) du Conseil européen (profilage, principe du guichet unique « *one-stop-shop* » et voies de recours, traitements à des fins de recherche historique, statistique et scientifique).

Une protection renforcée des droits des personnes concernées ? Un des objectifs déclarés de la réforme de la protection des données est le renforcement des droits des personnes concernées, plus particulièrement à l'ère du numérique omniprésent et face aux géants (européens et non européens) de l'Internet. Dans son avis 35/2012, la CPVP a d'emblée émis des doutes sur le renforcement réel qui serait apporté par le projet de Règlement, en particulier par rapport à l'acquis de la directive 95/46/CE.
Une protection réelle passe bien sûr par le contenu du droit mais aussi par sa mise en œuvre effective (notamment praticable pour les responsables de traitement) et, in fine, par les moyens accessibles mis à la disposition de la personne concernée pour les faire valoir tant auprès du responsable de traitement qu'auprès de l'autorité de contrôle et des instances judiciaires. A l'appui de ce postulat, la CPVP formule les commentaires ci-après.

I. Un champ d'application adéquat

1. Les traitements de données réalisés dans le cadre de l'utilisation des réseaux sociaux ne peuvent totalement échapper à l'application du projet de Règlement. Son champ d'application matériel doit les inclure et la portée de l'exception pour les activités purement personnelles et domestiques définie de manière à les couvrir (points 6 et s.)

2. La CPVP s'oppose à l'insertion de la notion de « données pseudonymes », qu'elles soient le résultat d'un codage ou un moyen d'identification dans l'environnement numérique. L'insertion d'une sous-catégorie de données personnelles dans le projet de Règlement complique davantage l'interprétation des notions actuelles de « données à caractère personnel » et « données anonymes », sur lesquelles repose le régime en vigueur. En prévoyant par ailleurs un régime de protection indistinctement « allégé » pour cette catégorie de données à caractère personnel, la réforme envisagée aboutirait à un inacceptable affaiblissement du niveau de protection garanti (points 9 et s.).

II. Des définitions adéquates

1. La CPVP plaide pour une définition des données relatives à la santé qui tienne compte du contexte dans lequel intervient le traitement de telles données (points 15 et s.). S'agissant de leur traitement à des fins thérapeutiques, elle s'oppose à l'obligation imposée aux États membres d'adopter une législation spécifique permettant le traitement (points 129 et s.).

III. Un régime dérogatoire adéquat

1. La Commission LIBE réduit les possibilités d'exemptions à l'application du Règlement, que ce soit par la voie des articles auxquels il peut être dérogé ou par le biais des motifs pour lesquels l'État membre peut instaurer un régime dérogatoire. A cet égard, la CPVP alerte le lecteur sur la suppression du motif « intérêt général de l'Union ou d'un État membre » et sur son remplacement par les seules « *taxation matters* » (points 56 et s.).

IV. Des droits effectifs, renforcés (ou au minimum préservés par rapport à l'acquis de la directive 95/46/CE) pour les personnes concernées

1. La CPVP accueille favorablement les modifications apportées par la Commission LIBE quant au contenu de l'information des personnes concernées, tout particulièrement en ce qui concerne le délai de conservation des données, les mesures de sécurité mises en place, la logique qui préside aux traitements, les éléments relatifs au profilage et les garanties entourant les flux transfrontières. Elle n'est par contre pas convaincue de la valeur ajoutée des pictogrammes proposés. Elle s'oppose enfin à la suppression de l'exercice de certains droits des personnes concernées dans les cas où le responsable de traitement serait soumis au secret professionnel (points 18 et s.).

2. La CPVP regrette que la suppression des termes « droit à l'oubli » à l'intitulé de l'article 17 ne s'accompagne pas de davantage de clarification quant à la portée exacte du droit à l'effacement que cet article consacre. En particulier, la CPVP est d'avis que l'obligation pour les responsables de traitement de contacter tous les tiers qui auraient légalement rediffusé les données initialement traitées sera difficilement praticable (points 24 et s.)

3. La CPVP relève que la Commission LIBE n'apporte pas de correctif complet à l'affaiblissement du droit d'opposition. En effet, le droit d'opposition prévu par la Loi Vie privée (LVP) disparaît dans les cas où le consentement de la personne concernée constitue la base légale du traitement de données. La balance des intérêts à opérer par le responsable de traitement lui-même - laquelle peut l'amener à refuser à la personne concernée l'exercice d'un droit – crée le risque inacceptable de voir les responsables de traitement continuellement invoquer leur intérêt légitime pour s'opposer à l'exercice du droit d'opposition (points 31 et s.).

4. Quant à l'encadrement proposé du profilage, la CPVP plaide pour un régime de protection qui encadre à la fois les traitements basés sur un profil constitué et les décisions individuelles automatisées actuellement visées par l'article 15 de la directive 95/46/CE. Quant au profilage à proprement parler, la création d'un profil d'une part et l'application de profils d'autre part devraient tous deux être règlementés, dans l'esprit de la Recommandation du Conseil de l'Europe relative au profilage, en ce compris dans le « droit à l'anonymat » qu'elle introduit (points 33 et s.).

5. La CPVP regrette la réduction de l'obligation de documentation à un strict minimum. L'obligation ainsi conçue n'amène plus le responsable de traitement à se poser les questions pertinentes au regard des traitements envisagés comme c'est le cas avec l'obligation actuelle de déclaration à laquelle elle entend se substituer. La CPVP est d'avis que la documentation devrait, au minimum, inclure, outre les données de contact des responsables de traitement, sous-traitants, représentant et délégué à la protection des données éventuels et destinataires des données, une description de la finalité des traitements et les catégories de données traitées (points 60 et s.).

6. La CPVP demande que le système des comités sectoriels et leur compétence d'autorisation de certains traitements spécifiques de données puisse être maintenu aux termes de la nouvelle règlementation européenne. Elle est en effet convaincue que le travail d'analyse de ces comités est essentiel et que les conditions posées dans leurs autorisations encadrent de manière adéquate les flux de données du secteur public (principalement). Elle plaide avec insistance pour le maintien de ce mécanisme bénéfique à la protection de la vie privée et des données à caractère personnel des citoyens (points 68 et s.).

7. En d'autres termes, la CPVP regrette qu'il n'ait pas été tenu compte de la pratique et de l'expérience positive de certaines autorités de protection des données dans l'application de leur règlementation nationale. Outre le mécanisme des autorisations délivrées par les comités sectoriels évoqué ci-dessus, la CPVP déplore la disparition de la disposition de la directive 95/46/CE actuellement en vigueur qui permet d'encadrer l'accès et l'utilisation du numéro de registre national. Elle plaide pour le possible maintien de cette règlementation (points 127 et s.).

8. Forte de son expérience en la matière, la CPVP propose également un certain nombre d'amendements à l'encadrement de la recherche historique, statistique et scientifique qui tendent à trouver le juste équilibre entre les intérêts des chercheurs d'une part et le nécessaire respect de la protection de la vie privée et des données à caractère personnel dans ce secteur d'autre part (points 131 et s.).

9. Quant aux instances et voies de recours accessibles à la personne concernée, la CPVP ne peut soutenir la traduction du principe du guichet unique en l'état. Ce principe s'accompagne d'une multiplicité de recours administratifs et judiciaires possibles pour la personne concernée, tant dans l'État membre dans lequel il réside habituellement qu'à l'étranger. Selon la CPVP, la complexité du système des voies de recours offertes par le projet de Règlement - notamment dans sa version votée par la Commission LIBE - n'offre pas de garanties suffisantes pour lui permettre de considérer que les articles 16 TFUE, 8 et 47 de la Charte des droits fondamentaux de l'Union et 6 (accès au tribunal) et 13 (recours effectifs) de la Convention européenne des droits de l'homme sont pleinement mis en œuvre (points 115 et s.).

10. La CPVP accueille favorablement la tentative de la Commission LIBE d'apporter une solution aux transferts de données vers des pays tiers non adéquats, du type notamment de ceux révélés par l'affaire SWIFT (et ses transferts de données vers l'UST (*US Treasury* des États-Unis)) ou encore plus récemment par les révélations d'E. Snowden relatives aux vastes programmes de surveillance des services secrets américains (NSA – National Security Agency). La CPVP s'oppose par contre au rôle qu'on voudrait y voir jouer les autorités de protection des données, notamment d'autoriser de tels transferts et émet de sérieux doutes sur l'opportunité et la praticabilité – tant d'un point de vue pratique que légal – de l'information individualisée à la personne concernée par de tels transferts (points 95 et s.)

V. Des obligations praticables pour les entreprises et bénéfiques à la protection des données des personnes concernées – *risk based approach*

1. Comme dans son avis 35/2012, la CPVP plaide pour un système d'obligations cohérentes et basées sur l'appréciation concrète du risque réel induit par les traitements réalisés.

2. La CPVP est d'avis que les violations de données (*data breach*) à notifier – que ce soit à l'autorité de protection des données ou à la personne concernée – ne sont pas (suffisamment) définies. Ce déficit de précision risque de rendre, dès leur conception, ineffectives cette obligation et l'information corrélative utile qu'elle se veut apporter à l'autorité de contrôle et à chacun (points 62 et s.).

3. La CPVP soutient le déploiement de la fonction de délégué à la protection des données pour autant que la désignation d'un tel délégué reste une faculté pour le responsable de traitement. Telle fonction doit être conçue comme une mesure *d'accountability* dont le responsable de traitement doit rester libre de faire le choix compte tenu des traitements opérés, des risques réels, de l'existence d'autres mécanismes de protection et du bénéfice réel pour la protection des données qu'elle apporterait. Partant, la CPVP ne peut souscrire à l'orientation de la Commission LIBE qui étend plus encore les cas dans lesquelles cette désignation d'un délégué est obligatoire, a fortiori dans des hypothèses fondées sur des critères de risque qui ne lui apparaissent pas pertinents (points 76 et s.).

4. Dans la même optique de soutenir les incitants à la diffusion et la mise en place d'une véritable culture de la protection des données en entreprise, la CPVP regrette que la Commission LIBE omette les BCR sous-traitants (*Binding Corporate Rules for processors*). Ces règles apportent un haut niveau de protection des données dans les cas de transferts de données traitées à l'origine par un groupe multinational en tant que sous-traitant. S'opposer à celles-ci ne fait que créer de l'insécurité juridique et pousser les entreprises à opter pour des outils moins protecteurs qui n'offrent pas cet avantage qu'ont les BCR de promouvoir nos règles européennes à l'étranger (points 86 et s.).

5. La CPVP insiste pour que les critères et exigences applicables aux mécanismes de certification, y compris les conditions d'octroi, de révocation et les conditions de reconnaissance au sein de l'Union et dans les pays tiers ainsi que les critères d'accréditation des certificateurs soient déterminés par les autorités de protection des données. A ces conditions seules, elle pourrait admettre que la certification intègre la liste des garanties adéquates de protection autorisant un flux de données vers un pays tiers non-adéquat au même titre que les clauses contractuelles types ou les BCR. Elle est par contre opposée à un régime de sanction allégé pour les entreprises certifiées qui se rendraient coupables d'un manquement au projet de Règlement (points 75-81 et 85).

VI. Une autorité de protection des données accessible

6. Quant à son propre rôle, la CPVP est d'avis qu'il est très certainement amené à évoluer, quel que soit le sort réservé à la proposition de Règlement déposé par la Commission européenne. Plusieurs commentaires ci-dessus soulignent certaines préoccupations de la CPVP quant au rôle qu'on voudrait lui voir jouer, quant aux compétences qu'on voudrait lui confier (certification, autorisation de certains transferts de données en – dehors de l'Union européenne (article 43a)), suppression de la compétence d'autorisation de flux de données dans le secteur public). Son indépendance est à préserver de même que sa vocation à sensibiliser comme à guider et assister le grand public et les entreprises.

7. Quant aux sanctions, la CPVP est particulièrement soucieuse de préserver l'objectif premier de son travail, soit la mise en conformité de traitements réalisés avec les exigences de la règlementation en matière de protection des données. A l'appui de son expérience, elle privilégie la médiation à la sanction, tout particulièrement pour des raisons liées au nécessaire respect du principe de la séparation des pouvoirs. Les montants, fussent-il maximaux, excessivement élevés des amendes administratives prévues par la Commission LIBE la confortent dans cette prise de position (points 123 et s.).

8. Enfin, la CPVP est convaincue qu'une coopération régulière et structurée entre autorités de protection (européennes) des données est indispensable. Elle privilégie toutefois la création d'une autorité européenne de protection des données (bénéficiant de la personnalité juridique, établie au niveau de l'Union européenne et dont les décisions s'imposeraient à l'ensemble des États de l'Union) dans les cas de traitements « transfrontières » (soit des traitements communs à plusieurs États membres de l'Union). A cet égard, elle est favorable au renforcement du rôle du Comité européen de la protection des données (CEPD – points 109 et s.), en ce compris dans la préparation des actes délégués (points 141 et s.). Subsidiairement, le concept d'autorité chef de file associé à une procédure de codécision lui semble davantage défendable que celui d'un guichet unique dont le rôle serait confié à la seule autorité du lieu de l'établissement principal du responsable de traitement et dont les décisions s'imposeraient à toutes les autorités de protection des données concernées. L'autorité de protection des données doit rester un interlocuteur de proximité, tout particulièrement pour les citoyens qui voudraient déposer plainte (points 104 et s.).

Service économique régional de Madrid

ESPAGNE

Q1/ Quelles sont les préoccupations majeures que soulève l'Internet dans le pays où vous représentez la France ?

L'expansion exponentielle d'Internet a eu pour conséquence de nombreux bénéfices sociaux et a contribué au progrès économique, mais elle a également donné lieu à l'apparition de risques qui inquiètent autant la population que le gouvernement.

Parmi ces inquiétudes se trouvent la cyber-sécurité, qui inclut la fraude online, et la protection des droits fondamentaux tels que la liberté d'expression, l'intimité, la protection des données personnelles ainsi que la protection des mineurs et la propriété intellectuelle. D'autre part, des questions telles que la contribution fiscale d'entreprises internationales d'Internet suscitent de grands débats. On observe également, parfois avec impuissance, les difficultés pour appliquer la législation espagnole à des entités dont le siège est dans un autre État mais qui prêtent pourtant leurs services à des citoyens résidant en Espagne.

Par ailleurs, conformément à l'Agenda Numérique pour l'Espagne, les défis du développement de la Société de l'Information ont principalement pour objectifs, l'économie numérique, l'innovation numérique, les services publics numériques, la confiance numérique, l'internationalisation, le développement des TIC au sein des PME et l'inclusion numérique.

Q2/- La place de l'Union européenne dans la gouvernance mondiale de l'internet est-elle un sujet de préoccupation importante dans le pays où vous représentez la France, soit au niveau politique (exécutif/législatif), soit dans l'opinion publique ? Avez-vous connaissance d'initiatives politiques en ce domaine ?

Les évènements récents autour de questions relevant de la gouvernance d'Internet, tels l'extension des domaines de premier niveau ou la supervision de la gestion des ressources critiques d'Internet, ont accru l'intérêt pour ces sujets, tant au niveau politique que de l'opinion publique.

La preuve en est le nombre croissant d'articles publiés dans la presse généraliste sur ce sujet.

Du point de vue politique, le Gouvernement espagnol s'implique davantage dans les questions importantes relatives à la gouvernance d'internet et a renforcé sa participation dans les forums internationaux sur ce sujet, avec pour objectif de défendre ses intérêts, convergents avec ceux de l'Union Européenne, et les principes directeurs qui doivent guider la gestion de cette ressource clé, que sont la transparence, l'ouverture et la responsabilité.

De même, les organes législatifs sont conscients de l'importance de cette question. Ainsi, à l'occasion de la journée d'Internet, le 16 mai dernier, le Sénat a organisé une Journée sur la Gouvernance de l'internet.

Q3/- Comment le pays où vous représentez la France considère-t-il le fonctionnement actuel de la gouvernance d'internet? Quelle est sa position à l'égard de la communication de la Commission européenne sur la gouvernance de l'internet publiée en février 2014 ?

La position de l'Espagne sur ces questions est détaillée dans la contribution publique présentée pour la conférence de Net Mundial (cf. lien).

De manière générale, l'Espagne estime que les structures actuelles de gouvernance d'internet, bien qu'innovantes en ce qui concerne le Droit international public, sont avantageuses en ce qu'elles permettent un système de gouvernement plus participatif ou collectif, qui assure ainsi un meilleur

engagement dans l'exécution des normes qui sont décidées, celles-ci étant mieux adaptées au rythme vertigineux de l'innovation dans Internet.

Cependant, la nature transnationale d'Internet, la croissance exponentielle de son usage dans le monde entier, parfois de manière délictueuse ou frauduleuse à l'encontre des consommateurs, et la place prise par cet outil dans le travail quotidien des citoyens, des entreprises et des gouvernements créent des défis pour la sécurité publique et les droits et intérêts légitimes des usagers qui requièrent le renforcement des forums mondiaux de débat au sein desquels peuvent émerger des recommandations concrètes ainsi qu'une augmentation de la coopération internationale.

L'Espagne considère que le GAC (Governmental Advisory Committee) ou Comité assesseur de l'ICANN doit entreprendre une réforme de ses méthodes de travail, de procédures et de prise de décision afin d'augmenter le nombre de représentants, d'augmenter son activité, de s'impliquer plus tôt dans l'élaboration des normes et de renforcer la portée de ses recommandations dans les décisions du Conseil de direction de l'ICANN.

L'Espagne appuie, dans l'ensemble, la position de la Commission de février 2014, mais elle estime qu'il conviendrait d'approfondir certains aspects en débat actuellement et qui le seront encore dans les mois à venir, tels que l'internationalisation des organes de gouvernance d'internet et le rôle des gouvernements. Au vu des propositions formulées par la Commission à Net Mundial, l'Espagne espère qu'elle continuera à développer des propositions concrètes sur ces sujets dans les prochains écrits et réunions, afin d'aider l'Europe à jouer un rôle important dans les négociations sur la gouvernance d'Internet.

Q4/- Quelle est la position des autorités du pays où vous représentez la France à l'égard du principe de la neutralité du net, et notamment à l'égard de la définition qu'en propose la Commission européenne dans la proposition de règlement « L'Europe, continent connecté » COM(2013) 627 final ?

La neutralité du net est un sujet très important en discussion actuellement au sein de la Commission européenne, avec une participation active de l'Espagne. Il affecte non seulement les opérateurs de télécommunications mais également une grande variété d'agents de l'écosystème de la Société de l'information. L'Espagne considère qu'il convient d'attendre les décisions qui seront arrêtées au niveau communautaire.

Dans la proposition de la Commission - actuellement débattue - de Règlement « L'Europe, un continent connecté », il est proposé d'établir des obligations permettant la fourniture de services d'accès à Internet de qualité garantie (ex. augmentation de la transparence envers les usagers) et limitant l'utilisation de techniques de gestion du trafic à des cas justifiés (tout en garantissant un traitement identique aux types de trafics équivalents).

L'Administration espagnole accueille positivement cette optique mais estime que les obligations de transparence ne doivent pas présenter un coût disproportionné pour les opérateurs. Les questions de neutralité du net doivent être abordées non seulement dans le cadre des réseaux de télécommunication mais également à d'autres étapes de la chaine de valeur des services numériques qui ont une incidence qui peut être plus importante sur le droit effectif d'accès ouvert à tous les usagers (terminaux, systèmes opératifs, plateformes). Il est impossible de garantir la neutralité d'Internet en se fondant sur les seuls fournisseurs d'accès à Internet.

Face à la croissance de la consommation de données et afin d'éviter la future saturation des réseaux, est en cours actuellement un processus d'actualisation et de modernisation des réseaux, principalement en termes d'accès, représentant des investissements importants au niveau des opérateurs de télécommunication.

Service économique régional de Madrid

Q5/- Quelles sont les relations entre les pouvoirs publics du pays où vous représentez la France et l'association gérant le nommage sur Internet dans ce pays, équivalent de l'Association française pour le nommage Internet en coopération (AFNIC) ? Comment cette association se coordonne-t-elle avec l'ICANN et quel est son degré d'autonomie par rapport à ce dernier ? Est-il jugé suffisant pour permettre une stratégie nationale de fixation des noms de domaine ?

Red.es est l'entreprise publique qui gère le nommage sur internet sous le code de l'Espagne « .es » (ccTLD (country code Top Level Domain)). L'entreprise dépend du Ministère de l'Industrie, de l'énergie et du tourisme et, plus directement, du Secrétariat d'État aux télécommunications et pour la Société de l'Information (SETSI).

Bien qu'elle soit une participante active aux réunions de la ccNSO (country code Name Supporting Organisation), l'entité Red.es n'en est pas membre et n'a aucun accord, formel ou informel avec l'ICANN. Elle ne participe pas non plus à son financement.

Par conséquent, l'Espagne est parfaitement indépendante pour approuver la stratégie nationale de nommage de domaine. Cependant, la Loi établit que celle-ci doit tenir compte, dans la mesure du possible, des pratiques généralement appliquées et des recommandations émanant des entités et organismes internationaux en la matière (Loi 34/2002 du 11 juillet sur les services de la Société de l'Information et le commerce électronique, 6ème disposition additionnelle).

Q6/- Quelle est la position des autorités du pays où vous représentez la France à l'égard de la proposition de règlement européen relatif à la protection des données personnelles en cours de négociation ? Quel avenir envisagent-elles pour l'accord Safe Harbor qui constitue depuis 2001, dans le domaine civil et commercial, le cadre juridique, pour permettre l'échange de données entre entreprises de l'Union européenne et entreprises américaines respectant un certain niveau de protection des données et qui repose donc sur l'auto-certification des entreprises? Quelle est leur position à l'égard de la communication de la Commission européenne publiée le 29 novembre 2013 et appelant au renforcement du « Safe Harbor » ?

En ce qui concerne le règlement européen de protection des données, l'Espagne considère qu'il constitue un pas en avant pour une protection adéquate de la confidentialité dans l'univers numérique.

Cependant, de nombreuses questions méritent encore un débat approfondi, telle le modèle de gouvernance à implanter pour la protection des données. Une approche satisfaisante pourrait passer par l'intervention des superviseurs nationaux pour les questions internes comme les plaintes d'usagers au niveau national, sans passage de frontières ; un super-régulateur européen ou un système de décision par consensus entre les autorités nationales pourrait être créé en plus pour réaliser un travail de coordination européenne et régler les litiges dans lesquels plusieurs États membres seraient concernés.

Concernant le Safe harbor, l'Espagne considère qu'il conviendrait de renforcer le cadre actuel ainsi que l'indique la Communication de la Commission du 27 novembre 2013, sous le principe de plus de transparence, supervision et vigilance permanente aux prestataires de services se soumettant à l'accord.

De plus, elle trouve particulièrement adaptées les recommandations de la Communication pour que l'exception de sécurité nationale, prévue dans la décision « Safe harbor », ne soit utilisée que de façon strictement nécessaire et proportionnée.

Antenne à Tallinn du SER de Varsovie

ESTONIE

Q1/ Quelles sont les préoccupations majeures que soulève l'Internet dans le pays où vous représentez la France ?

L'Estonie qui a hébergé les 28 et 29 avril la quatrième conférence de la Coalition Freedom Online (après la Haye, Nairobi et Tunis), est particulièrement attachée à la liberté d'expression sur Internet et à la transparence, en considérant que la sécurité et la liberté ne sont pas deux notions contradictoires dans le contexte du net.

Lors de la conférence FOC, le Président estonien (dont le bureau est également impliqué dans l'élaboration des positions et des propositions estoniennes en matière de numérique) a souligné dans son allocution, qu'un équilibre entre la libre circulation de l'information, la sécurité et le respect de la vie privée des individus devait être trouvé, mais que rien ne pouvait justifier la mise en cause du principe fondamental de la liberté dans la société de l'information ou la censure à laquelle ont recours certains gouvernements. Le Président a, certes, mis en exergue les dangers liées à la société de l'information (rappelons, par ailleurs, les cyberattaques perpétrées contre l'Estonie en 2007), mais a fortement insisté sur les dérives possibles d'une régulation renforcée et d'un contrôle accru de l'Internet par les gouvernements.

De manière plus générale, l'Estonie souhaite conserver sa place de chef de file dans le domaine du numérique. Au-delà des préoccupations liées à la gouvernance de l'Internet, les autorités estoniennes s'attachent tout particulièrement à faire reconnaître la signature numérique transfrontalière, que ce soit Europe ou dans le monde entier.

Q2/- La place de l'Union européenne dans la gouvernance mondiale de l'internet est-elle un sujet de préoccupation importante dans le pays où vous représentez la France, soit au niveau politique (exécutif/législatif), soit dans l'opinion publique ? Avez-vous connaissance d'initiatives politiques en ce domaine ?

Il y a peu de débats en Estonie sur le rôle de l'Union européenne dans la gouvernance de l'Internet de manière spécifique. Les autorités estoniennes estiment que l'Internet devrait être régi globalement par un modèle multipartite où aucun État ou organisation ne doit avoir une place prédominante.

Q3/- Comment le pays où vous représentez la France considère-t-il le fonctionnement actuel de la gouvernance d'internet? Quelle est sa position à l'égard de la communication de la Commission européenne sur la gouvernance de l'internet publiée en février 2014 ?

L'Estonie n'a pas encore élaborée de position officielle détaillée à l'égard de la communication de la Commission européenne sur la gouvernance de l'internet (février 2014). Néanmoins, l'Estonie a approuvé dans les grandes lignes la proposition des positions à exprimer par les États Membres de l'UE et la Commission lors de la Rencontre mondiale sur le futur de la gouvernance de l'Internet à Sao Paulo (23-24 avril).

Q4/- Quelle est la position des autorités du pays où vous représentez la France à l'égard du principe de la neutralité du net, et notamment à l'égard de la définition qu'en propose la Commission européenne dans la proposition de règlement « L'Europe, continent connecté » COM(2013) 627 final ?

Dans ce contexte, les positions estoniennes sont les suivantes :

- L'Estonie soutient le principe de la neutralité du net tel qu'il a été défini par la Commission européenne : interdiction pour les opérateurs de bloquer l'accès des usagers aux contenus numériques légaux, à une page Internet ou à une plateforme spécifique.
- Les autorités estoniennes estiment, de plus, que les start-up doivent pouvoir avoir accès aux utilisateurs finaux à travers le réseau des communications électroniques, afin d'encourager la création de nouveaux services innovants.
- L'Estonie est d'accord sur le principe des exceptions lorsque cela est justifiée ; en particulier afin de lutter contre la cybercriminalité, protéger les usagers des messages non désirés (spam) et prévenir les effets d'une congestion temporaire du réseau.

Q5/- Quelles sont les relations entre les pouvoirs publics du pays où vous représentez la France et l'association gérant le nommage sur Internet dans ce pays, équivalent de l'Association française pour le nommage Internet en coopération (AFNIC) ? Comment cette association se coordonne-t-elle avec l'ICANN et quel est son degré d'autonomie par rapport à ce dernier ? Est-il jugé suffisant pour permettre une stratégie nationale de fixation des noms de domaine ?

L'association estonienne en charge du nommage de l'Internet « Interneti SA » (Fondation pour l'Internet) a été créée par le ministère estonien de l'économie et l'association estonienne des technologies de l'information (ITL). Il s'agit d'est chargée de la gestion des noms de domaines estoniens (.ee).

Son rôle se définit de manière suivante :

- la représentation de la communauté de l'Internet estonien auprès de la communauté internationale, y compris l'ICANN et d'autres organisations impliquées
- la gestion des domaines ayant un nom de domaine estonien et leur enregistrement, ce dans le souci de l'intérêt général.
- l'élaboration des règles et des tarifs d'enregistrement des noms de domaine.
- la tenue des registres des systèmes d'information des noms de domaine, garantie de l'accessibilité et de la fiabilité de ces registres.

Q6/- Quelle est la position des autorités du pays où vous représentez la France à l'égard de la proposition de règlement européen relatif à la protection des données personnelles en cours de négociation ? Quel avenir envisagent-elles pour l'accord Safe Harbor qui constitue depuis 2001, dans le domaine civil et commercial, le cadre juridique, pour permettre l'échange de données entre entreprises de l'Union européenne et entreprises américaines respectant un certain niveau de protection des données et qui repose donc sur l'auto-certification des entreprises? Quelle est leur position à l'égard de la communication de la Commission européenne publiée le 29 novembre 2013 et appelant au renforcement du « Safe Harbor » ?

L'Estonie est globalement favorable aux objectifs du règlement européen relatif à la protection des données : le pays soutient notamment la proposition qui vise à rendre la protection des données plus efficace et réduire la fragmentation, tout en veillant à simplifier l'environnement en matière de réglementation et de réduire la charge administrative. Les autorités estoniennes considèrent, en outre, que la régulation devrait être favorable au développement de l'entreprenariat (et se prononcent sceptiques quant à la définition de sanctions financières dont l'impact négatif sera très important pour

Antenne à Tallinn du SER de Varsovie

les SME). L'Estonie soutient la mise en place d'une régulation claire pour le transfert de données hors de l'Union européenne.

L'Estonie considère que la poursuite du programme « Safe Harbor » ainsi que d'autres programmes internationaux similaires est nécessaire. Les autorités estoniennes sont en faveur de toute mesure contribuant à rendre le transfert des données entre l'UE et les États-Unis plus efficace et plus sûr. L'Estonie soutient également la signature d'accords bi- et multilatéraux entre l'UE et les États tiers en matière de protection des données personnelles.

Service économique régionale de Rome

ITALIE

Q1/ Quelles sont les préoccupations majeures que soulève l'Internet dans le pays où vous représentez la France ?

- La neutralité d'Internet

Une analyse des articles de presse met en lumière une inquiétude concernant le danger de la discrimination commerciale qui déboucherait sur un réseau Internet à deux vitesses entre colosses d'Internet d'un côté et usagers normaux de l'autre (La Repubblica du 5/05/14 : « L'Internet des riches »). La presse rend compte de la bataille entre les entreprises qui gèrent les infrastructures internet et ceux qui alimentent en contenus le réseau, attirant notamment l'attention sur le fait qu'un affrontement similaire est en train de se produire en Europe, les télécoms imitant les États-Unis (cf. par exemple la question de faire payer davantage Google pour l'utilisation interne des infrastructures).

- Le droit des usagers d'Internet

De nombreuses voix en Italie plaident pour une Charte des droits de l'Internet, qui permettrait de réintroduire l'Italie dans le débat international sur la gouvernance démocratique du web. La volonté de donner un cadre constitutionnel aux droits d'Internet (accessibilité, droit à la vie privée, neutralité, transparence) apparait ainsi comme une sorte de cheval de bataille de l'Italie dans ce secteur. Le projet d'une Charte des droits de l'Internet a été porté par le professeur Stefano Rodotà (homme politique de gauche, juriste, académicien) depuis 2006. Le 29 novembre 2010, il a présenté à l'Internet Governance Forum une proposition pour porter en Commission des Affaires constitutionnelles l'adoption d'un article 21bis sur l'accès pour tous à Internet. Des parlementaires ont repris ce projet et n'ont jamais cessé de militer pour faire de l'accès à Internet un droit constitutionnel.

- La gestion des adresses nationales et la « désaméricanisation » du web

La presse se fait l'écho de la volonté de certains pays (comme le Brésil et de l'Allemagne, la France n'étant presque jamais mentionnée) de relativiser l'hégémonie nord-américaine dans le secteur avec la substitution de l'ICANN par une gouvernance d'internet réellement internationale à partir de 2015.

- Sécurité d'Internet

Si la presse aborde le thème de la sécurité d'Internet en évoquant la multiplication des problèmes qui se succèdent avec une intensité croissante (sites piratés, vols de codes,…), la sécurité d'Internet ne semble pas être une priorité aussi pressante que la question des droits d'Internet en Italie. La presse s'est fait l'écho des préoccupations sur la sécurité de l'Internet après Snowden. Certains quotidiens (Repubblica) ont fait état d'intentions de l'agence de renseignement et de sécurité intérieure italienne (AISI), pour lutter contre l'espionnage, de mettre fin au réseau Internet unique en développant des infrastructures web nationales.

- La protection des droits de la propriété intellectuelle

Le gouvernement italien est préoccupé par les nouvelles assignations de termes génériques en noms de domaines de la part l'ICANN (Internet Corporation for Assigned Names and Numbers), tels .wine, .vin, .food, .pizza, .coffee. Dans ce cadre, l'Italie a présenté deux recours contre l'ICANN pour avoir assigné les noms de domaines .wine et .vin sans une protection adéquate des indications géographiques et des dénominations d'origine.

Service économique régionale de Rome

Q2/- La place de l'Union européenne dans la gouvernance mondiale de l'internet est-elle un sujet de préoccupation importante dans le pays où vous représentez la France, soit au niveau politique (exécutif/législatif), soit dans l'opinion publique ? Avez-vous connaissance d'initiatives politiques en ce domaine ?

Dans la majorité des articles consacrés à la gouvernance mondiale de l'Internet, la position ou, le cas échéant, l'action de l'Union Européenne est toujours mentionnée, notamment en ce qui concerne les thèmes de la neutralité du web et des droits de l'usager :

- Neutralité du web : les médias rapportent la position favorable à la neutralité d'internet prise par la Commission et le Parlement européen et le fait que le règlement (où le Parlement européen a défini pour la première fois le principe de neutralité d'internet) doit être examiné en juin par le Conseil, un accord n'étant selon eux pas acquis sur ce texte.
- Droits des usagers : les médias rapportent les initiatives en cours sur le sujet au Parlement européen et au Conseil de l'Europe. Ainsi, ils relèvent que le Parlement européen a approuvé une résolution invitant le Conseil à exhorter tous les acteurs d'Internet à s'engager dans le processus en cours de la Charte des droits fondamentaux liés à l'Internet. Le Sole commente la recommandation du Conseil de l'Europe sur un guide pour les droits des usagers de l'Internet en estimant qu'elle aura peu de retombées pratiques immédiates, même si ces recommandations restent un point positif car elles pourront être utilisées dans les différents pays d'Europe pour une action de lobbying en faveur de ces droits. La presse relève que les normes concernant Internet sont encore très fragmentées, raison pour laquelle l'Union Européenne souhaiterait créer un droit uniforme.

Pour le Ministère du Développement économique, compétent en matière de télécommunications, le rôle que peut jouer l'UE dans la gouvernance d'Internet ne suscite pas de préoccupations particulières. L'Italie retient néanmoins que les États Membres peuvent apporter des contributions significatives au niveau global, particulièrement par la définition de positions communes. L'Italie participe notamment aux différentes initiatives européennes, dont le HLIG (High Level Group on Internet Gouvernance).

Q3/- Comment le pays où vous représentez la France considère-t-il le fonctionnement actuel de la gouvernance d'internet? Quelle est sa position à l'égard de la communication de la Commission européenne sur la gouvernance de l'internet publiée en février 2014 ?

Le fonctionnement actuel de la gouvernance d'internet en Italie est considéré comme efficace du point de vue technique, mais peu participative. C'est pourquoi, le gouvernement italien et l'ensemble des parties prenantes considèrent, à l'instar de la position de la Commission européenne, que pour que le réseau internet, pour demeurer ouvert, libre, sûr, fiable et non fragmentée, il serait nécessaire de développer des politiques qui augmenteraient la transparence, la responsabilité et la participations de l'ensemble des parties prenantes à la gestion des ressources Internet et des processus de gouvernance.

Q4/- Quelle est la position des autorités du pays où vous représentez la France à l'égard du principe de la neutralité du net, et notamment à l'égard de la définition qu'en propose la Commission européenne dans la proposition de règlement « L'Europe, continent connecté » COM(2013) 627 final ?

Le gouvernement italien porte une attention particulière au principe de neutralité du réseau, au regard des conséquences sur le développement des activités et des technologies. L'Italie suit également le débat international sur ce thème, consciente de l'importance d'éviter un développement d'internet à deux vitesses, en maintenant, dans le même temps, les droits de tous les acteurs.

Selon la Confindustria, syndicat patronal italien, le gouvernement n'a pas exprimé officiellement et clairement sa position sur la neutralité du réseau. La Confindustria, quant à elle, regarde positivement la communication de la Commission, mais émet une opinion négative sur l'avis exprimé par le Parlement européen le 3 avril dernier, pour un « marché unique européen des communications

électroniques », estimant que le document voté par le Parlement européen augmenterait les charges pour les entreprises opérant dans le secteur des Télécoms.

Q5/- Quelles sont les relations entre les pouvoirs publics du pays où vous représentez la France et l'association gérant le nommage sur Internet dans ce pays, équivalent de l'Association française pour le nommage Internet en coopération (AFNIC) ? Comment cette association se coordonne-t-elle avec l'ICANN et quel est son degré d'autonomie par rapport à ce dernier ? Est-il jugé suffisant pour permettre une stratégie nationale de fixation des noms de domaine ?

Le ccTLD (country code Top Level Domains) en Italie a été confié à l'Institut d'Informatique et Télématique (IIT).

L'IIT est notamment chargée :

- du registre des noms de domaines en .it, cette activité absorbe l'essentiel du budget de l'institut ;
- de la gestion du réseau télématique.

En outre, l'ITT est membre de divers organismes internationaux, dont l'ICANN, le CENTR (Council of European National Top Level Domain Registries) et le RIPE (Réseaux IP Européens).

Un rôle important est également confié à l'autorité italienne des noms de domaines, appelée « Registro.it », afin d'organiser l'utilisation des noms de domaines en .it. L'organisme est responsable de la gestion des domaines Internet, et participe avec l'IIT et le ministère du Développement économique à l'activité d'enregistrement des noms de domaines.

Q6/- Quelle est la position des autorités du pays où vous représentez la France à l'égard de la proposition de règlement européen relatif à la protection des données personnelles en cours de négociation ? Quel avenir envisagent-elles pour l'accord Safe Harbor qui constitue depuis 2001, dans le domaine civil et commercial, le cadre juridique, pour permettre l'échange de données entre entreprises de l'Union européenne et entreprises américaines respectant un certain niveau de protection des données et qui repose donc sur l'auto-certification des entreprises? Quelle est leur position à l'égard de la communication de la Commission européenne publiée le 29 novembre 2013 et appelant au renforcement du « Safe Harbor » ?

L'Italie semble adhérer aux principes fixés par la Commission européenne, qui a rappelé l'importance d'établir un haut niveau de protection garantissant le droit à la vie privée.

S'agissant plus précisément la communication de la Commission relative à la protection des données personnelles, le « garant italien de la vie privée » (autorité administrative indépendante) y est favorable.

S'agissant de l'accord Safe Harbor, la Confindustria considère qu'il nécessite une révision du fait qu'il a établi une certaine distorsion de la concurrence. Le syndicat patronal propose de permettre l'international data flow, en parallèle d'une homogénéisation des règles entre les diverses zones géographiques.

Service économique de La Haye

PAYS-BAS

Éléments locaux de contexte :

Le secteur des nouvelles technologies de l'information et de la communication (NTIC) figure parmi les secteurs de pointes à partir desquels les Pays-Bas souhaitent préparer leur économie à faire face aux défis de la mondialisation.

Ce choix repose notamment sur la qualité des innovations néerlandaises dans ce secteur (protocole sans fil Bluetooth, norme Wifi ...), sur son poids économique et sur la présence d'un tissu industriel au sein duquel figurent des leaders mondiaux (Philips, Tom-Tom…).

60 % de la croissance néerlandaise sur la période 1985 - 2005 est liée directement ou indirectement au déploiement des innovations issues des NTIC. Aussi, les nouvelles technologies de l'information et de la communication représentent-elles un marché mature et très compétitif de 30 Mds €, dont la moitié sur les télécommunications et l'internet, sur lequel près de 54 000 entreprises sont présentes.

Les Pays-Bas enregistrent de bons résultats selon la plupart des indicateurs internationaux ; ils occupent notamment la 4ème place du Networtked Readiness Index (NRI) qui évalue la disponibilité des pays à exploiter les TIC en termes de croissance et de prospérité.

La société néerlandaise est bien formée et leader dans l'utilisation de services numériques. Les achats par internet se développent grâce notamment à la plateforme sécurisée de paiement en ligne Ideal (plateforme ATOS), l'administration utilise un guichet unique numérique à travers un identifiant personnel unique (Digid), les services d'online banking sont très développés et peu coûteux…

C'est également une population très connectée avec 1,21 téléphone mobile par habitant et un taux de connexion à internet de 100 % dont près de 44 % sur le très haut débit soit le taux le plus élevé d'Europe. Même les personnes âgées dans la catégorie 65-75 ans sont connectées à hauteur de 80% de cette catégorie de population.…

Répartition du nombre d'abonnés par type de connections :

	Nombre d'abonnés	Taux
DSL	3 264 000	49 %
Fibre optique	397 000	5,9 %
Câble	2 991 000	44,9 %
TOTAL	6 653 000	

Service économique de La Haye

Q1/ Quelles sont les préoccupations majeures que soulève l'Internet dans le pays où vous représentez la France ?

Les Pays-Bas font partie des pays les mieux « connectés » d'Europe, en particulier en matière de pénétration du haut débit.

Dans la période la plus récente, les préoccupations afférentes ont touché principalement :

-à la protection des données privées

-à la neutralité du net.

-à la capacité de recherche des cybercriminels et pédophiles.

-plus marginalement, la question de l'impact environnemental d'internet

Ces problématiques sont portées au niveau de la société civile par l'association néerlandaise de protection de la vie privée et des droits des internautes, « Bits of freedom ».

Sur le 1er point, les thèmes de débat sont assez classiques et incluent notamment la question du droit à l'oubli (google).

Sur le 2ème point, les Pays Bas ont été, en 2012, le 1er pays d'Europe et le 2ème pays au monde (après le Chili) à voter une loi garantissant la neutralité du net. Le processus législatif avait débuté dès juin 2011, s'achevant le 8 mai 2012 par le vote de la 1ère chambre (équivalent du Sénat français).

Cette loi fait suite à un débat déclenché par plusieurs opérateurs du pays, KPN, Vodafone et T-Mobile, qui avaient annoncé leur intention de limiter (voire d'empêcher) l'accès à certains services en ligne jugés trop consommateurs de bande passante, notamment Skype.

KPN avait également visé l'Américain WhatsApp, qui permet d'envoyer des SMS gratuitement, ce qui avait selon l'opérateur entraîné un recul de 13% de ces revenus sur ces messages courts au premier trimestre de 2011.

En vertu de cette loi, les opérateurs sont donc obligés de garantir un accès général et égal à l'ensemble du réseau à tous leurs abonnés mobiles. La loi ne les empêche pas d'établir plusieurs tarifs liés à différentes vitesses d'accès, par exemple, mais cet accès une fois acquis doit permettre un accès égal à l'ensemble des services en ligne. Afin de garantir la neutralité du net, la loi néerlandaise donne également un nouveau cadre plus restrictif au deep packet inspection, une pratique de surveillance des communications en ligne, et au filtrage et blocage de sites. Ces pratiques restent possibles mais doivent être ponctuelles et autorisées par la justice.

Le 3ème point concerne la traque des cybercriminels et pédophiles. Ce volet aborde à la fois le dispositif de contrôle et d'enquête, ainsi que l'ensemble des démarches pédagogiques en direction des familles et de leurs enfants, afin que la première des protections de l'enfance soit un usage contrôlé et compris de l'internet au sein de la cellule familiale. Le réseau Tor, permettant notamment l'anonymisation des utilisateurs a ainsi été mis en cause il y a quelques années, accusé de compliquer la tâche des enquêteurs dans leur recherche de cybercriminels ou pédophiles.

Sur le 4ème point, la prise en compte de l'impact environnemental de l'internet est plus marginale en comparaison des précédentes mais a été très tôt (dés 2008) évoquée, par application du principe de la compensation carbone. C'est ainsi que fut plantée la première « forêt internet », sous la forme de bouleaux (essence à croissance rapide), à Apeldoorn, en vue de compenser les émissions des dioxine de carbone induites par les serveurs.

Service économique de La Haye

Q2/- La place de l'Union européenne dans la gouvernance mondiale de l'internet est-elle un sujet de préoccupation importante dans le pays où vous représentez la France, soit au niveau politique (exécutif/législatif), soit dans l'opinion publique ? Avez-vous connaissance d'initiatives politiques en ce domaine ?

Tout comme la France et la plupart des pays européens, les Pays Bas n'avaient pas ratifié en 2012 la nouvelle version du règlement des télécommunications internationales lors d'une conférence internationale à Dubaï. Il s'est agi dans la période récente de la seule intrusion de la dimension internationale dans la problématique de l'Internet aux Pays-Bas.

Hormis cela, aucun débat n'apparaît aux Pays-Bas relatif à la question posée, liée à la place de l'Union européenne.

Q3/- Comment le pays où vous représentez la France considère-t-il le fonctionnement actuel de la gouvernance d'internet? Quelle est sa position à l'égard de la communication de la Commission européenne sur la gouvernance de l'internet publiée en février 2014 ?

Les Pays-Bas souscrivent pleinement à la communication de la commission européenne sur la gouvernance de l'internet et plaident pour l'inclusion des principes suivants :

- Internet doit rester un média ouvert, disponible, accessible, fiable, stable, sûr, libre et non censuré.
- La neutralité du Net doit être garantie.
- Les droits qui s'appliquent offline, doivent également l'être online.
- L'autorégulation d'Internet doit être maintenue.

Les Pays-Bas sont attachés au modèle de gouvernance multipartite et souligne l'importance pour l'Europe de parler d'une seule voix sur ce dossier tout en rappelant que la répartition actuelle des compétences entre les États membres et l'action extérieure de l'UE doit être respectée.

Comme la Commission, ils ne sont pas en faveur de la création de nouvelles organisations dédiées à la gouvernance d'internet. Les Pays-Bas plaident pour la poursuite de l'élargissement du nombre d'adhérents à l'ICANN et ils sont en faveur du renforcement du rôle des gouvernements dans la gouvernance de l'organisation afin que ses décisions servent l'intérêt public.

Les Pays-Bas ont longtemps plaidé pour la mondialisation de l'administration de l'Internet, sans créer de nouvelles organisations de l'Internet ou de traités, ou de compromettre la liberté d'Internet et de l'ouverture.

Par conséquent, les Pays-Bas se félicitent de la récente annonce du gouvernement américain de transférer le contrôle sur l'Internet Domain Name System pour la communauté Internet. Cette transition ne doit pas mettre en danger la continuité et la stabilité de l'Internet en aucune façon.

Les Pays-Bas sont prêts à coopérer avec les autres parties prenantes à élaborer des propositions concrètes pour la mondialisation de la surveillance sur Internet Domain Name System ainsi que d'autres propositions au cours de la conférence NETmundial.

Les Pays-Bas souscrivent également aux propositions de la commission en ce qui concerne la réforme et le renforcement du Forum sur la gouvernance de l'internet. Ils insistent sur la nécessité d'obtenir des résultats tangibles ainsi qu'un financement durable de l'IGF.

Les Pays-Bas sont également en faveur de la modernisation de l'Union internationale des télécommunications. Ils souhaitent une plus grande participation des organisations non gouvernementales dans les prises de décision et la simplification des processus et des procédures de cette organisation.

Par ailleurs, les Pays-Bas jugent qu'il n'est pas nécessaire de créer une nouvelle plate-forme de discussion multipartite au niveau européen pour coordonner la gouvernance de l'Internet à l'échelle

européenne. Ils préconisent plutôt l'implication des forums nationaux et régionaux liés à la gouvernance de l'Internet[5], tel que le Dialogue européen sur la gouvernance de l'Internet (EuroDIG).

De plus, les Pays-Bas souscrivent aux propositions faites par la commission en vue de soutenir le développement du numérique dans les pays en voie de développement.

Ils estiment, par ailleurs, que plus d'attention doit être portée aux problèmes sous-jacents au sein de ces pays tels que la cybercriminalité et le spaming.

Q4/- Quelle est la position des autorités du pays où vous représentez la France à l'égard du principe de la neutralité du net, et notamment à l'égard de la définition qu'en propose la Commission européenne dans la proposition de règlement « L'Europe, continent connecté » COM(2013) 627 final ?

Le 4 juin 2012, à l'occasion de la transposition du Paquet Télécom en droit néerlandais, les Pays-Bas sont devenus le premier pays européen à inscrire dans leur droit national une protection de la neutralité des réseaux.

L'article 7.4 a de la Loi sur les télécommunications stipule que les fournisseurs de services d'accès à Internet ainsi que les gestionnaires de réseaux de télécommunication ne peuvent pas interdire ou ralentir l'accès à des services ou applications Internet. En outre, il est interdit aux fournisseurs d'accès de facturer les utilisateurs finaux différemment pour l'utilisation de différents types de services Internet ou des applications.

Cette transcription dans la loi de la "neutralité du Net » fait suite à une année de débats liés aux velléités des opérateurs néerlandais de télécommunication de surfacturer leurs clients utilisant des applications consommatrices en bande passante ; En ligne de mire, notamment, figuraient Skype pour la VoIP et WhatsApp pour la messagerie. Pour appliquer cette facturation, l'opérateur historique KPN était suspecté de se préparer à l'utilisation du Deep Packet Inspection (DPI), mettant à mal la vie privée de ses clients pour connaître leurs usages.

La loi limite donc les possibilités d'utilisation de technologies potentiellement intrusives, comme le "deep packet inspection" (DPI) et encadrent aussi le filtrage et le blocage des sites Web.

Le non-respect de cette nouvelle version de la loi peut ainsi mener à une amende pour l'opérateur, pouvant atteindre jusqu'à 10% de ses revenus annuels.

L'approche néerlandaise de la neutralité du net est observée avec beaucoup d'attention par de nombreux pays et le gouvernement néerlandais entend jouer un rôle de premier plan dans la mise ne œuvre des préceptes de la neutralité du net notamment au sein de l'union Européenne.

Q5/- Quelles sont les relations entre les pouvoirs publics du pays où vous représentez la France et l'association gérant le nommage sur Internet dans ce pays, équivalent de l'Association française pour le nommage Internet en coopération (AFNIC) ? Comment cette association se coordonne-t-elle avec l'ICANN et quel est son degré d'autonomie par rapport à ce dernier ? Est-il jugé suffisant pour permettre une stratégie nationale de fixation des noms de domaine ?

SIDN est l'association néerlandaise en charge des noms de domaine " .nl ". Elle comptabilise en mars 2014 près de 5 441 358 domaines en " .nl ".

Au niveau mondial, l'extension .nl se classe en 9ème position derrière le .com, le .tk, le .de, le . net, le . cn, le .uk, le .org, le .info .Les extensions de domaines en .nl sont détenues pour 94 % par des entreprises ou des particuliers résidant aux Pays-Bas.

[5] Les Pays-Bas ont récemment lancé un forum national de la gouvernance d'Internet « NL IGF ». Celui-ci est une initiative conjointe du ministère des affaires économiques, de SIDN (fondation en charge de l'allocation et de la gestion de l'extension nationale .nl et de ECP (plateforme pour la société de l'information). NL IGF se veut une plateforme d'échange sur les sujets liés à la gouvernance de l'internet et notamment un relais des discussions nationales ou internationales.

Service économique de La Haye

Le .nl est l'extension nationale avec la meilleure pénétration avec quelques 32 noms de domaine pour 100 habitants. Depuis longtemps les .nl étaient accessibles aux entreprises comme aux particuliers sans qu'un droit au nom soit demandé. Ceci explique cette forte adhésion au .nl (73,5 % de part de marché). Une autre explication est le fait que les Pays-Bas sont un des pays les mieux connectés d'Europe, ceci motivant la demande et la création de contenus auxquels il est aisé de donner une adresse se terminant par .nl.

Par ailleurs, le nombre de domaines en .nl sécurisés par le protocole de sécurisation du protocole DNS (DNSSEC) est de 1 695 991.

SIDN adhère à l'ICANN et à CENTR. La contribution de SIDN à l'ICANN a été en 2013 de 114 000 € et de 46 000 € à CENTR.

L'accroissement du nombre de domaine ".nl" traduit également l'importance économique et sociale du ".nl" et a conduit le gouvernement néerlandais et la SIDN à collaborer afin de renforcer la stabilité et la continuité de l'extension nationale ".nl".

Pour le gouvernement néerlandais, l'affectation et l'enregistrement des noms de domaine ".nl" doit rester une activité néerlandaise.

Les deux parties ont donc signé un accord en 2005 dans lequel elles s'engagent à la protection indéfinie du nom de domaine ".nl" et à maintenir le système auto-régulé, en vertu duquel les noms de domaine ".nl" sont alloués par SIDN.

SIDN est ainsi reconnu comme le seul administrateur de l'extension nationale tout en confirmant l'intérêt particulier du gouvernement néerlandais pour la stabilité et la continuité du nom de domaine.

Les deux parties se sont également entendues sur une série de mesures techniques, organisationnelles et juridiques afin de conforter l'extension nationale. Il a également été acté la mise en place d'un dispositif d'alerte précoce afin que les deux parties puissent se tenir mutuellement informées sur les menaces possibles et des décisions politiques affectant l'extension.

Aussi, les Pays-Bas ont-ils défini un scénario de redélégation de la gestion du nom de domaine " .nl " afin de faire en sorte qu'en cas de perturbation majeure et irréversible de la fonction de SIDN à l'égard de la gestion du ".nl " une continuité de service puisse être assurée.

Q6/- Quelle est la position des autorités du pays où vous représentez la France à l'égard de la proposition de règlement européen relatif à la protection des données personnelles en cours de négociation ? Quel avenir envisagent-elles pour l'accord Safe Harbor qui constitue depuis 2001, dans le domaine civil et commercial, le cadre juridique, pour permettre l'échange de données entre entreprises de l'Union européenne et entreprises américaines respectant un certain niveau de protection des données et qui repose donc sur l'auto-certification des entreprises? Quelle est leur position à l'égard de la communication de la Commission européenne publiée le 29 novembre 2013 et appelant au renforcement du « Safe Harbor » ?

Les Pays-Bas sont favorables aux objectifs poursuivis par la proposition de règlement – assurer un niveau élevé et homogène de protection des données partout sur le territoire de l'Union--, néanmoins ils considèrent que les droits fondamentaux ne sont pas suffisamment pris en compte notamment en ce qui concerne le traitement des données.

Service économique régional de Varsovie

POLOGNE

Q1/ Quelles sont les préoccupations majeures que soulève l'Internet dans le pays où vous représentez la France ?

L'Internet est perçu en Pologne avant tout comme un instrument qui offre de grandes opportunités et comme une chance, davantage que comme une source majeure de préoccupation.

Certaines préoccupations existent néanmoins, elles concernent en particulier les atteintes portées à la protection des données personnelles. La confiance du grand public envers les gouvernements et les entreprises du net a été atteinte par les révélations sur le transfert de données personnelles à des pays tiers. Les autorités polonaises se félicitent ainsi que la déclaration adoptée à l'issue du forum NETmundial ne légitime pas les pratiques de surveillance généralisée. Les révélations d'E. Snowden ont néanmoins eu un impact plus limité en Pologne que dans d'autres États membres de l'UE, sans doute en raison de l'absence de mise en cause de pratiques contestables visant directement la Pologne, mais aussi du fait du souci de garder de bonnes relations avec le partenaire américain.

La question de l'ouverture du réseau et de la liberté d'expression est importante aux yeux des Polonais, qui considèrent que c'est cette philosophie ouverte qui a permis au net de se développer et qu'il convient de la conserver. Ils sont méfiants vis-à-vis des initiatives qui paraissent la mettre en cause (controverses liées à l'ACTA en 2011, méfiance vis-à-vis des projets d' « internet sûr » en Europe qui pourraient cacher une volonté de segmentariser le réseau global…).

Q2/- La place de l'Union européenne dans la gouvernance mondiale de l'internet est-elle un sujet de préoccupation importante dans le pays où vous représentez la France, soit au niveau politique (exécutif/législatif), soit dans l'opinion publique ? Avez-vous connaissance d'initiatives politiques en ce domaine ?

Au niveau institutionnel, le ministère de l'administration et de la numérisation, qui est en charge de définir la politique publique de la Pologne en la matière, estime qu'il s'agit d'une question dont l'importance est croissante, ce qu'illustre d'ailleurs la publication de la communication de la Commission européenne. Le ministère a procédé à une large consultation publique en amont de la définition d'une position officielle polonaise (qui est encore en cours d'élaboration).

Q3/- Comment le pays où vous représentez la France considère-t-il le fonctionnement actuel de la gouvernance d'internet? Quelle est sa position à l'égard de la communication de la Commission européenne sur la gouvernance de l'internet publiée en février 2014 ?

La Pologne considère que le modèle actuel de gouvernance de l'internet est certes imparfait, mais qu'il a permis au réseau de se développer de façon impressionnante, sans être soumis à des restrictions dues au contrôle par des gouvernements ou des entreprises du net. Elle est très attachée au modèle multi-parties prenantes. Elle est consciente de la nécessité de renforcer la gouvernance centrale et prône l'amélioration du fonctionnement de l'*Internet Governance Forum* (renforcement du secrétariat,

rythme plus fréquent des réunions), tout en conservant le modèle actuel. Elle soutient la globalisation des fonctions IANA.

La position officielle de la Pologne sur la communication de la Commission est encore en cours d'élaboration (cf. ci-dessus), mais à titre préliminaire, le ministère de l'administration et de la numérisation fait part de 2 points qui suscitent sa préoccupation :

- Le danger d'une définition trop stricte des rôles respectifs des acteurs : une dose de flexibilité est nécessaire ;
- La question du rôle des gouvernements dans la définition des standards techniques (remise en cause possible du système actuel des *internet engineering task-forces*).

Q4/- Quelle est la position des autorités du pays où vous représentez la France à l'égard du principe de la neutralité du net, et notamment à l'égard de la définition qu'en propose la Commission européenne dans la proposition de règlement « L'Europe, continent connecté » COM(2013) 627 final ?

La Pologne soutient le principe de la neutralité du net, même si sa position officielle formelle fait toujours l'objet de consultations. Le secteur des industries du net n'est pas favorable à l'établissement d'une nouvelle régulation comportant une définition précise, considérant que la situation actuelle est satisfaisante. Selon le ministère de l'administration et de la numérisation, la définition de la neutralité du net proposée par le Parlement européen pour le projet de règlement sur le marché unique des télécoms ne devrait guère poser de problèmes. En revanche, le ministère considère que la définition proposée pour les services spécialisés est problématique car trop prescriptive. La Pologne considère que ces services ne constituent pas une menace pour l'accès aux services généraux, et souhaite d'une manière générale une régulation aussi souple que possible.

Q5/- Quelles sont les relations entre les pouvoirs publics du pays où vous représentez la France et l'association gérant le nommage sur Internet dans ce pays, équivalent de l'Association française pour le nommage Internet en coopération (AFNIC) ? Comment cette association se coordonne-t-elle avec l'ICANN et quel est son degré d'autonomie par rapport à ce dernier ? Est-il jugé suffisant pour permettre une stratégie nationale de fixation des noms de domaine ?

Le registre du domaine .pl est tenu par la NASK (Naukowa i Akademicka Sieć Komputerow, Réseau informatique scientifique et académique), qui est un opérateur indépendant (historiquement lié à l'Université de Varsovie), qui bénéficie du statut d'institut de recherche et fonctionne grâce à des subventions publiques et des recettes commerciales. La tutelle est exercée par le ministère de la science et de l'enseignement supérieur (qui désigne le directeur de la NAK), mais l'établissement dispose d'une grande autonomie de gestion (la quasi-totalité des membres du conseil de direction sont des scientifiques et universitaires).

La NASK, en tant qu'organisme gérant le nommage sur internet en Pologne, se coordonne avec l'ICANN, mais, pour autant que le gouvernement polonais puisse en juger, dispose d'une autonomie suffisante par rapport à ce dernier. La Pologne ne gère que domaine .pl et n'a pas vraiment de stratégie nationale de fixation des noms de domaine, qui n'est pas jugée indispensable : l'attribution des noms de domaine répond à la règle « premier arrivé, premier servi ».

Service économique régional de Varsovie

Q6/- Quelle est la position des autorités du pays où vous représentez la France à l'égard de la proposition de règlement européen relatif à la protection des données personnelles en cours de négociation ? Quel avenir envisagent-elles pour l'accord Safe Harbor qui constitue depuis 2001, dans le domaine civil et commercial, le cadre juridique, pour permettre l'échange de données entre entreprises de l'Union européenne et entreprises américaines respectant un certain niveau de protection des données et qui repose donc sur l'auto-certification des entreprises? Quelle est leur position à l'égard de la communication de la Commission européenne publiée le 29 novembre 2013 et appelant au renforcement du « Safe Harbor » ?

Concernant le projet de règlement sur la protection des données, la Pologne soutient une adoption aussi rapide que possible, de préférence avant la fin de 2014, qui serait compatible avec l'objectif d'achèvement du marché unique numérique en 2015. Elle défend également un niveau de protection élevé, et porte son attention sur un certain nombre de points prioritaires (voir la liste détaillée en annexe), parmi lesquels le consentement explicite, le profilage non-discriminatoire, le contrôle sur le transfert de données à des États tiers et la mise en place d'un guichet unique avec une supervision centralisée. La Pologne réfléchit à l'opportunité d'adopter dès le Conseil JAI de juin une partie des dispositions du projet de règlement, afin de marquer une première avancée.

La Pologne a accueilli favorablement la communication de la Commission appelant au renforcement de l'accord Safe Harbor, mais les dispositions que la Pologne souhaiterait voir adopter vont plus loin que ce que contient cette communication. En particulier, la Pologne insiste sur la gratuité des plaintes introduites par les citoyens, l'augmentation du nombre de requêtes des autorités de protection des données européennes à la Federal Trade Commission, et d'une manière plus générale un engagement accru du Département du commerce américain en faveur de la protection des données personnelles. Au cas où les négociations avec les États-Unis ne permettraient pas de progrès significatifs, la Pologne estime qu'il ne faut pas exclure, à terme, la possibilité que la Commission prononce la révocation de l'accord. Elle estime en tout état de cause qu'il n'est pas nécessaire d'attendre l'adoption du nouveau règlement européen sur la protection des données personnelles pour renégocier l'accord Safe Harbor. Une nouvelle décision de la Commission sur l'adéquation de Safe Harbor aux règles communautaires, après l'adoption du règlement, devrait suffire pour assurer la compatibilité.

Service économique régional de Varsovie

Annexe : Liste des points de vigilance de la Pologne concernant le projet de règlement sur la protection des données personnelles (en anglais)

From the Polish perspective the most important rules, which should constitute the foundation of the new EU data protection law are:

1. The **wide territorial and material scope** of the regulation (Poland is in favour of applying the new rules to entities from outside the EU in order to ensure a high level of data protection for our citizens enjoying the services of entities such as ones based in the U.S., and to provide a level playing field for our businesses).

2. **Broad definition of personal data** (in the Polish view, a broad definition of personal data is needed in the digital society – more and more seemingly irrelevant information may be used to identify us as individuals, especially on the Internet).

3. **Full control over one's data** (in our opinion effective protection of personal data is possible only if data subject has full control over his/her data)

4. **Explicit consent** (in our opinion, consent must be explicit, it can never be implied from other declarations of intent, only such consent will allow citizens to retain control over their own data).

5. **Privacy by design and by default** (all products and services should be designed with privacy in mind and offer the fullest protection by default)

6. **Informed and non-discriminatory profiling** (we think that in any case the data subject should be informed that it is subjected to profiling, profiling should also have not the effect of discrimination).

7. **Personal data protection based on the risk-based approach** (we are in favour of the further development of this concept, which links the obligations of the controller or processor with the risks that arise for citizens in relation to the particular processing of their data by a given administrator/processor).

8. **Reasonable sanctions** (sanctions adjusted to the scale of infringement, size of responsible party and caused risks to personal data protection)

9. **One-stop-shop** (we see benefits for both business and citizens related to the introduction of the "one-stop-shop" in the EU, we support the idea of a "meaningful" one-stop-shop with a single supervisory decision. We want to make the one-stop-shop fast, providing legal certainty and reducing administrative burdens).

10. **Control over data transfers to third countries** (Poland supports any solution that would allow the Member States to regain control over their citizens' personal data transferred to third countries. Instruments adopted by the Member States should aim to restore the confidence of citizens impaired, inter alia, due to media reports regarding PRISM and other surveillance programs. Poland supports i.a. the introduction to Chapter V of the draft regulation the additional Article 42a (as submitted in document 12884/13).

Service économique régional de Londres

ROYAUME-UNI

Q1/ Quelles sont les préoccupations majeures que soulève l'Internet dans le pays où vous représentez la France ?

Les révélations sur les programmes de grande envergure de surveillance de l'internet n'ont pas déclenché de réaction importante de l'opinion publique et des élus britanniques, bien que le journal Le Guardian continue de publier très régulièrement des articles sur le sujet. En particulier, la problématique très technique de la gouvernance d'Internet ne soulève pas d'intérêt dans l'opinion publique britannique selon les experts du ministère de la Culture, des Médias et des Sports en charge de la politique gouvernementale sur ces sujets. Bien que l'Open Data (privé et public) et le Big Data connaissent un essor significatif au Royaume-Uni, l'opinion britannique se montre assez peu sensible à l'enjeu de la protection des données (sauf dans le domaine de la santé qui soulève des véritables questions).

Le gouvernement britannique est néanmoins très intéressé par ces questions, plusieurs ministères (Cabinet Office, Ministère des Affaires Etrangères, Ministère des Entreprises, de l'Innovation et des Compétences) collaborant activement sur ces sujets avec le régulateur des télécommunications, l'Ofcom. Le gouvernement est également très actif sur les problématiques de protection des enfants (mise en place de filtres ISP pour contrôler les contenus, campagne de sensibilisation des parents sur la sécurité d'Internet) et de cyber sécurité.

Q2/- La place de l'Union européenne dans la gouvernance mondiale de l'internet est-elle un sujet de préoccupation importante dans le pays où vous représentez la France, soit au niveau politique (exécutif/législatif), soit dans l'opinion publique ?

Comme en France, le sujet de la gouvernance de l'Internet n'est pas perçu comme un enjeu majeur ni pour l'opinion publique, ni pour la classe politique. Le NetMundial n'a bénéficié d'aucune couverture médiatique par exemple.

Si le Royaume-Uni reconnait que l'UE joue un rôle important pour faciliter la coordination entre les États membres, il ne souhaite pas, sur ce sujet comme sur d'autres de façon plus générale, que l'UE obtienne plus de compétences en matière de gouvernance d'Internet. Le Royaume-Uni désapprouve notamment la volonté de la Commission européenne de «se proposer comme médiateur dans les futures négociations mondiales sur la gouvernance de l'internet »[6], estimant que la Commission n'est pas légitime pour parler au nom de l'ensemble des États membres sur ce sujet.

Avez-vous connaissance d'initiatives politiques en ce domaine ?

Le gouvernement a créé début 2013 un groupe consultatif multipartite sur la gouvernance de l'Internet (Multistakeholder Advisory Group on Internet Gouvernance - MAGIG) pour l'aider à affiner ses positions sur le sujet. Près de 5 réunions sont organisées annuellement, en règle générale en amont de grands évènements internationaux ou européens qui traiteront des questions de gouvernance de l'Internet. Le MAGIG est présidé par le Ministère de la Culture, des Médias et des Sports (DCMS), qui est en charge de la politique en matière de télécommunications et d'Internet. Des membres du ministère des Entreprises, de l'Innovation et des Compétences (BIS), du ministère des Affaires Etrangères (FCO), du ministère de l'Intérieur (Home Office) et du ministère du Développement International (DfID) assistent également aux réunions. Le MAGIG regroupe une trentaine de membres de la société civile : le régulateur Ofcom, l'association professionnelle du secteur technologique Tech

[6] « La Commission se propose comme médiateur dans les futures négociations mondiales sur la gouvernance de l'internet », lien

UK, des entreprises du secteur des télécommunications (BT, Vodafone, Yahoo UK, Microsoft, Skype, ARM Holdings, Virgin Media, Google UK, Facebook, GSMA, Intel UK etc.), le London Stock Exchange, un représentant de l'ICANN et des membres du Third Sector (Taxpayers Alliance, London School of Economics, Oxford Internet Institute, Trade Union Congress, Childnet, Global Partner Digital etc.). Les réunions se déroulent dans le respect de la règle 'Chatham House'.[7]

Q3/- Comment le pays où vous représentez la France considère-t-il le fonctionnement actuel de la gouvernance d'internet? Quelle est sa position à l'égard de la communication de la Commission européenne sur la gouvernance de l'internet publiée en février 2014 ?

Le Royaume-Uni soutient le modèle de gouvernance multipartite actuellement en vigueur. Il estime qu'il apporte la flexibilité suffisante permettant de s'adapter aux évolutions rapides d'Internet. Dans cette optique, le RU s'inquiète que les tentatives de codification des rôles et des responsabilités de chacun aboutisse à une structure rigide qui sera incapable de répondre de manière efficace aux défis futurs et étouffera l'innovation et le dynamisme d'Internet.

Le RU n'est pas favorable à un renforcement du rôle des États. Notre contact au DCMS a notamment avancé deux éléments de justification :

- Le RU estime qu'un renforcement du rôle des États risque de nuire au dynamisme qui résulte des négociations multi-acteurs ;
- Il considère que cette approche risque d'aboutir à une fragmentation de l'Internet, ce qui aurait des conséquences économiques négatives (développement de standards techniques différents, obstacles aux commerce etc.) et des conséquences sociales négatives (un rôle accru des états permettrait à certains gouvernements autoritaires de restreindre les libertés publiques sur Internet sur leur territoire) ;

S'il est favorable au modèle actuel, le Royaume-Uni souhaiterait voir des évolutions dans deux domaines :

- Réformer le Forum International sur la Gouvernance (IGF) afin qu'il soit en mesure de produire des résultats plus concrets sur des enjeux spécifiques (secrétariat renforcé etc.)
- Soutenir le renforcement des compétences des pays en développement et les économies émergentes (capacity building) : le RU considère que le modèle actuel prend insuffisamment en compte les acteurs n'ayant pas les ressources suffisantes pour agir dans ce domaine : les forums et les organisations internationales d'Internet devraient mieux intégrer cette nécessité de capacity building (développement des infrastructures, régimes réglementaires etc.) par des mesures pratiques afin qu'ils puissent également bénéficier des retombées économiques et sociales d'Internet;

Q4/- Quelle est la position des autorités du pays où vous représentez la France à l'égard du principe de la neutralité du net, et notamment à l'égard de la définition qu'en propose la Commission européenne dans la proposition de règlement « L'Europe, continent connecté » COM(2013) 627 final ?

Le Royaume-Uni soutient le principe de neutralité du net mais estime que l'application de ce principe doit découler de l'autorégulation et non de la réglementation. Il considère que la position initiale de la Commission est trop contraignante et aurait préféré que la Commission propose une recommandation et non une réglementation. Le RU estime que le texte adopté par la commission ITRE va beaucoup trop loin. Le RU s'inquiète du fait que la tentative de définition soit trop restrictive et nuise aux politiques nationales mises en place, par exemple dans le cas de la lutte pour la protection des enfants où les fournisseurs internet devront au préalable obtenir une décision du tribunal (court order) pour

[7] Les membres peuvent divulguer publiquement des informations révélées lors de la discussion mais ne sont pas autorisés à révéler l'identité ou l'affiliation de l'individu qui a fait la remarque.

bloquer des pages Internet contenant des images d'abus d'enfants, alors qu'ils sont en mesure de le faire actuellement sans aucune décision judiciaire.[8]

Q5/- Quelles sont les relations entre les pouvoirs publics du pays où vous représentez la France et l'association gérant le nommage sur Internet dans ce pays, équivalent de l'Association française pour le nommage Internet en coopération (AFNIC) ? Comment cette association se coordonne-t-elle avec l'ICANN et quel est son degré d'autonomie par rapport à ce dernier ? Est-il jugé suffisant pour permettre une stratégie nationale de fixation des noms de domaine ?

Nominet est l'association gérant le nommage Internet au Royaume-Uni (noms de domaine uk, .wales et .cymru). Créé en 1996, Nominet est une private, not-for-profit membership company, limited by guarantee. Le gouvernement entretient une relation de collaboration avec Nominet, avec qui il travaille notamment dans le cadre de l'élaboration de la position britannique sur les enjeux liés à l'Internet. Nominet est notamment membre du groupe consultatif MAGIG. Nominet entretient comme l'AFNIC des relations d'échange avec l'ICANN. Nominet est un acteur actif dans les débats sur la gouvernance d'internet, participant notamment au World Wide Web Consortium (W3C), à l'Internet Governance Forum (IGF and also UK-IGF) and the Council for European National Top Level Domain Registries (CENTR).

Le Royaume-Uni salue le fait que l'ICANN ait pris des mesures pour « se mondialiser ». Il s'est félicité de l'affirmation des engagements (Affirmation of Commitments), la considérant comme première étape dans le processus de mondialisation de la responsabilité de l'ICANN. Le RU estime que ce dernier devrait continuer, recommandant notamment la mise en place de mécanismes d'auto-évaluation et de révision par les pairs. Ainsi, si le Royaume-Uni est favorable à plus de mesures de « responsabilité » (accountability), il souhaite que celles-ci ne soient pas de nature juridique. Par ailleurs, le Royaume-Uni est favorable à la mise en place d'un droit de recours mais est opposé à la mise en place d'un droit de réparation.

Q6/- Quelle est la position des autorités du pays où vous représentez la France à l'égard de la proposition de règlement européen relatif à la protection des données personnelles en cours de négociation ?

Le Royaume-Uni souhaiterait que la législation en matière de protection des données prenne la forme d'une directive et non d'une réglementation. Il est satisfait de la proposition d'avoir un « one stop shop » pour les entreprises et les citoyens lorsqu'ils veulent formuler une plainte contre une entreprise qui opère dans plusieurs pays de l'UE.

Quel avenir envisagent-elles pour l'accord Safe Harbor qui constitue depuis 2001, dans le domaine civil et commercial, le cadre juridique, pour permettre l'échange de données entre entreprises de l'Union européenne et entreprises américaines respectant un certain niveau de protection des données et qui repose donc sur l'auto-certification des entreprises?

Quelle est leur position à l'égard de la communication de la Commission européenne publiée le 29 novembre 2013 et appelant au renforcement du « Safe Harbor » ?

Le Royaume-Uni est favorable à une réforme de Safe Harbor mais il est clairement opposé à une suspension de cet accord lors des négociations, estimant qu'il est non seulement très utile mais également qu'une telle décision générerait de l'incertitude juridique. Le RU pense qu'il faut faire évoluer le modèle actuel car il considère que certaines options alternatives ne seront pas viables car beaucoup trop contraignantes et coûteuses (contrats inter-entreprises, binding corporate rules, adequacy)

[8] At present a UK-based organisation called the Internet Watch Foundation maintains a list of web pages containing images of child abuse so that ISPs can block the content - a process that does not involve court orders.

Service économique de Stockholm

SUÈDE

Q1/ Quelles sont les préoccupations majeures que soulève l'Internet en Suède ?

Selon le gouvernement suédois, le développement de l'internet doit être caractérisé par l'ouverture, la liberté, l'accessibilité et la sécurité au bénéfice des citoyens, des entreprises, des organisations et du secteur public. La Suède milite également pour un internet non-fragmenté.

En Suède, internet joue un rôle majeur dans l'économie et dans le secteur de la protection sociale, et son utilisation est prise en compte dans la définition des politiques publiques suivantes : la santé, le droit des consommateurs, la défense etc…

La Suède s'engage à l'international dans le développement de l'internet au travers de l'ICANN et du Forum de la Gouvernance de l'Internet. Cependant, la Suède ne souhaite pas un renforcement du pouvoir des gouvernements dans la gouvernance mondiale de l'internet, et favorise une approche décentralisée et multipartite.

Q2/- La place de l'Union européenne dans la gouvernance mondiale de l'internet est-elle un sujet de préoccupation importante en Suède, soit au niveau politique (exécutif/législatif), soit dans l'opinion publique ? Avez-vous connaissance d'initiatives politiques en ce domaine ?

La place de l'Union européenne dans la gouvernance mondiale de l'internet n'est pas un sujet de préoccupation pour le gouvernement suédois.

Si la question porte plus précisément sur le champ d'application des domaines de compétence de la Commission européenne, la Suède ne voit aucune raison de considérer que la gouvernance mondiale de l'internet ne devrait pas être un domaine de compétence de la Commission européenne.

Q3/- Comment la Suède considère-t-elle le fonctionnement actuel de la gouvernance d'internet? Quelle est sa position à l'égard de la communication de la Commission européenne sur la gouvernance de l'internet publiée en février 2014 ?

La Suède accueille favorablement la communication de la Commission européenne de février 2014 portant sur la gouvernance de l'internet. En particulier, la Suède soutient : (i) un internet unique et non fragmenté qui promeut la liberté et l'ouverture sur le monde; (ii) un modèle de gouvernance multipartite de l'internet concernant les noms de domaines et les numéros attribués à internet ; (iii) un internet qui défend et promeut les droits de l'homme et la liberté d'expression, que ce soit en ligne ou hors-ligne.

Sur certains points, la Suède a des positions qui diffèrent de la Commission européenne: (i) les principes de l'internet devraient être globaux afin de bénéficier d'un soutien maximal ; (ii) la gestion des noms de domaines et des numéros attribués à internet relève des questions d'ordre technique ; (iii) la Suède est membre du groupe de travail mis en place pour renforcer le Forum de la Gouvernance de l'Internet, mais le gouvernement suédois ne soutient pas l'idée d'une réforme globale et ne souhaite pas que ce forum devienne un organe de décision ; (iv) le gouvernement suédois souligne l'importance de ne pas définir clairement les rôles des parties prenantes puisque les différents acteurs ont des intérêts qui se chevauchent.

Par ailleurs, la Suède favorise une approche souple et ouverte, afin de favoriser le développement et l'innovation.

Concernant la mise en place de normes, la Suède souhaite améliorer les échanges entre les gouvernements et les organismes de normalisation, mais, selon elle, c'est aux gouvernements de s'adapter aux systèmes de normalisation, et non l'inverse.

Q4/- Quelle est la position des autorités suédoises à l'égard du principe de la neutralité du net, et notamment à l'égard de la définition qu'en propose la Commission européenne dans la proposition de règlement « L'Europe, continent connecté » COM(2013) 627 final ?

La Suède promeut un internet ouvert et est consciente du fait que la régulation de la neutralité du net est un grand défi. Le gouvernement suédois souligne que les violations du principe de neutralité du net ne sont pas un problème majeur dans le pays.

La Suède émet de profondes réserves concernant la communication « COM(2013) 627 final » de la Commission européenne. L'article 23 (23.2 et 23.5) cristallise à lui seul les doutes de la Suède sur ce texte selon lequel « le diable serait dans le détail ». Selon la Suède, la régulation ne devrait pas être trop contraignante et ne pas se faire au détriment du développement de services innovants sur internet. La Suède est en faveur d'une régulation concernant les principes généraux de l'internet, et se montre réservée quant aux définitions très détaillées et techniques qui pourraient paraitre appropriées aujourd'hui, mais qui seraient vouées à l'échec dans le long terme. La Suède émet donc des réserves sur les définitions suivantes : la « neutralité du net » en tant que tel, ainsi que les «services spécialisés», les «services d'accès à Internet» et la «qualité générale des services d'accès à Internet ». Selon le gouvernement suédois, il serait important que la régulation choisie puisse être supervisée et appliquée facilement.

Pour résumer, la Suède ne soutient pas la Communication de la Commission en l'état. Selon le gouvernement suédois, un texte plus court et plus simple, qui impliquerait davantage l'ORECE et qui favoriserait le développement de critères techniques pour surveiller la neutralité du net, pourrait améliorer la future législation européenne.

Q5/- Quelles sont les relations entre les pouvoirs publics suédois et l'association gérant le nommage sur Internet dans ce pays, équivalent de l'Association française pour le nommage Internet en coopération (AFNIC) ? Comment cette association se coordonne-t-elle avec l'ICANN et quel est son degré d'autonomie par rapport à ce dernier ? Est-il jugé suffisant pour permettre une stratégie nationale de fixation des noms de domaine ?

La « Stiftelsen för Internetinfrastruktur » (la Fondation de l'infrastructure de l'internet) est une entité indépendante du gouvernement suédois qui gère le nom de domaine « .SE ». Elle est nommée par l'ICANN et est obligée de respecter la loi sur les noms de domaines nationaux.

Le gouvernement suédois nous a précisé qu'il existait une bonne coopération entre ces différentes entités et que la « Stiftelsen för Internetinfrastruktur » servait de point de référence lors des échanges avec les parties prenantes.

Service économique de Stockholm

Q6/- Quelle est la position des autorités suédoises à l'égard de la proposition de règlement européen relatif à la protection des données personnelles en cours de négociation ? Quel avenir envisagent-elles pour l'accord Safe Harbor qui constitue depuis 2001, dans le domaine civil et commercial, le cadre juridique, pour permettre l'échange de données entre entreprises de l'Union européenne et entreprises américaines respectant un certain niveau de protection des données et qui repose donc sur l'auto-certification des entreprises? Quelle est leur position à l'égard de la communication de la Commission européenne publiée le 29 novembre 2013 et appelant au renforcement du « Safe Harbor » ?

La Suède estime qu'il est nécessaire de moderniser le cadre juridique actuel de la protection des données au sein de l'Union européenne, et le pays partage l'ambition de moderniser le fonctionnement du marché intérieur. Cependant, la Suède souhaite : (i) laisser une certaine flexibilité aux États membres dans le secteur public ; (ii) laisser la possibilité aux États membres de mettre en place des législations nationales concernant le droit d'accès aux documents officiels ; (iii) souligne la nécessité de fixer des règles adaptées aux différentes autorités, afin d'assurer une protection suffisante des données ; (iv) appliquer le principe de subsidiarité avec la mise en place de règles au niveau national, afin de considérer les différences de structures entre les États membres.

La Suède accueille favorablement la communication de la Commission européenne publiée en novembre 2013 et appelant au renforcement du « Safe Harbor ». La Suède est favorable à la révision des principes du « Safe Harbor », afin que les nouvelles règles assurent une protection suffisante de la vie privée des individus. La Suède met l'accent sur l'importance, pour les milieux d'affaires, du maintien d'un flux de données entre l'Union européenne et les États-Unis. Cependant, le gouvernement suédois ne souhaite pas que les décisions soient prises à la hâte, et veut prendre le temps d'étudier les futures réactions des Américains concernant la communication de la Commission européenne. La Suède se félicite de la poursuite du débat sur ces questions.