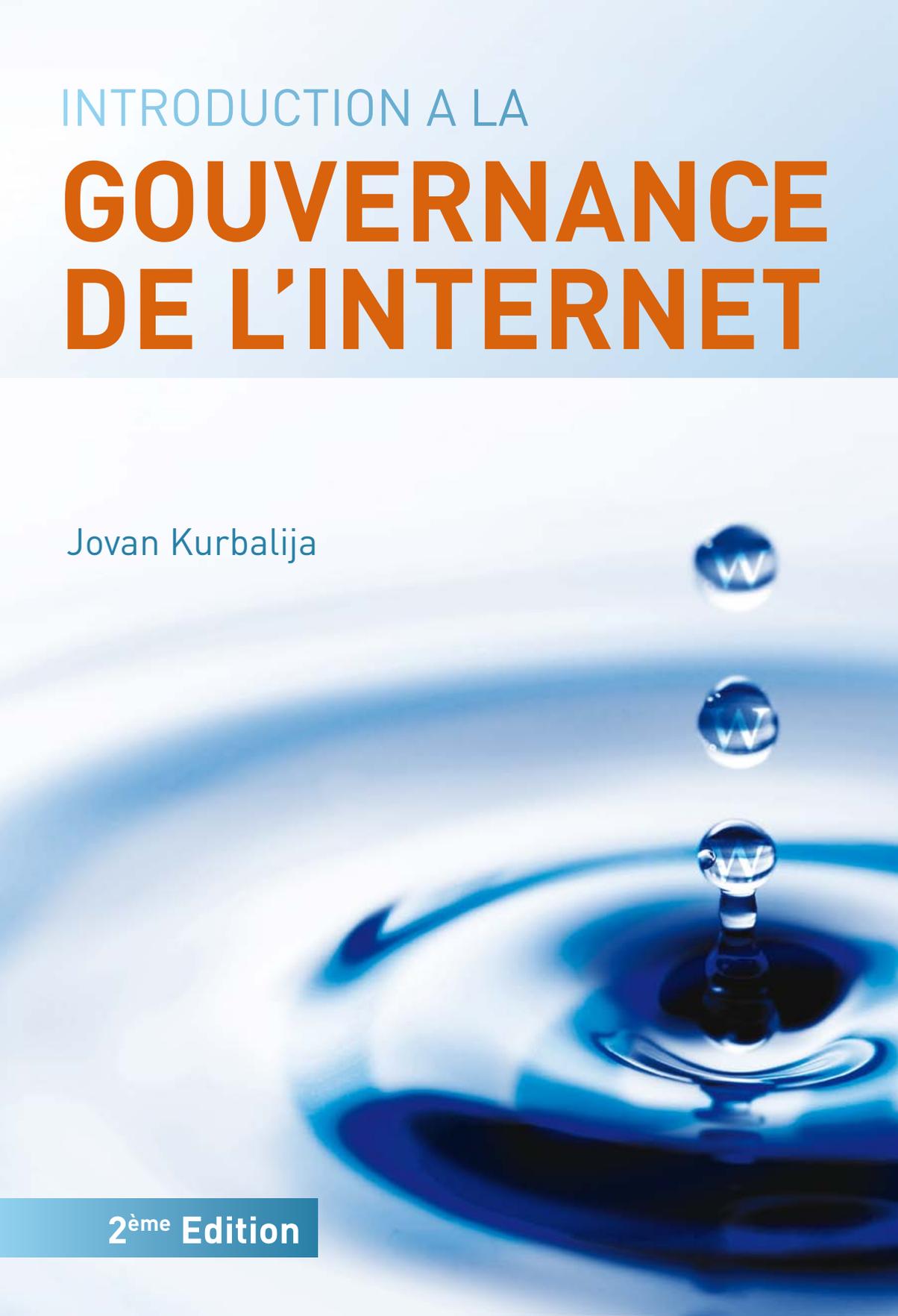


INTRODUCTION A LA

# GOUVERNANCE DE L'INTERNET

Jovan Kurbalija

2<sup>ème</sup> Edition



L'histoire de ce livre est longue, si on tient compte de la date d'apparition de l'Internet. Le texte original et l'approche générale, y compris la méthodologie des cinq corbeilles, ont été développés en 1997 pour un cours de formation sur les politiques des Technologies de l'Information et de la Communication (TIC) pour les officiels gouvernementaux des pays membres du Commonwealth.

En 2004, Diplo a publié une version imprimée de son document sur la gouvernance de l'Internet, sous forme d'un livret intitulé- *Gouvernance de l'Internet- Problèmes, Actions et Fractures*.

Ce livret a fut intégré à la *Documentation sur la Société de l'Information* une initiative de Diplo conduite par Stefano Baldi, Eduardo Gelbstein et Jovan Kurbalija. Que nos remerciement soient adressés spécialement à Eduardo Gelbstein, qui a fait d'importantes contributions aux sections traitant de la cyber-sécurité, du Spam, et de la vie privée ; à Vladimir Radunovic et Ginger Paque qui ont mis à jour les matériaux de cours. Les commentaires et suggestions d'autres collègues ont été pris en compte dans le texte. Stefano Baldi, Eduardo Gelbstein, et Vladimir Radunovic ont tous de façon significative contribué au développement des concepts qui sont expliqués par les illustrations de ce livre.

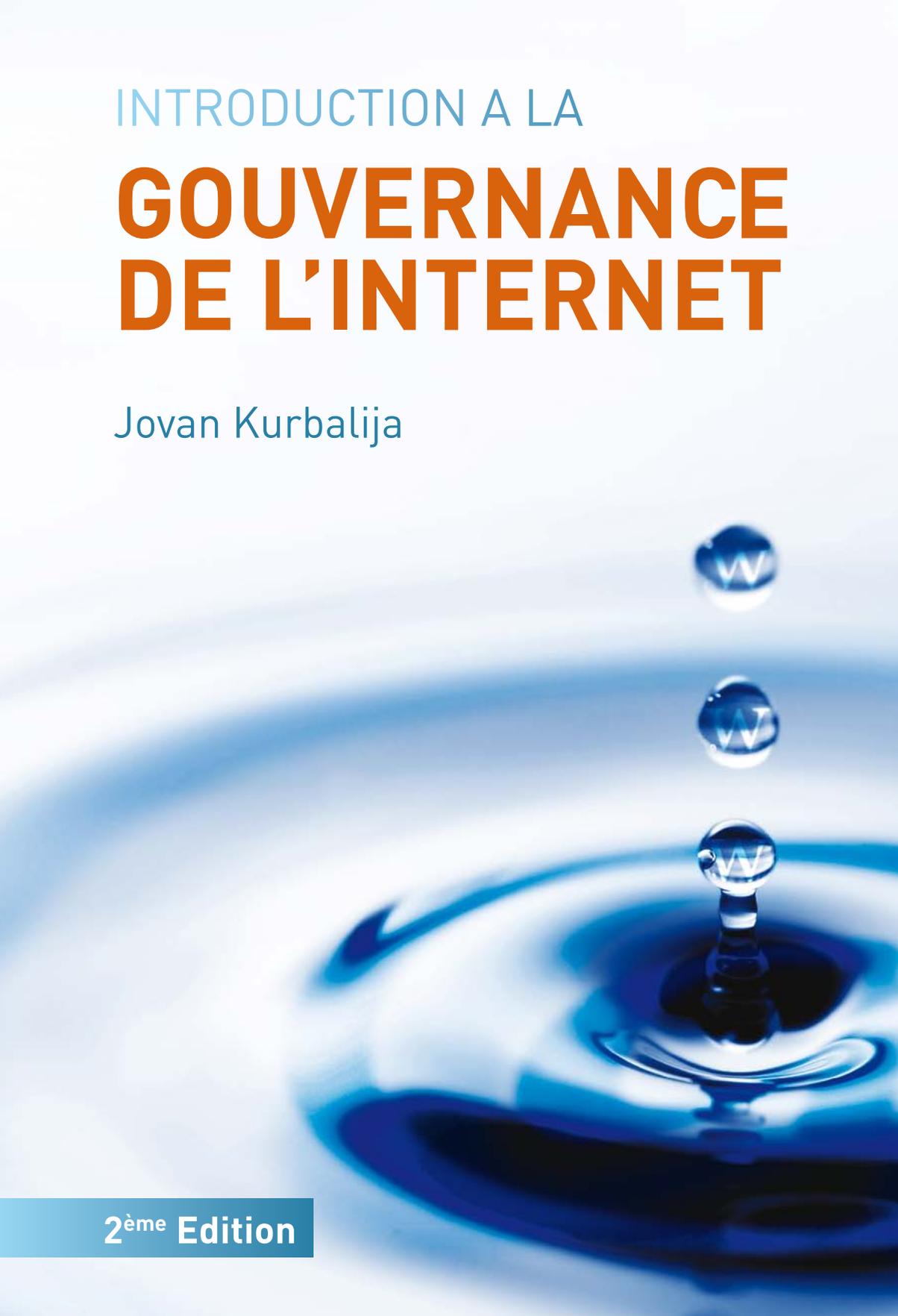
En 2008, une version spéciale révisée du livret intitulée simplement *une introduction à la gouvernance de l'Internet* avait été éditée en coopération avec la NIXI-Inde, à l'occasion du Forum sur la Gouvernance de l'Internet 2008 tenu à Hyderabad en Inde. En 2009, une troisième édition révisée a été publiée en coopération avec le Ministère des Technologies de l'Information et de la Communication de l'Egypte. Le livret *Gouvernance de l'Internet* en est maintenant à sa quatrième édition (2010), laquelle a été produite avec l'appui du Secrétariat du Groupe des Etats ACP et Union Européenne.

INTRODUCTION A LA

# GOUVERNANCE DE L'INTERNET

Jovan Kurbalija

2<sup>ème</sup> Edition



---

**Publié par DiploFoundation (2011)**

Malte: 4th Floor, Regional Building Regional Rd. Msida, MSD 13, Malta

Suisse: DiploFoundation Rue de Lausanne 56 CH-1202 Genève 21, Suisse

Courriel: [diplo@diplomacy.edu](mailto:diplo@diplomacy.edu)

Site Web: <http://www.diplomacy.edu>

Couverture: the Argument by Design

Edition:

Illustrations: Zoran Marcetic – Marča & Vladimir Veljašević

Mise en page et Maquette: the Argument by Design

La traduction et la publication de cet ouvrage dans d'autres langues est encouragée. Pour plus d'information, veuillez contacter [diplo@diplomacy.edu](mailto:diplo@diplomacy.edu)



Sauf disposition contraire, cet ouvrage est sous licence sous.  
<http://creativecommons.org/licences/by-nc-nd/3.0/>

---

Toute référence à un produit particulier de cet ouvrage doit être purement donnée à titre d'exemple servir d' et ne doit en aucun cas pas être considéré comme une approbation ou une recommandation dudit produit.. Tous les liens hypertextes utilisés dans cet ouvrage étaient valides jusqu'au 6 Aout 2010.

Ce document a été produit avec l'appui financier de l'Union Européenne. Les positions exprimées dans ce document relèvent de la seule responsabilité de Diplofondation et ne peuvent en aucune circonstance être considérées comme reflétant celles de l'Union Européenne.

---

Cette deuxième édition française de l'Introduction à la gouvernance de l'Internet a été traduite de la 4ème édition anglaise, et édité par les institutions partenaires suivantes: le Centre Africain de Complémentarité Scolaire, Universitaire et de Promotion (CACSUP) et au Burundi Youth Training Centre (BYTC).

ISBN: 978-99932-53-25-9



**DIPLO**  
www.diplomacy.edu



# Table des Matières

Avant-propos	1
<b>Section 1: Introduction</b>	<b>5</b>
Que veut dire gouvernance de l'Internet?	5
L'évolution de la gouvernance de l'Internet	7
La trousse à outils cognitive de la Gouvernance de l'Internet	13
Approches et modèles	15
Principes directeurs	21
Les analogies	24
Classification des enjeux de la gouvernance de l'Internet	30
Immeuble en construction: Sommes-nous entrain de construire la tour de Babel du 21ème siècle?	32
<b>Section 2: La corbeille de l'infrastructure et normalisation</b>	<b>37</b>
Les infrastructures de télécommunications	38
Le 'Transport Control Protocol/ Internet Protocol' (TCP/IP)	40
Le système de nom de domaine (DNS)	43
Les serveurs racines	48
La neutralité de réseau	51
Les Fournisseur d'Accès Internet (FAI)	60
Les Fournisseurs de Bande Passante Internet (Internet Broadband Band Providers - IBP)	62
Un modèle économique de l'inter connectivité de l'Internet	63
Les normes du web	67
Informatique en nuages	68
Convergence internet-télécommunication-multimédia	70
La cyber sécurité	72
Le cryptage	76
Pollupostage	78
<b>Section 3: La corbeille juridique</b>	<b>91</b>
Instruments juridiques	91
Juridiction	97
Arbitrage	100
Droits d'auteur	102
Marques déposées	108
Brevets	108
Cyber criminalité	108
Droit du travail	110
<b>Section 4: La corbeille économique</b>	<b>117</b>
La définition du commerce électronique	117
La protection des consommateurs	121
Fiscalité	123
Signature numérique	124
Paiement électronique: Transaction bancaires et monnaie électronique	126

<b>Section 5: La corbeille développement</b>	<b>135</b>
La fracture numérique .....	137
L'accès universel .....	138
Stratégies pour surmonter la fracture numérique.....	138
<b>Section 6: La corbeille socio-culturelle</b>	<b>147</b>
Les droits de l'homme .....	147
La politique du contenu .....	150
La vie privée et la protection des données .....	155
Multilinguisme et diversité culturelle .....	160
Biens publics universels .....	161
Droits des personnes vivant avec un handicap.....	163
Education .....	164
La sécurité de l'enfant en ligne .....	166
<b>Section 7: Les parties prenantes de la gouvernance de l'Internet</b>	<b>177</b>
Les gouvernements .....	179
Le secteur privé .....	184
La société civile .....	187
Les organisations internationales .....	188
La communauté de l'Internet .....	189
LICANN (Internet Corporation for Assigned Names and Numbers) .....	191
<b>Section 8: Le processus de la gouvernance de l'Internet</b>	<b>199</b>
Ce que les décideurs peuvent apprendre du FGI.....	199
Approches de résolution des questions de politiques globales .....	201
Gestion des processus d'élaboration des politiques .....	203
Traitements des aspects scientifiques et techniques dans les processus d'élaboration des politiques .....	206
Augmenter l'inclusion et la participation.....	208
<b>Section 9: Annexe</b>	<b>217</b>
Un voyage à travers la gouvernance de l'Internet .....	217
Le cube de la gouvernance de l'Internet .....	218
Un aperçu de l'évolution de la gouvernance de l'Internet .....	219
Au sujet des paysACP, de Diplo, et de l'UE .....	222
Au sujet de l'auteur .....	224

# Avant-propos

**E**n 2004, quand j'ai dit à mes amis ce que je faisais en tant que membre du Groupe de Travail sur la Gouvernance de l'Internet (GTGI)-, ils faisaient souvent appel à moi pour réparer leurs imprimantes ou installer de nouveaux logiciels. Pour eux, je faisais quelque chose lié à l'informatique. Je me rappelle avoir réalisé un bref sondage auprès de mes collègues membres du GTGI, leur demandant comment ils expliquaient aux amis, partenaires et aux enfants ce qu'ils faisaient. Comme moi, ils avaient les mêmes difficultés. C'est l'une des raisons pour lesquelles j'ai commencé à concevoir et monter le premier texte de Diplo ainsi que les dessins à propos de la Gouvernance de l'Internet.

Aujourd'hui, six ans plus tard, les mêmes personnes qui me demandaient d'installer leurs imprimantes reviennent à moi avec des questions sur la façon de protéger leur vie privée sur Facebook ou comment s'assurer que leurs enfants peuvent naviguer sur l'Internet en toute sécurité. Certains se demandent même si la relation apparemment tumultueuse entre la Chine et Google ou l'actuel débat sur une cyber-guerre ont quelque chose à voir avec la gouvernance de l'Internet. Comme nous sommes tous venus de loin !

La gouvernance de l'Internet prend de plus en plus d'importance dans l'opinion publique. Plus la société moderne dépendra de l'Internet, plus les questions liées à la gouvernance de l'Internet seront pertinentes. Loin d'être une affaire de quelques-uns, la Gouvernance de l'Internet nous concerne tous, à un degré plus ou moins grand, que nous soyons l'un des 2 milliards d'utilisateurs de l'Internet ou un non-utilisateur qui dépend juste de ses services.

La gouvernance de l'Internet est évidemment plus intéressante pour ceux qui sont profondément versés dans le cyber-espace, que ce soit par le e-business ou tout simplement en réseau sur Facebook. Pourtant, elle a une portée plus large. Les responsables gouvernementaux, les militaires, les avocats,

les diplomates et d'autres qui sont impliqués soit dans l'offre des services publics ou dans la préservation de la stabilité de l'ordre public sont également concernés. La gouvernance de l'Internet, et en particulier la protection de la vie privée et des droits de l'homme, est un point important pour les militants de la société civile et les organisations non gouvernementales (ONG).

Pour les universités et les innovateurs du monde entier, la gouvernance d'Internet doit s'assurer que l'Internet reste ouvert pour le développement et l'innovation. Les inventeurs de Google, Skype, Facebook et Twitter de demain sont là quelque part, entrain de surfer sur le Net. Leur créativité et innovation ne doivent pas être étouffées ; elles devraient plutôt être encouragées afin de développer de nouvelles façons plus créatives d'utiliser Internet. L'un des principaux objectifs de la gouvernance de l'Internet est de créer un environnement favorable au développement, qui permettrait une meilleure utilisation de l'Internet en tant que moteur du développement.

J'ai bon espoir que ce livre fournira une introduction claire et accessible sur la Gouvernance de l'Internet. Pour certains d'entre vous, ce sera votre première rencontre avec le sujet. Pour d'autres, il peut servir comme un rappel sur ce que vous faites déjà dans votre domaine d'activité, que ce soit l'e-santé, l'e-commerce, l'e-gouvernance, ou e-n'importe quoi faisant partie de la grande famille de la Gouvernance de l'Internet.

L'objectif sous-jacent à une approche aussi diversifiée est de contribuer modestement à la préservation de l'Internet comme un médium intégré et plein d'opportunités pour des milliards de personnes vivant dans le monde. Pour terminer j'ose espérer que cela aiguïsera votre appétit et vous encouragera à approfondir ce sujet aussi remarquable qu'abordable.

Restez au courant. Suivez les derniers développements sur <http://www.diplomacy.edu/isl/ig/>

**Jovan Kurbalija**  
**DiploFoundation**  
**Août 2010**

# Section 1

---

## Introduction

Bien que la gouvernance de l'Internet traite du symbole majeur du monde **numérique**, la gouvernance ne peut pas être gérée dans une logique numérique binaire vrai/faux et bon/mauvais. Au lieu de cela, la gouvernance d'Internet exige de nombreuses subtilités et nuances de sens et de perception; elle nécessite donc une approche **analogique**, couvrant un continuum d'options et de compromis.

Par conséquent, ce livre ne vise pas à fournir des solutions toutes faites sur les questions de la gouvernance de l'Internet. Au contraire, son but est de proposer un cadre pratique d'analyse, de discussion et de résolution d'importantes questions dans le domaine.





# Introduction

La controverse qui entoure la question de la gouvernance de l'Internet commence avec sa définition. Cela n'est pas seulement un jeu de mots. Les différentes interprétations du terme 'gouvernance de l'Internet' ont conduit à des approches et attentes différentes. Par exemple, les spécialistes en télécommunications voient la gouvernance de l'Internet à travers le prisme du développement de l'infrastructure technique. Les informaticiens eux se concentrent sur le développement de différentes normes et applications, telles que le XML (eXtensible Markup Language) ou – Java. Les spécialistes de la communication insistent sur la facilité que cela implique dans la communication. Les militants des droits de l'Homme voient la gouvernance de l'Internet dans une perspective de liberté d'expression, de respect de la vie privée et d'autres droits humains fondamentaux. Les juristes se concentrent sur les aspects juridictionnels et le règlement des différends. Les politiciens dans le monde entier se focalisent généralement sur les médias et les questions en relation avec leur électorat ; comme le techno-optimisme (plus d'ordinateurs = plus d'éducation) et les menaces (sécurité sur l'Internet, protection des enfants). Les diplomates sont principalement préoccupés par le processus sous l'angle de la protection des intérêts nationaux. La liste des professionnels potentiellement en conflit par leur point de vue sur la gouvernance d'Internet n'est pas exhaustive.

## Que veut dire gouvernance de l'Internet?

Le Sommet Mondial sur la Société de l'Information (SMSI)<sup>1</sup> est parvenu à la définition pratique suivante de la gouvernance de l'Internet:

*La gouvernance de l'Internet est le développement et l'application par les Gouvernements, le secteur privé et la société civile, dans leurs rôles respectifs, de principes partagés, de normes, de règles, de procédures décisionnelles et de programmes qui modèlent l'évolution et l'usage de l'Internet.<sup>2</sup>*

## 'I'nternet ou 'i'nternet et signalement diplomatique

En 2003, le magazine 'The Economist' a commencé écrire le mot Internet avec un 'i' minuscule. Ce changement de politique éditoriale a été inspiré par le fait que l'Internet était devenu un sujet de tous les jours, plus unique et assez spécial, pour justifier une première lettre en majuscule. Le mot 'Internet' a suivi le destin linguistique de (t)élégraphe, (t)éléphone, (r)adio, et (t)élévision, et d'autres inventions similaires.

La question d'écrire l'Internet/internet avec un 'i' majuscule ou minuscule est réapparue à la conférence de l'Union Internationale des Télécommunications (UIT) d'Antalya (novembre 2006), là où une dimension politique a été présentée quand le terme Internet est apparu dans la résolution de l'UIT concernant la gouvernance de l'Internet avec un 'i' minuscule au lieu de 'l'habituel' 'I' majuscule. **David Brut**, l'ambassadeur des Etats Unis responsable de la gouvernance de l'Internet, a exprimé des inquiétudes dans le sens que l'épellation minuscule de l'UIT pourrait signaler l'intention à traiter l'Internet comme d'autres systèmes de télécommunications internationalement régis par l'UIT. Certains ont interprété cela comme un signal diplomatique de l'UIT de jouer un rôle plus important dans la gouvernance de l'Internet.<sup>3</sup>

Cette définition, plutôt large, et fonctionnelle, ne résout pas la question des différentes interprétations des deux termes clés: 'Internet' et 'gouvernance'.

### Internet

Certains auteurs soutiennent que le terme 'Internet' ne couvre pas l'ensemble des aspects existants de l'évolution numérique mondiale. Deux autres termes – société de l'information et technologie de l'information et de la communication (TIC) – sont souvent présentés comme plus explicites. Ils incluent les secteurs qui sont en dehors du domaine de l'Internet, telle que la téléphonie mobile. Cependant, l'argument en faveur de l'utilisation du terme 'Internet' est surtout dicté par la rapide transition des communications mondiales vers l'utilisation du protocole Internet (IP) en tant que principal standard technique de communication. L'Internet déjà ubiquitaire continue de croître à un rythme rapide, non seulement en termes de nombre d'utilisateurs mais aussi en termes de services qu'il offre, notamment le protocole de la voix sur IP (VoIP), qui pourrait supplanter la téléphonie classique.

## Gouvernance

Au cours du débat sur la gouvernance de l'Internet, particulièrement dans les premiers moments du SMSI-2003, la polémique a surgi au sujet de terme 'gouvernance' et ses diverses interprétations. Selon une interprétation, gouvernance est synonyme de gouvernement. Beaucoup de délégations nationales ont eu cette première impression, menant à l'interprétation que la gouvernance de l'Internet devrait être l'affaire des gouvernements et par conséquent être traitée au niveau intergouvernemental avec la participation limitée des autres acteurs, principalement ceux non-étatiques.<sup>4</sup> Cette interprétation a contrasté avec une signification plus large du concept, qui inclut la gouvernance des affaires de toute institution, y compris celles non gouvernementales. Ce fut l'interprétation admise par les communautés de l'Internet, puisqu'elle correspond à la manière dont l'Internet a été régi depuis ses débuts.

La confusion terminologique a été encore compliquée par la traduction du terme gouvernance dans d'autres langues. En espagnol, le terme se réfère principalement aux activités publiques ou au gouvernement (*gestión pública, gestión del sector público et función de gobierno*). La référence aux activités publiques ou au gouvernement apparaît également en français (gestion des affaires publiques, efficacité de l'administration, qualité de l'administration, et mode de gouvernement). Le portugais suit le même modèle en se référant au secteur public et au gouvernement (*gestão pública and administração pública*).

## L'évolution de la gouvernance de l'Internet

### Premiers moments de la gouvernance de l'Internet (1970–1994)

L'Internet a commencé comme un projet gouvernemental. A la fin des années 1960, le gouvernement américain a sponsorisé le projet 'Defense Advanced Research Project Agency Network' (DARPA Net), un système de communication robuste. Au milieu des années 1970, avec l'invention du protocole TCP/IP (Transmission Control Protocol/Internet Protocol), ce réseau a évolué jusqu'à ce qui est aujourd'hui connu comme Internet. Un des principes clé de l'Internet est sa nature distribuée: les paquets de données peuvent prendre différents chemins à travers le réseau, évitant les barrières traditionnelles et les mécanismes de contrôle. Ce principe technologique était couplé à une approche similaire de régulation de l'Internet dans ses premiers débuts: l'Internet Engineering Task Force (IETF), mis en place en 1986, a géré le développement de l'Internet à travers un processus coopératif, basé sur

une prise de décision consensuelle impliquant une grande variété d'individus. Il n'y avait ni gouvernement central, ni planning centralisé, et encore moins de grande organisation.

Ceci a conduit beaucoup de gens à penser que l'Internet était en quelque sorte unique et qu'il pourrait apporter une alternative aux politiques du monde moderne. Dans sa fameuse déclaration sur l'indépendance du cyberspace, *John Perry Barlow* a fermement souligné que:

*[L'internet] est par nature extra-national, intrinsèquement anti-souverain et la souveraineté de vos [Etats] ne peut pas être appliquée à nous. Nous devons concevoir les choses par nous-mêmes'*<sup>5</sup>

### 'La guerre du DNS' (1994-1998)

Cette approche décentralisée de la gouvernance de l'Internet devait très bientôt commencer à changer quand les gouvernements et le secteur privé ont réalisé l'importance de ce réseau mondial.

En 1994, la 'National Science Foundation (NSF) qui s'occupait de la gestion de l'infrastructure clé de l'Internet décida de sous-traiter la gestion du système de nom de domaine (DNS) à une compagnie privée américaine appelée Network Solution, Inc., (NSI). Ceci ne fut pas bien reçu (perçu) par la communauté Internet et a conduit à ce qu'on peut appeler "la guerre du DNS".

Cette 'guerre du DNS' a fait entrer en jeu de nouveaux acteurs, en l'occurrence les organisations internationales et les Etats. Elle a pris fin en 1998 avec la création d'une nouvelle organisation: *The Internet Corporation for Assigned Names and Numbers* (ICANN). Depuis lors, le débat sur la gouvernance de l'Internet se caractérise par une implication plus prononcée des gouvernements nationaux.

### Le Sommet Mondial sur la Société de l'Information SMSI (2003-2005)

Le SMSI, tenu à Genève (2003) et Tunis (2005) a officiellement inscrit la question de la gouvernance de l'Internet dans les agendas diplomatiques. Les points à l'ordre du jour de la phase de Genève, précédée par un certain nombre de rencontres préparatoires (PrepComs) et de rencontres régionales étaient diversifiés, comportant une large gamme de sujets relatifs à l'information et à la communication mis en avant par les participants. En fait, ni le concept 'gouvernance de l'Internet', ni même le terme 'Internet' n'étaient utilisés lors des premières rencontres préparatoires et rencontres régionales.

## Le préfixe e- /virtuel/cyber/

Les préfixes e-/virtuel/cyber/numérique- sont employés pour décrire divers développements de TIC/Internet. Leur utilisation a commencé dans les années 90 et implique des influences sociales, économiques et politiques dans le développement de l'Internet. Par exemple, le 'e' du préfixe est habituellement associé au commerce électronique et à la commercialisation de l'Internet tard dans les années 90. Les universitaires et les pionniers de l'Internet utilisaient les deux termes, cyber et virtuel, pour accentuer la nouveauté de l'Internet et l'émergence d'un nouveau monde courageux. Le numérique est entré dans l'usage en premier dans les domaines techniques puis a pris de l'importance dans le contexte de la discussion sur la fracture numérique.

Sur la scène internationale, le préfixe cyber a été employé par la Convention du Conseil de l'Europe sur la cybercriminalité (2001). Plus récemment, ce préfixe a été employé pour décrire les problèmes de cybersécurité. L'UIT a désigné son initiative dans ce domaine sous le terme, 'l'agenda global sur la Cyber-sécurité'. Le mot **virtuel** apparaît rarement dans des documents internationaux. Le préfixe a recueilli une faveur particulière dans l'UE, où il décrit diverses politiques liées à l'e-science ainsi qu'à l'e-santé.

Durant le processus du SMSI, le e- était introduit durant la réunion pan-Européenne de Bucarest, et est devenu important dans tous les textes du SMSI, y compris dans les documents finaux. La mise en œuvre du SMSI est centrée sur des lignes d'action comprenant l'e-gouvernement, l'e-commerce, l'e-formation, l'e-santé, l'e-emploi, l'e-agriculture, et l'e-science.

Le terme 'gouvernance de l'internet' a été introduit dans le processus du SMSI au cours de la réunion régionale de l'Asie de l'Ouest, en février 2003, et après le Sommet de Genève, il est devenu la question clé des négociations du SMSI.

Après de longues négociations et des arrangements de dernière minute, le SMSI de Genève a décidé de la création du Groupe de Travail sur la Gouvernance de l'Internet (GTGI). Le GTGI a préparé un rapport qui a été utilisé comme base des négociations lors du deuxième sommet du SMSI tenu à Tunis (novembre 2005). L'Agenda de Tunis sur la société de l'information donna plus de détails sur la question de la gouvernance de l'Internet, y compris l'adoption d'une définition, le listing des questions liées la gouvernance de l'Internet, et l'institution du Forum sur la Gouvernance de l'Internet (FGI), un organe constitué de toutes les parties prenantes mis en place par le Secrétaire Général des Nations Unies.

## Développements en 2006

Après le sommet de Tunis qui s'est tenu en novembre 2005, trois faits majeurs ont marqué le débat sur la gouvernance de l'Internet en 2006. En premier lieu, il y a eu l'expiration du Protocole d'accord (MoU, en anglais) existant et l'établissement d'un nouvel accord entre l'ICANN et le Département du Commerce des États-Unis. Certains avaient l'espoir que cet événement changerait le rapport entre l'ICANN et le gouvernement américain, et que l'ICANN deviendrait un nouveau type d'organisation internationale. Cependant, bien que le nouveau MoU ait simplement créé un cordon ombilical 'plus mince' entre l'ICANN et le Département du commerce, ce protocole ouvre la perspective d'une éventuelle internationalisation du statut de l'ICANN.

Le deuxième événement de 2006 a été le Forum sur la gouvernance de l'Internet, tenu à Athènes. C'était le premier forum du genre, et à bien des égards, une expérimentation dans le domaine de la diplomatie multilatérale. Le forum était vraiment ouvert à toutes les parties prenantes. Tous les acteurs – États, secteur privé et société civile – ont participé sur le même pied d'égalité. Le Forum avait aussi une structure organisationnelle intéressante pour ses principaux travaux et ateliers. Les discussions ont été modérées par des journalistes et ainsi, le Forum se démarquait du style des rencontres classiques des Nations Unies. Cependant, certaines critiques ont affirmé que le forum était simplement 'une causerie' sans résultats tangibles et sans document final ni plan d'action.

Le troisième principal développement, en 2006, fut la Conférence plénipotentiaire de l'UIT tenue en Antalya (Turquie), en novembre 2006. Un nouveau Secrétaire général de l'UIT fut élu en la personne du Dr. Hamadoun TOURE. Ce dernier annonça qu'un accent particulier serait mis sur la cyber sécurité et sur l'aide au développement. Il était aussi attendu qu'il introduise de nouvelles modalités d'approche à l'égard de la gouvernance de l'Internet à l'UIT.

## Développements en 2007

En 2007, les discussions au sein de l'ICANN ont mis l'accent sur les domaines 'xxx' (domaines pour des contenus d'adultes), relançant ainsi les débats sur plusieurs points de la gouvernance, y compris la question de savoir si l'ICANN devrait traiter seulement des problèmes techniques ou s'il devrait aussi s'occuper des questions ayant trait aux politiques publiques.<sup>7</sup> Les interventions des États-Unis et d'autres gouvernements concernant les domaines xxx ont soulevé la question sur la manière dont les gouvernements

nationaux devraient s'impliquer dans les discussions de l'ICANN. Le 2<sup>ème</sup> FGI tenu en novembre 2007 à Rio de Janeiro a vu comme principale nouveauté l'inscription des ressources critiques de l'Internet comme nouveau thème dans le débat sur la gouvernance de l'Internet.

### Développements en 2008

Le principal fait de 2008, qui a influencé la gouvernance de l'Internet ainsi que d'autres sphères politiques, a été l'élection de Barack Obama comme président des États-Unis. Pendant sa campagne, il a utilisé de façon intensive les outils de l'Internet et du Web 2.0. Certains affirment même que l'une des raisons de sa brillante élection était l'usage de l'Internet. La plupart de ses conseillers venaient du secteur de l'Internet y compris le Président de Google. En plus de sa conscience technique avérée, le Président Obama soutient le multilatéralisme qui devra inévitablement influencer les discussions sur l'internationalisation de l'ICANN et le développement du régime de la gouvernance de l'Internet.

En 2008, la question de la neutralité du réseau<sup>8</sup> a émergé comme l'une des questions les plus importantes de la gouvernance de l'Internet. Elle était principalement en débat aux États-Unis entre deux principaux blocs opposés.

La question de la neutralité, défendue par le président OBAMA, figurait en bonne place dans la campagne présidentielle aux États-Unis. La neutralité du réseau est principalement soutenue par ce qu'on peut appeler l'industrie d'Internet y compris les compagnies telles que Google, Yahoo et Facebook. Un quelconque changement dans l'architecture de l'Internet pourrait compromettre leurs affaires. D'un autre côté, il y a des compagnies de télécommunications telles que Verizon, et AT&T, ainsi que des fournisseurs d'accès internet et l'industrie du multimédia. Pour diverses raisons, ces industries voudraient voir une sorte de différenciation dans la circulation des paquets sur Internet.

L'autre développement majeur a été la croissance rapide de Facebook et du réseautage social. En ce qui concerne l'Internet, l'utilisation croissante des applications du Web 2.0 a ouvert le débat sur les questions de la protection de la vie privée et la protection des données sur Facebook et des services connexes.

## Développements en 2009

La première partie de 2009 a vu naître le cercle de Washington qui essaie de (montrer) les implications de la politique du président Obama sur les questions liées à l'Internet. Les nominations faites par le président Obama à des postes liés à l'Internet n'ont pas apporté de surprises majeures. Elles ont suivi les soutiens d'Obama pour un Internet ouvert. Son équipe a également soutenu le principe de la neutralité du réseau conformément aux promesses faites pendant sa campagne.

Le fait le plus marquant de 2009 a été la conclusion de ' l'Affirmation of Commitment' entre l'ICANN et le Département américain du commerce qui devrait faire de l'ICANN une organisation plus indépendante. Tandis que ce changement résout un problème dans le processus de la gouvernance de l'Internet – la mainmise américaine sur l'ICANN – il ouvre plusieurs nouvelles questions telles que le statut international de l'ICANN ainsi que la supervision des activités de l'ICANN. 'L'Affirmation of Commitment' donne les grandes lignes directrices, mais reste muette sur plusieurs questions auxquelles il faudrait trouver des réponses dans les années à venir.

En novembre 2009, le quatrième FGI a eu lieu à Sharm el Sheikh, en Egypte. Le thème principal du Forum était l'avenir du FGI dans une perspective de révision de son mandat en 2010. Dans leurs contributions, les parties prenantes ont fait plusieurs propositions sur l'avenir du FGI. En même temps que tous défendent le maintien du FGI, les opinions divergent sur son mode d'organisation dans l'avenir. La Chine et la majorité des pays en développement ont plaidé pour un ancrage plus prononcé du FGI dans le système onusien, ce qui impliquerait un plus grand rôle des États. Les États-Unis et la majorité des pays développés, le secteur privé ainsi que la société civile ont opté pour le statu quo.

## Développements en 2010

En août 2010, les principales questions de la gouvernance de l'Internet étaient liées à l'importance croissante des plateformes des réseaux sociaux tels *Facebook* et *Twitter*. L'une des principales questions est la protection de la vie privée des utilisateurs sur ces plateformes. Dans ce qui peut être labellisé comme 'la géopolitique de l'internet', le fait marquant a été le discours de la Secrétaire d'État Hilary Clinton à propos de la liberté d'expression sur Internet, en particulier en direction de la Chine.<sup>9</sup> Google et les autorités chinoises se sont brouillés au sujet de la restriction de l'accès au moteur de recherche de Google en Chine. Ceci a conduit à l'interdiction des opérations du moteur de recherche de Google dans le pays.

Il y a eu deux autres faits majeurs du côté de l'ICANN. Le premier fait réside en l'introduction des noms de domaine non-ASCII pour l'arabe et le chinois. En résolvant le problème des noms de domaines en d'autres langues, l'ICANN a réduit le risque de la désintégration du DNS Internet. Le second fait a été l'approbation par l'ICANN du domaine .xxx (contenus pour adultes). Avec cette décision, l'ICANN a franchi le Rubicon en adoptant officiellement une décision de haute portée pour la politique publique à propos d'Internet. Auparavant, l'ICANN, ne se contentait, du moins formellement, que de prendre des décisions de nature technique.

La revue du processus du FGI qui a commencé en 2010 avec la Commission des Nations Unies pour la Science et le Développement (CSTD) qui vient de prendre la résolution de continuer l'expérience du FGI, pour les cinq années à venir, avec seulement quelques changements mineurs dans son organisation et sa structure actuelles. En juillet 2010, le Conseil Economique et Social des Nations Unies (ECOSOC) a entériné cette résolution. La décision finale sur la continuation du FGI a été prise au cours de l'Assemblée générale des Nations Unies, à l'automne 2010.

## La trousse à outils cognitive de la gouvernance de l'Internet

*Les vérités profondes sont reconnues par le fait que l'opposé est également une vérité profonde, contrairement aux trivialités où les contraires sont évidemment absurdes.*

**Niels Bohr, physicien atomique (1885-1962)**

La boîte à outils cognitive de la gouvernance de l'internet est une série d'outils pour le développement et la préparation de l'argumentaire de la politique de l'Internet. Elle a de nombreuses fonctions pratiques pour celui qui s'intéresse à la gouvernance de l'Internet. Elle aide à naviguer à travers une grande quantité d'informations, de documents, et d'études sur la gouvernance de l'internet, et aide aussi au développement de la politique théorique et à la compréhension d'autres approches politiques.

En fin de compte, cette boîte à outils améliore la qualité des négociations en augmentant les opportunités pour des solutions inclusives basées sur le compromis. Elle traite du régime évolutif de la gouvernance de l'Internet, qui en est encore à ses premières phases de son développement. L'expérience



d'autres régimes internationaux (exemple l'environnement, le transport aérien, le contrôle des armes) a montré que de tels régimes tendent d'abord à développer un cadre de référence commun, avec des valeurs, une perception des relations de cause à effets, des modes de raisonnement, une terminologie, un vocabulaire, un jargon et des abréviations. Ce cadre de référence est hautement pertinent dans la vie politique. Elle construit une façon de percevoir des questions particulières et des actions à entreprendre.

Dans beaucoup de cas, le cadre de référence commun est influencé par une culture professionnelle spécifique (les modes de connaissance et comportement partagés par les membres d'une même profession). D'habitude, l'existence d'un tel cadre aide à faciliter la communication et la compréhension.

Ceci peut aussi servir à protéger sa corporation et à se protéger de l'influence extérieure. Pour citer le linguiste Américain Jeffrey MIREL, 'Tout langage professionnel est un langage fermé'.

Le régime de la gouvernance de l'Internet est complexe car il implique beaucoup de sujets, acteurs, mécanismes, procédures et instruments. La figure ci-dessus, inspirée par l'artiste Allemand M.C. Escher démontre quelques perspectives paradoxales associées à la gouvernance de l'Internet.

La boîte à outils reflète la nature de la gouvernance de l'Internet, comme une sorte de 'vilain domaine', caractérisé par une large gamme des catalyseurs et également par la difficulté d'assigner la cause du développement d'une politique à une raison spécifique. Dans la plupart des cas, chaque problème est le symptôme d'un autre problème, créant parfois des cercles vicieux. Certaines approches cognitives, telle l'approche linéaire, mono-causale et/ou de telles façon de penser, ont une utilité très limitée dans le domaine de la gouvernance de l'Internet. La gouvernance de l'Internet est trop complexe pour être cantonnée à l'intérieur d'une sorte de concordance, de non-contradiction et d'uniformité. La flexibilité, l'ouverture et la préparation à l'éventualité de rencontrer un problème imprévu, pourrait être la meilleure expression de la gouvernance de l'Internet.<sup>10</sup>

Comme le processus de la gouvernance de l'Internet, la boîte à outils est également en perpétuel changement. Les approches, les modèles, les principes directeurs, et les analogies émergent et disparaissent selon leur pertinence par rapport au processus actuel.

## Approches et modèles

La gouvernance de l'Internet prise comme un 'tout' aussi bien que les questions spécifiques de la gouvernance de l'Internet ont fait partie des débats et d'échanges entre universitaires depuis quelque temps. Un certain nombre d'approches et de modèles ont graduellement émergé, en représentant des points communs où des différences dans les positions de négociation et également dans les cultures professionnelles et nationales peuvent être identifiées. Identifier les approches et les modèles communs pourrait réduire la complexité des négociations et aider à créer un système commun de références.

### L'approche étroite ou l'approche large

Un débat sur une approche étroite *par opposition* à une approche large de la gouvernance de l'Internet a atteint une étape cruciale, reflétant les différents intérêts et approches dans le processus.

L'approche 'étroite' met l'accent sur l'infrastructure de l'Internet (DNS, numéros IP et les serveurs racines) et sur le rôle de l'ICANN comme acteur principal dans ce domaine. Selon l'approche dite 'large', les négociations sur la gouvernance de l'Internet doivent aller au-delà des

points liés à l'infrastructure, et traiter les problèmes juridiques, économiques, socioculturels et ceux liés au développement. Cette dernière approche est adoptée dans le rapport de GTGI et dans le document final du SMSI. Cette approche est aussi utilisée comme principe directeur de l'architecture du FGI.

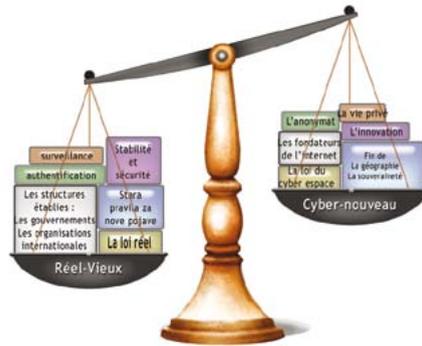
La distinction entre ces deux approches était particulièrement importante pendant les négociations du SMSI. Cependant, ce problème n'était pas complètement résolu à la fin du processus du SMSI. Les discussions tenues lors du Forum de la Gouvernance de l'Internet à Rio de Janeiro (novembre 2007) ont clairement souligné que l'approche large ne signifie pas que le discours devrait être vague. Le FGI de Rio a décidé de garder la question des ressources critiques de l'Internet (les soi-disant problèmes de l'ICANN) dans l'agenda du Forum.

### Cohérence entre aspects techniques et aspects politique

Le plus grand défi du processus de la gouvernance de l'Internet a été l'intégration des aspects politiques et techniques; car il est difficile de faire une distinction claire entre les deux. Les solutions techniques ne sont pas neutres. En fin de compte, chaque solution/option technique développe certains intérêts, avantage certains groupes, et, dans une certaine mesure, influence la vie sociale, politique et économique.

Dans le cas de l'Internet, les deux aspects, technique et politique, étaient pendant longtemps juste gérés par un groupe social, la communauté des premiers usagers de l'Internet. Avec la croissance de l'Internet et l'émergence des nouvelles parties prenantes dans les années 1990 – principalement dans le secteur privé et les gouvernements – la couverture intégrées des aspects techniques et politiques sous une même bannière de la communauté des premiers usagers de l'Internet fut perdue. Il en découla des réformes dont la création de l'ICANN, pour essayer de rétablir la cohérence des aspects techniques et politiques. Ce problème demeure ouvert, et comme prévu, il a été démontré qu'il était l'un des sujets les plus controversés lors des débats au FGI.

### Paradigme de la gouvernance de l'Internet Réel-Vieux contre Cyber-nouveau



#### L'approche 'vieux-réel' contre 'nouveau-virtuel'

Il y a deux approches à presque tous les problèmes de gouvernance de l'Internet. L'approche dite 'vieux-réel' – faisant penser au 'nouveau vin dans des veilles outres' – qui soutient que l'Internet n'a rien apporté en termes de nouveauté dans le domaine de la gouvernance. Il s'agirait juste d'un autre dispositif dans le cadre de la gouvernance. Rien n'est différent de ses prédécesseurs: le télégraphe, le téléphone ou la radio.

Par exemple, dans les discussions juridiques, cette approche argumente que les lois existantes peuvent être appliquées à l'Internet avec quelques petits réajustements. Dans le domaine, cette approche argumente qu'il n'y a aucune différence entre le commerce régulier et l'e-commerce. Par conséquent il n'y a pas besoin d'un traitement juridique spécial du e-commerce.

L'approche dite 'Nouveau-virtuel' soutient le fait que l'Internet est un système de communication fondamentalement différent de tous les précédents. Le principe fondamental de l'approche virtuelle est que l'Internet a réussi à déconnecter notre réalité sociale et politique des frontières géographiques des États souverains. Le cyberspace est différent de l'espace réel et il nécessite une forme différente de gouvernance. Dans le domaine juridique, le courant de pensée de la cyber-école argumente que les lois existantes sur la législation, la cybercriminalité et les contrats ne peuvent pas s'appliquer à l'Internet et que de nouvelles lois doivent être créées. L'approche "vieux-réel" est de plus en plus entrain de prendre le dessus dans le domaine du travail de la régulation et des politiques.

## Structure décentralisée contre structure centralisée pour la gouvernance de l'Internet

Selon le point de vue de la structure décentralisée, la structure de la gouvernance de l'Internet devrait refléter la vraie nature de l'Internet: un réseau des réseaux. Ce point de vue souligne que l'Internet est tellement complexe qu'il ne peut être placé sous le chapeau d'une structure unique telle qu'une organisation internationale, et qu'une gouvernance décentralisée est un facteur majeur qui permet la croissance rapide de l'Internet. Ce point de vue est principalement soutenu par la communauté technique de l'Internet ainsi que par les pays développés.

D'autre part, l'approche centralisée est partiellement basée sur la difficulté pratique des pays ayant des ressources financières et humaines limitées, de suivre les discussions de la gouvernance de l'Internet dans un cadre hautement multi-institutionnel et décentralisé. De tels pays n'arrivent pas à assister aux rencontres des principaux centres diplomatiques (Genève, New York), sans parler du suivi des activités d'autres institutions, telles que, l'ICANN, W3C et l'IETF. Ces pays, principalement en développement, soutiennent une 'boutique-tout-en-un' de préférence dans le cadre d'une organisation internationale.

## La protection des intérêts publics sur Internet

L'une des principales forces de l'Internet est sa nature ouverte qui a permis sa croissance rapide et favorisé la créativité et l'inclusion. La protection de la nature publique de l'Internet restera l'un des débats-clé de la gouvernance de l'Internet. Ce problème est spécialement compliqué vu qu'une partie essentielle de l'infrastructure de base de l'Internet – depuis les pivots transcontinentaux jusqu'aux réseaux locaux – est tenue par des privés. L'une des questions cruciales qui attend des réponses claires est de savoir si l'on peut demander à ces privés de garantir l'intérêt public, et quelle est la partie de l'Internet qui peut être considérée comme un bien public. Plus récemment cette question de la nature publique de l'Internet est revenue en force à travers le débat sur la neutralité du réseau.

## Géographie et Internet

L'une des caractéristiques de l'Internet est le fait que ce dernier a traversé les frontières nationales et érodé le principe de souveraineté. Avec l'Internet, les communications transcendent facilement les frontières et l'anonymat des utilisateurs est au cœur même du principe créateur de l'Internet, il semble,

pour citer la fameuse Déclaration d'indépendance du cyber-espace,<sup>11</sup> que 'les gouvernements n'ont aucun droit moral sur nous (utilisateurs)', de plus, 'ils n'ont aucune autre méthode légalement contraignante que nous pourrions avoir de bonnes raisons de redouter'.

Cependant, les développements technologiques apparus dans un passé récent intègrent pleinement des applications de géo-localisation de plus en plus sophistiquées, qui défient de plus en plus la vision de la 'fin de la géographie' à l'ère de l'Internet. Aujourd'hui, il est très difficile d'identifier avec exactitude qui est derrière un écran mais il est assez aisé d'identifier le FAI à partir duquel l'on accède à Internet.

Plus l'Internet sera intégré avec les aspects géographiques, moins son mode de gouvernance sera unique. Par exemple avec la possibilité de localiser géographiquement les utilisateurs, et les transactions, la complexe question de la juridiction sur Internet pourra être résolue à travers les lois existantes.

### Incertitude stratégique

Le débat sur la gouvernance de l'Internet est conduit dans un contexte de grande incertitude en ce qui concerne le développement technique de l'Internet. Cette incertitude a affecté l'agenda de la gouvernance de l'Internet. Par exemple, en 2002 lorsque le processus de SMSI a commencé,<sup>12</sup> Google n'était juste qu'un des nombreux moteurs de recherche. A la fin du processus, en novembre 2005, Google s'était révélé comme la première compagnie façonnant l'utilisation de l'Internet. En 2002, l'utilisation de blogs en était à ses débuts. A présent, les bloggeurs ont une emprise importante sur des gouvernements, repoussent les limites de la liberté d'expression et ont une influence considérable sur la vie économique et sociale. La liste de développements technologiques spectaculaires ayant un impact sur la gouvernance de l'Internet incluent notamment Facebook, Skype, You Tube, Twitter et Wiki.

Aujourd'hui, nombreux sont ceux qui pensent que le noyau traditionnel des problèmes de la gouvernance de l'Internet (les problèmes relatifs à l'ICANN) est entrain de perdre graduellement de sa pertinence par rapport aux questions concernant la neutralité de l'Internet, la convergence des différentes technologies (ex: la téléphonie, la télévision et l'Internet), les problèmes de gouvernance concernant les réseaux sociaux du net (Facebook et Twitter) ainsi que le rôle de Google et Wikipédia comme 'gardiens du temple' de la connaissance et de l'information numérique.

## La politique variante dans l'histoire

Avant 1875, l'Union Internationale des Télégraphes (prédécesseur de l'UIT d'aujourd'hui) a tenu une conférence à Saint-Petersbourg, réunion qui a influencée le développement futur du télégraphe. L'une des questions les plus controversées était le contrôle du contenu de la communication du télégraphe. Tandis que les participants à la conférence venant des Etats-Unis et de la Grande Bretagne faisaient la promotion du principe de l'intimité de la correspondance du télégraphe, ceux de la Russie et de l'Allemagne insistaient pour limiter cette intimité à la protection de la Sécurité de l'Etat, de l'ordre public, et de la moralité publique. Un compromis avait été trouvé par une vieille technique diplomatique – l'ambiguïté diplomatique. Tandis que l'article 2 de la Convention de Saint-Petersbourg garantissait l'intimité de communication de télégraphe, l'article 7 a limité cette intimité et a introduit la possibilité de la censure de l'Etat. Les Etats-Unis ont refusé de signer la Convention en raison de l'article sur la censure.

### Actes d'équilibrage politique

L'équilibrage est probablement l'illustration graphique la plus appropriée de la gouvernance de l'Internet et des débats sur ses politiques. Sur beaucoup de sujets de la gouvernance de l'Internet, l'on doit établir un certain équilibre entre différentes approches et intérêts. Établir cet équilibre est très souvent la base d'un compromis. Les domaines de l'équilibre politique incluent:

- La liberté d'expression contre la protection de l'ordre public: le débat bien connu entre l'article 19 (la liberté d'expression) et l'article 27 (la protection de l'ordre public) de la déclaration universelle de droits de l'homme a été étendu à l'Internet. Elle est très souvent discutée dans le contexte du contrôle du contenu et de la censure sur l'Internet.
- Cyber sécurité contre vie privé: comme la sécurité dans la vie réelle, les impératifs de la cyber sécurité peuvent mettre en danger certains droits humains comme par exemple le respect de la vie privée. L'équilibre entre la cyber sécurité et le respect de la vie privée est en perpétuel remaniement, en fonction de la situation politique mondiale. Après le 11 septembre 2001, avec l'accent mis sur les impératifs de sécurité dans l'agenda mondial, l'équilibre a plutôt penché vers la cyber sécurité.
- La propriété intellectuelle – protection des droits d'auteur des droits d'auteurs contre l'utilisation gracieuse des ouvrages: un autre "vrai" dilemme de la loi qui a pris une nouvelle envergure dans le monde numérique.

Nombreux sont ceux qui critiquent ces 'types d'équilibrage' en les considérant comme de faux dilemmes. Par exemple, il y a de forts arguments qui soutiennent que plus de cyber sécurité ne veut pas nécessairement dire

moins de protection de la vie privée. Il y a des approches qui permettent de rehausser à la fois la cyber sécurité et la protection de la vie privée. Bien que ces arguments tiennent, la réalité de la gouvernance de l'Internet est encore dominée par les options politiques 'binaires' susmentionnées.

## Principes directeurs

Les principes directeurs représentent certaines valeurs et intérêts qui sont au centre de l'émergence du régime de la gouvernance de l'Internet. Certains de ces principes ont été adoptés par le SMSI, tels que la transparence et l'inclusivité. D'autres principes ont été introduits, globalement de manière tacite, à travers les discussions sur la gouvernance de l'Internet.

### 'Ne pas réinventer la roue'

Toute initiative dans le domaine de la gouvernance de l'Internet devrait commencer à partir de lois et règlements existants, qui peuvent être divisés en trois grands groupes:

- 1 Ceux qui sont inventés pour l'Internet (ex: ICANN);
- 2 Ceux qui nécessitent un ajustement considérable dans le but d'aborder les problèmes liés à l'Internet (ex: protection de la marque, e- taxation);
- 3 Ceux qui peuvent être appliqués à Internet sans ajustements significatifs (ex: la protection de la liberté d'expression).

L'usage des règles existantes augmenterait de façon significative la stabilité juridique, et réduirait la complexité du développement du régime de la gouvernance de l'Internet.

### 'Si ce n'est pas cassé, inutile de le réparer'

La gouvernance de l'Internet doit maintenir la fonctionnalité et la robustesse actuelles de l'Internet, en même temps, elle doit rester assez flexible afin d'intégrer les importants changements qui devraient favoriser une fonctionnalité accrue et une plus grande légitimité. Un consensus général reconnaît que la stabilité et la fonctionnalité de l'Internet devraient être l'un des principes directeurs de la gouvernance de l'Internet. La stabilité de l'Internet devrait être préservée à travers l'approche primitive de l'Internet à savoir 'code évolutif' qui implique une introduction graduelle des changements bien testés dans l'infrastructure technique.

Cependant certains acteurs craignent que l'utilisation du slogan 'Si ce n'est pas cassé, inutile de le réparer' ne fournisse une immunité totale contre toute modification du régime actuel de la gouvernance de l'Internet, même pour les changements qui n'ont rien à voir avec l'infrastructure technique. Une solution serait de l'appliquer en guise de critère d'évaluation des décisions spécifiques liées à la gouvernance de l'Internet (par ex. l'introduction de nouveaux protocoles et de changements dans les mécanismes de prise de décision).



### Promotion d'une approche holistique et hiérarchisation

Une approche holistique devrait faciliter, non seulement le traitement des aspects techniques, mais également les aspects juridiques, sociaux, économiques, et développementaux de l'Internet. Cette approche devrait également prendre en considération la croissance des technologies numériques, y compris la migration des services de télécommunications vers les protocoles Internet.

Tout en maintenant une approche holistique dans les négociations sur la gouvernance d'Internet, les parties prenantes devraient identifier les questions prioritaires en fonction de leurs intérêts particuliers. Ni les pays en développement, ni les pays développés ne sont des groupes homogènes. Entre pays en développement, il existe des différences considérables en termes des priorités, de niveau de développement, et de préparation technologique (par exemple entre pays avancés dans les TIC comme l'Inde, la Chine, le Brésil, et notamment certains pays en développement d'Afrique sub-saharienne).

Une approche holistique et une priorisation au niveau de l'agenda de la gouvernance de l'Internet devraient aider les parties prenantes des pays développés et ceux des pays en développement à se centrer sur un ensemble de questions particulières. Ceci devrait mener probablement vers des négociations plus significatives et moins politisées. Les parties prenantes

se grouperaient autour des questions plutôt qu'autour des traditionnelles lignes de séparation fortement politisées (comme pays développés – en développement, gouvernements – société civile).

### Le principe de neutralité technologique

Selon le principe de neutralité technologique, des politiques ne doivent pas être conçues pour des dispositifs techniques ou technologiques spécifiques. Par exemple, les règles pour la protection de la vie privée doivent spécifier ce qui doit être protégé (par exemple des données personnelles, des dossiers de santé), et non comment elle doit être protégée (par exemple l'accès aux bases de données, la crypto-protection). L'utilisation du principe de la neutralité technologique fait de quelques instruments de la protection de la vie privée et de protection des données personnelles, telles que les lignes directrices de l'OCDE de 1980 aussi pertinentes aujourd'hui qu'elles ne l'étaient en 1980.

La neutralité technologique offre de nombreux avantages du point de vue de la gouvernance. Il assure la continuité de la gouvernance indépendamment des développements technologiques futurs et de la probable convergence des principales technologies (télécommunications, médias, Internet, etc.). La neutralité technologique est différente de la neutralité du réseau: la première indique qu'une politique particulière est indépendante de la technologie qu'elle régule, la dernière ne se concentre que sur la neutralité du trafic Internet.

### Que des solutions techniques tacites n'explicitent pas nécessairement les principes de politique

C'est un point de vue généralement partagé par la communauté de l'Internet que certaines valeurs sociales telles que la libre communication sont facilitées par la manière dont l'Internet est techniquement conçue. Par exemple, le principe de la neutralité du réseau, selon lequel le réseau devrait simplement transmettre les données entre les deux points finaux plutôt que d'introduire des intermédiaires. Ceci est souvent vécu comme une garantie pour la liberté de parole sur l'Internet. Ce point de vue pouvait conduire à une fausse conclusion que les solutions technologiques sont seules suffisantes pour promouvoir et protéger les valeurs sociales. Les derniers développements dans l'Internet, telle que l'utilisation des technologies de pare-feu pour restreindre la circulation de l'information, ont prouvé que la technologie peut être utilisée apparemment et de manière contradictoire de plusieurs façons. Chaque fois que possible, des principes tels que la liberté de communication doivent être clairement exprimés au niveau de la politique et ne pas être considérés comme sous entendus au niveau technique.

Les solutions techniques devraient renforcer les principes de politique mais ne devraient pas être les seuls moyens de les promouvoir.

### Eviter le risque que le fonctionnement de la société ne soit seulement régi à travers le code des programmeurs:

Un aspect clé du rapport entre la technologie et la politique fut identifié par *Lawrence Lessig*, qui a constaté qu'avec la dépendance croissante de l'Internet, la société moderne pourrait finir par être réglementée par un code logiciel à la place des lois. En fin de compte, certaines fonctions législatives du parlement et du gouvernement pouvaient *de facto* être prises par des compagnies d'informatiques et par des développeurs de logiciels. A travers une combinaison de logiciels et de solutions techniques, ils seraient capables d'avoir une grande influence sur la vie sociale dans les sociétés de plus en plus dépendantes de l'Internet. Si jamais une société était régie par le code numérique en lieu et place des lois, cela compromettrait pratiquement les bases de l'organisation politique et légale de la société moderne.

## Les analogies

*Bien que l'analogie soit souvent trompeuse, c'est la chose la moins trompeuse que nous ayons.*

**Samuel Butler, Poète Anglais (1835–1902)**

L'analogie nous aide à comprendre les nouveaux développements par comparaison à ce qui est déjà connu. Faire la comparaison entre le passé et les exemples courants, malgré ces risques, est l'un des processus cognitifs clé dans la loi et la politique. La plupart des affaires juridiques au sujet de l'Internet sont résolues à travers les analogies, notamment dans le système Anglo-Saxon.

L'utilisation des analogies dans la gouvernance de l'Internet a quelques limitations importantes. D'abord 'Internet' est un terme très vaste qui englobe une grande variété de services y compris le courrier électronique (voir l'analogie à la téléphonie), les services Web (voir l'analogie aux services de la radiodiffusion et télévision) et les bases des données (voir l'analogie à la bibliothèque). Une analogie à n'importe quel aspect particulier de l'Internet pourrait mener à une simplification à outrance de la compréhension de l'Internet.

Ensuite, avec la convergence croissante de différents services de télécommunication et de media, les différences traditionnelles entre eux tendent à s'estomper. Avec l'introduction de la voix sur IP par exemple, il est de plus en plus difficile de distinguer clairement l'Internet de la téléphonie.

Malgré ces facteurs de limitation, les analogies sont encore puissantes et restent toujours le principal outil cognitif pour régler les cas juridiques et développer un régime de la gouvernance de l'Internet.

### Internet-Téléphonie

*Similarités:* Au tout début de l'Internet, cette analogie était influencée par le fait que le téléphone était utilisé pour accéder à Internet. En plus, il y a une analogie fonctionnelle entre le téléphone et Internet (e-mail et discussion en ligne), les deux étant des moyens de communication directs et personnels.

*Différences:* Internet utilise les paquets en lieu et place des circuits (téléphonie). A la différence du téléphone, Internet ne peut aucunement garantir le service. Il ne peut que garantir 'le meilleur effort'. L'analogie ne souligne qu'un seul aspect de l'Internet: la communication via courrier électronique ou le clavardage. Les autres applications majeures telles que le World Wide Web, les services interactifs etc. n'ont rien à voir avec la téléphonie.

*Utilisé par:* Cette analogie est utilisée par ceux qui s'opposent à la régulation du contenu Internet (principalement aux États-Unis). Si Internet était analogue au téléphone, le contenu d'Internet ne devrait pas être contrôlé comme cela est le cas du téléphone. Cette analogie est aussi prônée par ceux qui soutiennent qu'Internet devrait être géré comme tout autre système de communication (ex: la téléphonie, la poste) par les autorités nationales avec une coordination internationale telle que l'UIT. Selon cette analogie, le DNS Internet devrait être organisé et géré comme le système de numérotation téléphonique.<sup>13</sup>

#### L'ICANN et le système postal

Paul Twomy, ancien Président de l'ICANN, a employé l'analogie suivante entre le système postal et la fonction de l'ICANN: Si vous pensez à l'Internet comme un bureau de poste ou un système postal, le nom de domaine et l'adresse IP s'assurent essentiellement que les adresses sur le devant d'une enveloppe fonctionnent. Ces adresses n'ont rien à avoir avec ce que vous mettez à l'intérieur de l'enveloppe qui envoie l'enveloppe, qui a le droit de lire l'enveloppe, combien de temps l'enveloppe prend pour arriver, quel est le prix de l'enveloppe ; aucune de ces questions n'est importante pour les fonctions de l'ICANN. La fonction de l'ICANN est de juste s'assurer que l'adresse fonctionne.

## Internet – Courrier/ services postaux

*Similarités:* Il y a une analogie fonctionnelle entre les deux notamment en ce qui concerne la livraison du courrier. Le nom même de courrier électronique souligne bien cette similarité.

*Différences:* Cette analogie ne couvre qu'un service de l'Internet: le courrier électronique. En outre les services postaux sont largement mieux élaboré du point de vue de la structure intermédiaire entre l'expéditeur et le récipiendaire par rapport au courrier électronique où le service intermédiaire est exécuté par un FAI ou fournisseur de service de courrier électronique tel que Yahoo! ou Hotmail.

*Utilisé par:* La Convention Postale Universelle établit cette analogie entre courrier simple et courrier électronique: le courrier électronique est un service postal qui utilise les télécommunications pour sa transmission. Cette analogie peut avoir des conséquences sur la délivrance des documents officiels. Par exemple recevoir une décision de justice par e-mail serait considéré comme officiel.

Les familles des soldats américains morts en Irak ont aussi essayé d'utiliser cette analogie entre courrier postal (lettre) et courrier électronique pour accéder aux messages électroniques et blogs privés de leurs bien-aimés, arguant qu'ils ont le droit d'hériter des boîtes de courrier électronique et blogs privés comme ils le feraient pour les lettres et les journaux intimes. Les FAI ont trouvé difficile de traiter un problème aussi émotionnel. Au lieu d'aller dans le sens de l'analogie 'courrier simple – courrier électronique', la plupart des FAI ont dénié l'accès en se basant sur les accords de respect de la vie privée qu'ils avaient signé avec leurs utilisateurs.

## Internet et Télévision

*Similarités:* l'analogie initiale était liée à la ressemblance entre ordinateurs et écrans de téléviseur. Une analogie beaucoup plus sophistiquée fait un lien entre l'utilisation des deux média - Web et Télévision - pour la télédiffusion.

*Différences:* Internet est un concept plus vaste que la télévision. A côté de la ressemblance des écrans, ils ont de grandes différences structurelles. La télévision est un média qui diffuse dans le sens d'un vers plusieurs téléspectateurs tandis qu'Internet permet plusieurs types de communications (un vers un, un vers plusieurs, plusieurs vers plusieurs).

*Utilisé par:* cette analogie est utilisée par ceux qui voudraient introduire un contrôle plus strict dans le contenu de l'Internet. Selon eux, avec son pouvoir de média de masse au même titre que la télévision, Internet doit être strictement contrôlé. Le gouvernement américain a essayé d'utiliser cette analogie dans la retentissante affaire de 'Reno contre ACLU'. Ce cas a été mis en lumière par le '*Communication Decency Act*' adopté par le Congrès et qui exige un strict contrôle afin de prévenir les enfants d'être exposés à la pornographie via Internet. La justice a refusé de reconnaître cette analogie.

### Internet-Bibliothèque

*Similarités:* Internet est parfois considéré comme un vaste réservoir d'informations, et le terme 'bibliothèque' lui est souvent appliqué pour le décrire: 'une grande bibliothèque numérique', 'cyber bibliothèque', 'la bibliothèque d'Alexandrie du 21<sup>ème</sup> siècle' etc.

*Différences:* le stockage des informations et des données n'est qu'un seul aspect de l'Internet. Il y a des différences considérables entre les bibliothèques et Internet:

- Les bibliothèques traditionnelles desservent des personnes vivant dans un endroit donné (ville, pays, etc.), tandis qu'Internet est mondial.
- Les livres, les articles et les journaux sont produits en tenant compte d'une exigence qualitative (les éditeurs). Internet n'en a pas toujours.
- Les bibliothèques sont organisées selon un schéma de classification spécifique qui permet aux usagers de trouver leurs ouvrages selon leurs collections. Il n'y a pas une telle classification d'information sur internet.
- En dehors de la description par mot-clé, les contenus d'une bibliothèque (textes des livres et articles) ne sont pas disponibles jusqu'à ce que l'utilisateur emprunte un livre ou un journal spécifique. Les contenus Internet sont immédiatement disponibles via les moteurs de recherche.

*Utilisée par:* cette analogie est utilisée par différents projets qui comptent créer un système détaillé d'information et de savoir sur des points bien particuliers (portails, bases de données, etc.). Récemment, cette analogie a été utilisée pour le projet de 'Google book' qui vise à numériser tous les ouvrages imprimés.

### Internet-Photocopieur, VCR

*Similarités:* cette analogie se fonde sur la reproduction et la dissémination des contenus (ex: les textes et les livres). Les ordinateurs ont simplifié la

reproduction via le procédé 'copier et coller'. Ceci, à son tour a rendu plus simple la dissémination de l'information sur Internet.

*Différences:* l'ordinateur a beaucoup plus de fonctions que la simple copie des documents, bien que copier soit beaucoup plus simple sur Internet que par un VCR ou un copieur.

*Utilisée par:* cette analogie a été utilisée dans le contexte du *Digital Millenium Copyright Act* (DMCA) des USA qui pénalise les institutions qui contribuent à enfreindre le droit d'auteur (développant des logiciels pour contourner les dispositifs de protection du droit d'auteur). Le contre-argument dans de tels cas est que les développeurs de ces logiciels, les fabricants des VCR et des copieurs ne peuvent savoir à l'avance que leurs produits seront illégalement utilisés.

Cette analogie a été utilisée contre les développeurs de logiciel de style Napster permettant un échange de fichiers entre particuliers (*P2P*) comme *Grokster* et *Steamcast*.

### Internet – Autoroute

*Similarités:* cette analogie est liée à la fascination des américains pour la découverte des nouvelles frontières. Les voies ferrées et les autoroutes font toujours partie intégrante de ce processus. L'Internet en tant que frontière dans le monde virtuel, correspond analogiquement aux autoroutes du monde réel.

*Différences:* en dehors de l'aspect transport de l'internet; il n'y a pas de similarités entre Internet et les autoroutes. L'Internet transporte des éléments immatériels tandis que les autoroutes transportent des personnes et des biens.

*Utilisée par:* l'analogie avec les autoroutes a largement été utilisée au milieu des années 1990 après qu'Al Gore ait parlé de 'super autoroutes de l'information'. Le terme autoroute a aussi été utilisé par le gouvernement allemand pour justifier l'introduction, en 1997, d'une loi introduisant un contrôle plus strict du contenu internet:

*'C'est une loi libérale qui n'a rien à voir avec la censure mais qui établit clairement ce qu'un fournisseur doit faire ou pas. Internet est un moyen de transport et de distribution du savoir...juste comme pour les autoroutes, on aura besoin de principes directeurs pour les deux modes de trafic.'*<sup>15</sup>

## Internet et les autoroutes

Hamadoun TOURE, le Secrétaire général de l'UIT, a employé une analogie entre les autoroutes et l'Internet en rapportant les autoroutes aux télécommunications et le trafic Internet aux camions ou aux voitures: *'Je donnais un exemple simple, comparant l'Internet et les télécommunications aux voitures et aux autoroutes respectivement. Ce n'est pas parce que les autoroutes vous appartiennent que tous les camions ou toutes les voitures roulant sur elles sont à vous, et certainement pas les marchandises qu'ils transportent, ou vice versa; c'est une simple analogie. Mais, afin de faire circuler très facilement votre trafic, vous devez savoir, au moment où vous construisez vos autoroutes, le poids, la hauteur et la vitesse que supporte votre structure, de sorte que vous construisiez les ponts en conséquence autrement, le système ne va pas fonctionner. Pour moi, c'est la relation entre l'Internet et le monde de télécommunications. Et, ils sont condamnés à fonctionner ensemble.'*<sup>14</sup>

### Internet-Haute mer

*Similarités:* initialement, cette analogie était dictée par le fait même qu'Internet, comme la haute mer, semble échapper à toute juridiction nationale. Aujourd'hui il est clair qu'Internet répond de certaines juridictions nationales. L'infrastructure technique via laquelle le trafic Internet est canalisé est la propriété de sociétés privées et des entreprises d'États via des opérateurs de télécommunications. La plus proche analogie avec Internet serait celle des containers transportés par des sociétés de navigation.

*Différences:* le transport maritime est régulé par un arsenal de conventions internationales qui commencent par la Convention sur le Droit de la Mer qui a des ramifications avec plusieurs traités des organismes maritimes internationaux qui traitent de la sécurité et de la protection de l'environnement. Ces conventions régulent les activités maritimes au-delà des juridictions nationales, tel qu'en haute mer. Il n'y a rien de tel dans le domaine de l'Internet et des télécommunications.

*Utilisé par:* cette analogie est utilisée par ceux qui soutiennent une régulation internationale de l'Internet. Concrètement parlant, cette analogie suggère l'utilisation et l'application du vieux concept de droit romain *'res communis omnium'* (l'espace est un héritage commun à toute l'espèce humaine et il doit être géré et régulé par toutes les nations) à l'Internet comme tel est le cas pour la haute mer.

## Classification des enjeux de la gouvernance de l'Internet

La gouvernance de l'Internet est un nouveau domaine complexe qui requiert une cartographie et une classification conceptuelles initiales. Cette complexité est liée à sa nature multidisciplinaire, englobant une variété d'aspects incluant la technologie, la socio-économie, le développement, le droit et la politique. Le besoin pratique de classification a été démontré pendant le processus du SMSI. Dans la première phase, celle qui a conduit vers le Sommet de Genève (2003), plusieurs acteurs, gouvernements inclus; ont eu du mal à circonscrire la complexité de la gouvernance de l'Internet. Une cartographie conceptuelle, fournie par plusieurs points de vue scientifiques et le rapport du GTGI, a efficacement contribué à des négociations dans le contexte du processus du SMSI. Le rapport du GTGI, en 2004, a identifié quatre centres d'intérêt majeurs:

- 1 Les enjeux en rapport à l'infrastructure et la gestion des Ressources Critiques de l'Internet;
- 2 Les enjeux relatifs à l'utilisation de l'Internet y compris les questions de pollupostage, de sécurité du réseau et de cyber criminalité;
- 3 Les enjeux important pour l'Internet mais dont l'impact est beaucoup plus étendu qu'Internet lui-même, et pour lesquels les organisations existantes sont responsables comme les questions de Droits de Propriété Intellectuelle et de commerce international;
- 4 Les enjeux liés aux aspects développementaux de la gouvernance de l'Internet, en particulier la question de renforcement des capacités dans les Pays les moins avancés (PMA).

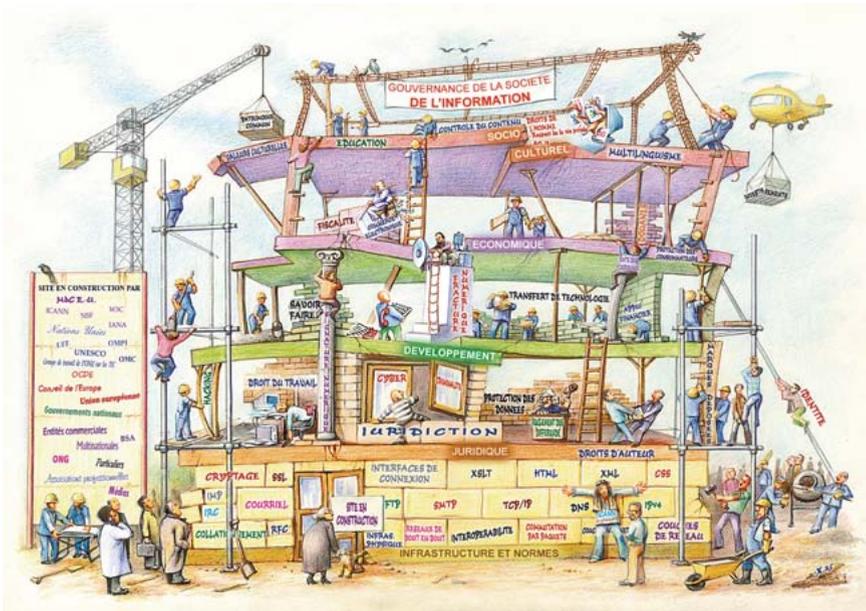
L'ordre du jour du premier FGI tenu à Athènes, en 2006, a été construit autour des thématiques suivantes:

- 1 l'accès;
- 2 la sécurité;
- 3 l'ouverture;
- 4 la diversité.

Au second FGI de Rio, en 2007, une cinquième thématique a été ajoutée à l'ordre du jour:

- 5 la gestion des ressources critiques de l'Internet.

Bien que cette classification soit changeante, la gouvernance de l'Internet traite plus ou moins du même groupe spécifique de 40 à 50 enjeux spécifiques, plus quelques enjeux disposant d'une pertinence particulière.

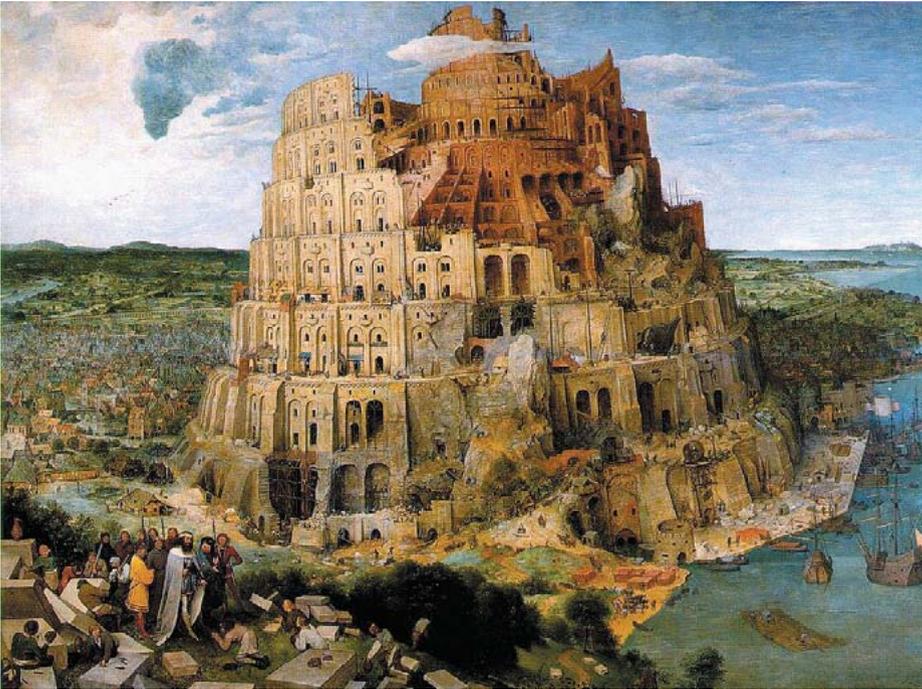


Par exemple, bien que la question du pollupostage ait figuré en bonne place dans la classification faite par le GTGI en 2004, sa pertinence a été réduite lors des réunions du FGI, durant lesquelles cette question est devenue l'un des thèmes les moins en vue dans le thème traitant de la sécurité.

La classification de Diplo des enjeux de la gouvernance de l'Internet groupe les 40-50 enjeux principaux dans les cinq paniers suivants :

- 1 Infrastructure et normalisation;
- 2 Législation (Juridique);
- 3 Économique;
- 4 Développemental;
- 5 Socioculturel.

Cette classification reflète à la fois les approches du FGI et du GTGI telles que mentionnées ci-dessus, de même que celle de la recherche académique dans le domaine. Ladite classification a été développée depuis 1997 par un ajustement constant basé sur la rétroaction des étudiants (850 étudiants jusqu'en 2010), les résultats de recherches et les expériences du processus politique. La classification des cinq corbeilles sur la gouvernance de l'Internet est présentée par la métaphore de l'image d'un bâtiment en construction (voir ci-dessus) développée par des chercheurs de Diplo.



## Un immeuble en construction: Sommes-nous entrain de construire la Tour de Babel du 21ème siècle?

Un tableau peint par Pieter Bruegel the Elder (1563), affiché au musée Kunsthistorisches à Vienne, montre la construction de la Tour de Babel (voir ci-dessus). Un autre, plus petit, peint la même année et sur le même sujet est affiché dans le musée de Boijmans Van Beuningen à Rotterdam.

Le livre de la Genèse (11.7) dans la Bible fait référence à la construction de la Tour de Babel: 'Allons ! Descendons, et semons la confusion dans leur langage, comme cela ils n'arriveront plus à comprendre les messages des uns et des autres' L'analogie avec la construction de la Tour de Babel semble appropriée lorsque l'on regarde les défis posés par l'Internet. Cette analogie nous a incités à considérer un autre bâtiment en construction – dont la finalité n'est pas de toucher le ciel mais qui vise à toucher au moins chaque individu de la planète. Diplo a développé un cadre de discussion sur la gouvernance de l'Internet illustré sur la page précédente.

Chaque étage de ce bâtiment est discuté dans les sections qui suivent. Il est important de se rendre compte que tous les étages sont liés, et que sa construction est un processus continu qui ne finit jamais.

## Notes de fin

- 1 La résolution 56/183 (21 décembre 2001) de l'Assemblée générale de l'ONU a approuvé la tenue du Sommet mondial sur la société de l'information (SMSI) en deux phases. La première phase du Sommet a eu lieu à Genève du 10 au 12 décembre 2003; et la deuxième phase a eu lieu à Tunis, du 16 au 18 novembre 2005. L'objectif de la première phase était de développer et de se focaliser sur une déclaration claire de volonté politique et de faire des pas concrets pour jeter les fondations d'une Société de l'Information pour tous, reflétant tous les intérêts de toutes les parties prenantes en jeu. Plus de 19.000 participants de 174 pays ont assisté au Sommet et aux événements y afférents. (Source: <http://www.itu.int/wsis/basic/about.html>)
- 2 La définition du GTGI suit le modèle des définitions fréquemment utilisées dans la théorie du régime. Le fondateur de la théorie du régime, Stephen D. Krasner, indique que: "*Les régimes peuvent être définis comme un ensemble de principes, de normes, de règles, et de procédures de décisions implicites ou explicites autour desquels les attentes des acteurs convergent vers un domaine donné des relations internationales. Les principes sont des croyances de faits, de causation, et de rectitude*".  
  
Les normes sont des standards de comportement définis en termes de droits et d'obligations. Les règles sont des prescriptions spécifiques ou des prescriptions à l'action. Les procédures de prises de décision sont des pratiques qui prévalent afin de mettre en place et d'appliquer un choix collectif. Krasner S (1983) *Introduction aux Régimes Internationaux*. Presse de l'Université de Cornell: Ithaca, NY, Etats-Unis.
- 3 Shannon V (2006) What's in an i? *International Herald Tribune*, 3 Décembre 2006. Disponible sur: <http://www.iht.com/articles/2006/12/03/technology/btitu.php>
- 4 La confusion terminologique a été accentuée; d'ailleurs le terme 'gouvernance' a été utilisé par quelques organisations internationales. Par exemple, le terme 'bonne gouvernance' a été employé par la Banque Mondiale pour favoriser la réforme des États en présentant plus de transparence, en réduisant la corruption, et en augmentant l'efficacité de l'administration. Dans ce contexte, le terme gouvernance est directement lié aux fonctions clés du gouvernement.
- 5 Barlow JP (1996) *A declaration of the independence of cyberspace*. Disponible sur: <https://projects.eff.org/~barlow/Declaration-Final.html>
- 6 Pour l'évolution de l'utilisation du mot 'Internet' durant la préparation du Sommet de Genève, voir: DiploFoundation (2003) *The Emerging Language of ICT Diplomacy –Keywords*. Disponible sur: <http://www.diplomacy.edu/IS/Language/html/words.htm>
- 7 En juin 2010, l'ICANN a approuvé le .xxx comme de premier niveau pour les contenus adultes.
- 8 La neutralité de réseau est un principe proposé pour permettre aux utilisateurs de réseaux membres de l'Internet d'y accéder sans restriction. Ce principe préconise qu'il n'ait aucune restriction ni par des fournisseurs d'accès Internet, ni par des gouvernements sur les contenus, sites, plateformes, et sur tous les types d'équipements qui y seraient reliés, sans restriction aucune en ce qui concerne les modes de communication permis. Le principe stipule que si un utilisateur quelconque paye pour un certain niveau de qualité d'accès à l'Internet, et qu'un autre utilisateur paye pour le même niveau de qualité d'accès ; alors les deux utilisateurs devraient pouvoir se connecter entre eux au niveau de qualité d'accès pour lequel ils ont souscrit. (Source: Wikipédia)

- 9 Disponible sur: <http://www.state.gov/secretary/rm/2010/01/135519.htm>
- 10 Cette section ne pourrait pas avoir été accomplie sans discussions avec Aldo Matteucci, membre d'honneur de Diplo, dont les points de vue à contre courant sur les questions modernes de gouvernance sont une confrontation avec la réalité constante dans les activités de l'enseignement et de recherche de Diplo.
- 11 Barlow (1996) *op. cit.*
- 12 Le processus du SMSI a commencé avec la première réunion préparatoire tenue en juillet 2002 à Genève. Le premier sommet a eu lieu à Genève (décembre 2003) et le deuxième en Tunisie (en Novembre, 2005).
- 13 Volker Kitz argumente en faveur d'une analogie entre la gouvernance du système téléphonique et les noms et numéros Internet. Kitz V. (2004) '*ICANN may be the only game in town, but Marina del Rey isn't the only town on Earth: Some thoughts on the so-called 'uniqueness' of the Internet*'. (L'ICANN serait l'unique jeu en ville, mais Marina del Rey n'est pas l'unique ville sur Terre: Quelques pensées sur ce que l'on appelle 'originalité' de l'Internet).  
  
Disponible sur: <http://smu.edu/stlr/articles/2004/Winter/Kitz.pdf>
- 14 Extrait du discours du Secrétaire général (de l'UIT), discours donné à la réunion de l'ICANN au Caire (6 novembre 2008). Disponible sur: <https://cai.icann.org/.les/meetings/cairo2008/tourespeech-06nov08.txt>
- 15 Cité dans Mock K, Armony L (1998), *Hate on the Internet*. Disponible sur: [http://www.media-awareness.ca/english/resources/articles/online\\_hate/hate\\_on\\_internet.cfm](http://www.media-awareness.ca/english/resources/articles/online_hate/hate_on_internet.cfm)
- 16 Le terme 'corbeille' a été introduit dans la pratique diplomatique lors des négociations de l'Organisation sur la Sécurité et la Coopération en Europe (OSCE).

## Section 2

---

# La corbeille infrastructure et normalisation

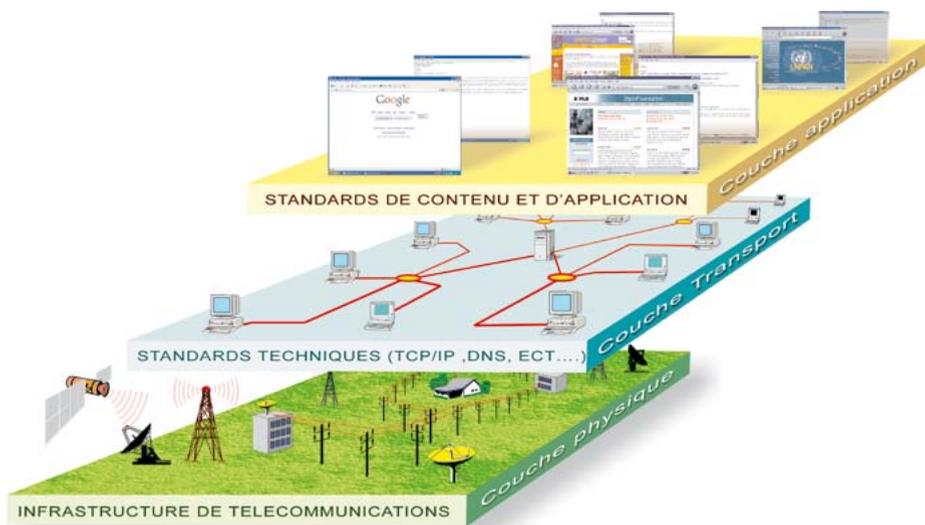




# La corbeille infrastructure et normalisation

La corbeille de l'infrastructure et de la normalisation contient les enjeux élémentaires, essentiellement techniques, liés au fonctionnement de l'Internet. Le principal critère pour placer un enjeu dans cette corbeille est sa pertinence dans le fonctionnement de base de l'Internet. Il ya ici deux groupes d'enjeux.

Le premier groupe se compose des questions essentielles sans lesquelles l'Internet et le World Wide Web ne pourraient pas exister<sup>1</sup>. Ces questions sont regroupées en trois couches:



- 1 l'infrastructure des télécommunications, à travers laquelle circule tout le trafic Internet ;
- 2 les normes (standards) et services techniques de l'Internet, l'infrastructure qui fait fonctionner l'Internet (par exemple TCP/IP: *Transmission Control Protocol/Internet Protocol*; DNS: *Domain Name Services*; SSL: *Secure Sockets Layer*).
- 3 les contenus et les normes régissant les applications (par exemple HTML: *HyperText Markup Language*, XML: *eXtensible Markup Language*).

Le second groupe comprend les questions relatives à la sauvegarde de la sécurité et de la stabilité opérationnelle de l'infrastructure de l'Internet et inclut la cyber sécurité, le cryptage et le pollupostage.

## Les infrastructures de télécommunications

### La situation actuelle

Les données Internet peuvent circuler sur une gamme variée de supports de communication: câble téléphoniques de cuivre, câbles à fibres optiques, satellites, micro-ondes, et des liaisons sans fil. Même le réseau électrique de base peut être utilisé pour relayer le trafic Internet en utilisant la technologie du courant porteur en ligne<sup>2</sup>.

Tenant compte du fait que la couche des télécommunications assure le trafic Internet, toute nouvelle réglementation liée aux télécommunications aura inévitablement un impact sur l'Internet. L'infrastructure de télécommunications est réglementée au niveau national et au niveau international par une variété d'organisations publiques et privées. Parmi les organisations internationales clés impliquées dans la régulation des télécommunications, il y a l'Union internationale des télécommunications (UIT), qui a développé et des règles détaillées pour gérer la relation entre opérateurs nationaux, l'allocation du spectre radio, et la gestion du

### La régulation internationale de l'UIT

La régulation internationale de l'IUT (ITR) de 1998 a facilité la libéralisation internationale de la tarification et des services et a permis une plus grande créativité dans l'usage des services au niveau de l'internet, tel que l'utilisation de lignes internationales louées dans le domaine de l'Internet. Elle a fourni l'une des bases palpable pour la croissance rapide de l'Internet dans les années 1990.

positionnement des satellites; et l'Organisation Mondiale du Commerce (OMC), qui a joué un rôle capital dans la libéralisation des marchés des télécommunications à travers le monde<sup>3</sup>.

Les rôles de l'OMC et l'UIT sont tout à fait différents. L'UIT définit des normes techniques détaillées non contraignantes, les réglementations internationales spécifiques des télécommunications, et fournit une assistance aux pays en développement. L'OMC en revanche offre un cadre pour les règles générales du marché<sup>4</sup>.

La libéralisation des marchés nationaux des télécommunications a donné aux grands groupes de télécommunications telles qu'AT & T, Câble and Wireless, France Telecom, Sprint, et WorldCom, l'opportunité d'étendre leur marché à l'échelle mondiale. Comme une grande partie du trafic Internet est transportée via les infrastructures de télécommunication de ces sociétés, ces dernières ont une influence importante sur le développement de l'Internet.

## Les enjeux

### Le 'dernier kilomètre' – 'la boucle locale'

La 'boucle locale' (ou 'dernier kilomètre') est le nom donné au lien de connexion existant entre les Fournisseurs d'accès Internet (FAI) et leur clients finaux. Les problèmes avec les 'boucles locales' résident dans le fait qu'elles constituent un obstacle à une utilisation plus répandue de l'Internet dans de nombreux pays, particulièrement ceux en développement. La communication sans fils est l'une des solutions peu coûteuse au problème de la boucle locale. En dehors des options techniques de plus en plus accessibles, la solution au problème de la 'boucle locale' dépend également de la libéralisation de ce segment du marché des télécommunications.

### La libéralisation des marchés des télécommunications

Un nombre considérable de pays ont libéralisé leurs marchés des télécommunications. Cependant, beaucoup de pays en développement sont confrontés à un choix difficile: libéraliser et rendre le marché des télécommunications plus efficace, ou préserver une importante source de revenus budgétaires des monopoles de télécommunications existants<sup>5</sup>. L'assistance étrangère, la transition progressive, et le fait de lier le processus de libéralisation à la protection de l'intérêt public pourraient être des voies de sorti de ce dilemme.

### La création de normes techniques d'infrastructure

Les normes techniques sont de plus en plus fixées par les institutions privées et professionnelles. Par exemple, la norme WiFi, IEEE 802.11b, a été développée par 'the Institute of Electric and Electronic Engineers' (IEEE). La certification des équipements WiFi compatibles est faite par l'Alliance WiFi. La fonction même de la création ou de la mise en œuvre des normes dans un marché qui se développe rapidement confère une influence considérable à ces institutions.

## Le 'Transport Control Protocol/ Internet Protocol' (TCP/IP)

### La situation actuelle

Le TCP/IP est la norme technique principale de l'Internet, précisant comment les données sont transférées par Internet, il est basé sur trois principes: commutation des paquets, la mise en réseau de bout en bout et la robustesse. La gouvernance de l'Internet en rapport avec le protocole TCP/IP a deux aspects importants: l'introduction de nouvelles normes et l'attribution des adresses IP.

Les normes TCP/IP sont fixées par l'Internet Engineering Task Force (IETF). Etant donné la pertinence de ces protocoles pour l'Internet, ces derniers sont soigneusement gardés par l'IETF. Toute modification du protocole TCP/IP requiert au préalable une grande discussion et la preuve que la solution en question soit réellement efficace (principe du 'code fonctionnel').

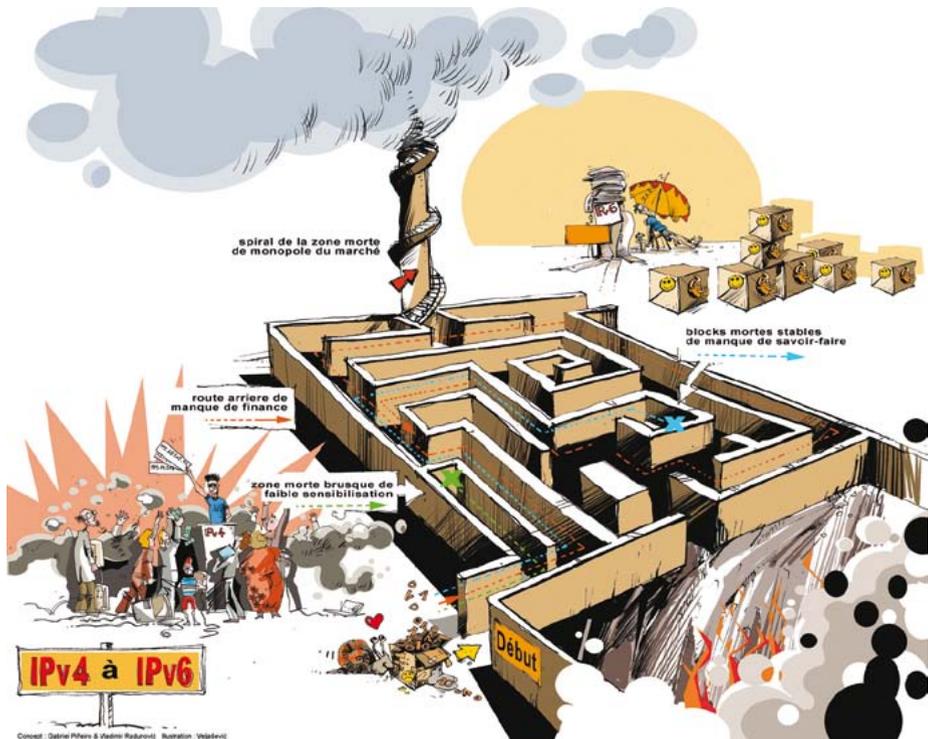
Les adresses IP sont des adresses numériques que tout ordinateur connecté à Internet doit avoir. Les adresses IP sont uniques, deux ordinateurs connectés à l'Internet ne peuvent pas avoir la même adresse IP. Cela fait des adresses IP une ressource potentiellement rare. Le système d'attribution des adresses IP est hiérarchiquement organisé. Au sommet, il y a l'Internet Assigned Numbers Authority (IANA) – une filiale de l'ICANN, qui distribue des blocs d'adresses IP aux cinq Registres internet régionaux (*RIR*)<sup>6</sup>. Les RIR distribuent les adresses IP aux Registres Internet Locaux (Local Internet Registries-LIR) et dans les Registres Internet Nationaux (National Internet Registries-NIRS), qui à leur tour, distribuent les adresses IP aux petits fournisseurs de services Internet, aux entreprises et aux individus au plus bas de l'échelle.

## Les enjeux

### Comment faire face au nombre limité d'adresses IP (Transition vers IPv6)

Le pool actuel des adresses IP sous la forme IPv4 (Internet Protocol, version 4) contient quelque quatre milliards d'adresses et pourrait arriver à épuisement dans quelques années face à l'introduction de gadgets/terminaux-Internet, tels que les téléphones mobiles, les organisateurs personnels, les consoles de jeu, et les appareils ménagers. La préoccupation liée au fait que les adresses IP risqueraient de s'épuiser et inhiberait éventuellement le développement de l'Internet a conduit la communauté technique à prendre les mesures suivantes:

- Rationaliser l'utilisation du pool existant d'adresses IP par le biais de l'introduction du Network Address Translation (NAT);
- Répondre au gaspillage des algorithmes d'attribution d'adresses utilisés par le RIR, en introduisant le routage inter-domaines sans classe (*Classless Inter-Domain Routing*: CIDR);
- Introduire une nouvelle version du protocole TCP/IP – IPv6 – qui prévoit un nombre beaucoup plus élevé d'adresses IP (340,000,000,000,000,000).



Concept : Daniel Pflanz & Dennis Reuter / Illustration : Vajević

La réponse de la communauté Internet au problème du risque de pénurie d'adresses IP est un exemple de gestion rapide et proactive. Bien que le NAT et le CIDR aient fourni une solution rapide au problème, une solution à long terme est la transition vers l'IPv6.

Bien qu'introduit en 1996, le déploiement d'IPv6 a été très lent. Avec l'épuisement prochain du pool d'adresses de l'IPv4 en 2011, la lenteur du déploiement de l'IPv6 renforce les éléments d'une crise en gestation. L'un des principaux défis à relever pour le déploiement de l'IPv6 est le manque de compatibilité entre l'IPv4 et l'IPv6. Les réseaux utilisant l'IPv6 ne peuvent pas communiquer directement avec ceux qui, encore en nombre dominant aujourd'hui, utilisent l'IPv4. Comme il est très probable que les réseaux utilisant l'IPv4 et l'IPv6 coexistent à l'avenir, il est important de s'assurer que les nouveaux réseaux – basés sur l'IPv6 – ne restent pas isolés. Une solution technique comprendra un tunnel spécial entre les deux types de réseaux, ce qui entraînera un routage plus complexe sur l'Internet et quelques autres problèmes 'collatéraux'.

Le déploiement est également retardé par le faible intérêt de la part des Fournisseurs d'accès Internet (FAI) et des utilisateurs. Bien qu'ils soient conscients du risque d'épuisement d'adresses IP, ils préfèrent la tactique de 'attendre et voir'. Par exemple, une enquête récente au Japon a montré que si plus de 70% des FAI sont conscients du risque d'épuisement de l'IPv4, seulement 30% d'entre eux se préparent à la transition vers l'IPv6. Dans une telle situation, lorsque la motivation du marché ne peut pas fournir de solution, il y a une pression croissante sur les gouvernements et les autres autorités publiques pour qu'ils jouent un rôle de premier plan dans le pilotage de la transition vers l'IPv6 à travers la sensibilisation sur les risques d'épuisement d'adresses IPv4, et dans le soutien financier pour la transition vers IPv6 et l'utilisation d'IPv6 pour les réseaux des gouvernements.

Étant donné la complexité de la transition vers IPv6, les pays en développement, essentiellement les pays d'Afrique, pourraient être avantagés par le retard pris dans l'acquisition des réseaux et de la possibilité de l'introduction directe des réseaux basés sur IPv6. Dans ce processus, les pays en développement vont avoir besoin d'une assistance technique<sup>7</sup>.

Outre le problème de la transition, le cadre politique pour l'attribution de l'IPv6 a besoin d'une bonne répartition d'adresses IP, exigeant ainsi l'introduction de mécanismes ouverts et concurrentiels de façon à répondre de la manière la plus optimale aux besoins des utilisateurs finaux.

### Les changements dans le protocole TCP/IP et la cybersécurité

À l'origine, la sécurité n'était pas un enjeu majeur pour les développeurs de l'Internet puisqu'à cette époque l'Internet n'était qu'un réseau fermé d'institutions de recherche. Avec l'expansion de l'Internet à plus de deux milliards d'utilisateurs dans le monde et de son importance croissante comme outil commercial, la question de la sécurité fut placée au devant de la scène des problèmes de gouvernance de l'Internet.

Étant donné que l'architecture de l'Internet n'a pas été conçue en ayant à l'esprit la sécurité, incorporer la cyber sécurité de façon intrinsèque nécessite d'apporter des changements substantiels au fondement même de l'Internet, c'est-à-dire au protocole TCP/IP. Le nouveau protocole IPv6 offre certaines améliorations de sécurité, mais ceci reste en deçà d'une solution globale. Cette protection va demander des modifications considérables sur le TCP/IP.<sup>8</sup>

### Les changements dans le protocole TCP/IP et le problème de la bande passante limitée

Afin de faciliter la fourniture de contenus multimédia (par exemple la téléphonie sur Internet, ou vidéo à la demande), il est nécessaire de garantir une qualité de service (Quality of Service – QoS) capable de garantir un niveau minimal de performance. La QoS est particulièrement importante pour les applications sensibles aux délais (temps de réponse), telle que la diffusion d'événements en direct; et il est souvent difficile de la réaliser en raison des contraintes de la bande passante. L'introduction de la QoS peut nécessiter des changements dans le protocole Internet, sans écartier un risque potentiel pour le principe de la neutralité du réseau.

## Le système des noms de domaine (DNS)

### La situation actuelle

Le DNS gère les adresses Internet (telle que [www.google.com](http://www.google.com)) et les convertit en adresses IP (une illustration simplifiée de ce processus est présenté dans le dessin qui suit). Le DNS est constitué de serveurs racine, serveurs de premier niveau (Top-Level Domain – TLD) et un grand nombre de serveurs DNS sont placés à travers le monde. La gestion du DNS a été un des sujets brûlants dans le débat sur la gouvernance de l'internet. L'une des principales controverses concerne l'autorité du gouvernement des États-Unis (via le ministère du Commerce, Department of Commerce – DOC) sur les serveurs racine, le niveau supérieur hiérarchiquement organisé du système du

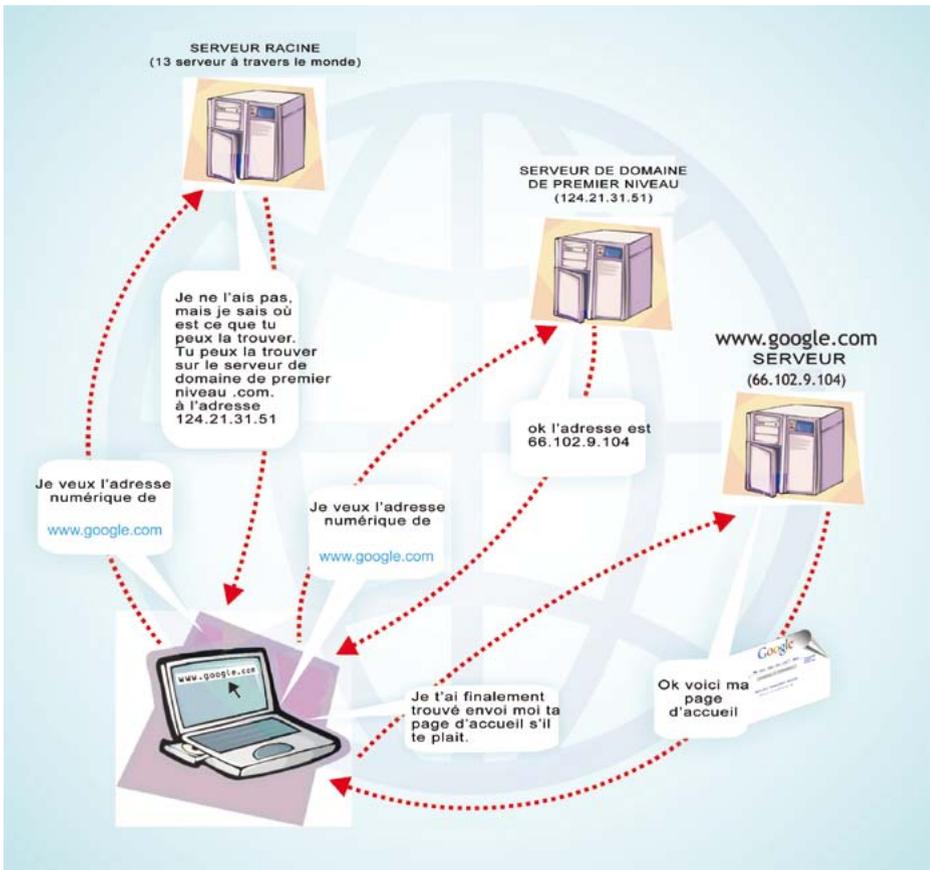
## Technologie, standards, politiques

Le débat sur les protocoles réseau illustre comment les normes peuvent être considérées comme des politiques en ayant une autre perspective. En considérant que l'intervention gouvernementale dans la technologie et les affaires (telle que la régulation de la sécurité et les actions anti-trust) est aisément considérée comme ayant une signification politique et sociale; les normes techniques sont généralement reconnues comme socialement neutres et donc jouissant d'un intérêt historique très faible. Mais les décisions techniques peuvent avoir des conséquences économiques et sociales de grande envergure, changeant l'équilibre des forces entre les entreprises ou les nations en concurrence et rendant contraignante la liberté des utilisateurs. Des efforts pour créer des normes formelles poussent à des décisions techniques privées des constructeurs de systèmes dans le domaine public; de cette façon, les batailles de normes peuvent mettre en lumière des acceptations tacites et des conflits d'intérêt. La grande passion avec laquelle les parties prenantes contestent des décisions sur les normes devrait nous alerter quant à la signification plus profonde sous les écrous et les boulons.<sup>9</sup>

nom de domaine. La situation s'est encore aggravée par le fait que 10 des 13 serveurs racine existants sont aux États-Unis (avec trois autres en Europe et en Asie). Pour résoudre ce problème et améliorer l'évolutivité du système de serveurs racine, le 'régime *Anycast*' a été élaboré, en incluant désormais une centaine de serveurs dans le monde entier et dans tous les continents.

Le DNS est fondé sur trois types de domaines de premier niveau: générique (gTLD), codes pays (ccTLD), et sponsorisés (sTLD). Les gTLD sont des domaines que n'importe qui peut obtenir (.com., .info, .net et .org). Les sTLD sont limités à des groupes spécifiques. Par exemple, les sTLD '.aero' n'ont pas été ouverts à l'enregistrement que pour l'industrie du transport aérien. Les ccTLD sont réservés à des pays spécifiques (.uk, .cn, .in).

Pour chaque domaine générique de premier niveau (gTLD) Il y a un registre qui maintient une liste d'adresses. Par exemple, le gTLD '.com' est géré par VeriSign. La fonction de 'vendeur' est assurée par les registraires. L'ICANN assure la coordination globale du système DNS en concluant des accords avec des registres d'accréditation et d'enregistrement. L'ICANN définit également les prix de gros auxquels le registre (VeriSign) 'loue' les noms de domaine aux bureaux d'enregistrement, et impose des conditions sur les services offerts par le registre ainsi qu'aux structures travaillant avec ce dernier. C'est pour dire que l'ICANN agit en tant que régulateur économique et juridique du *business* des noms de domaine pour les gTLD.



Une partie importante de la gestion du système des noms de domaine est la protection des marques et le règlement des différends. Le principe du 'premier arrivé, premier servi' dans l'attribution des noms de domaine a été utilisé dès les premiers jours où l'Internet a vu se déclencher le phénomène connu sous le nom de *cyber-squatting*, la pratique d'enregistrer des noms de domaine qui sont revendus par la suite. Les politiques uniformes de règlement des litiges *Uniform Disputes Resolution Policy (UDRP)*, développées par l'ICANN et l'Organisation Mondiale de la Propriété Intellectuelle (OMPI) prévoient des mécanismes qui ont considérablement réduit le *cyber-squatting*.

Un autre élément important dans l'enquête sur l'organisation actuelle de la gouvernance du système DNS est la gestion des codes de pays de niveau supérieur (*Top-Level Domains*) (ccTLD). Actuellement, certains codes de pays sont encore gérés par une variété d'institutions ou des personnes qui ont reçu l'accréditation dans les tous premiers jours de l'Internet, lorsque certains gouvernements n'étaient pas tous intéressés à la question.

## Les problèmes

### La création des nouveaux domaines génériques

Techniquement, la création de nouveaux domaines de premier niveau est presque illimitée. Cependant, l'introduction de nouveaux domaines génériques de premier niveau (gTLD) a été très lente, avec un certain nombre de nouveaux TLD génériques introduits que récemment. Actuellement, 20 gTLD sont actifs et trois autres sont à l'étude.<sup>10</sup> La principale opposition à la création de nouveaux TLD génériques provient du secteur privé, dont le souci est que l'augmentation du nombre de domaines compliquerait la protection de leurs marques.

Sous la pression d'introduire de nouveaux gTLD, l'ICANN a entamé des consultations pour concevoir une nouvelle politique dans ce domaine. La nouvelle politique devrait traiter de la manière de résoudre les demandes concurrentes pour les gTLDs, les questions de moralité publique, et les frais d'inscription, entre autres.

### Les contenus en relation avec des noms de domaine génériques

Une autre question politique de l'ICANN est de décider de la création de nouveaux domaines, qui pourrait s'impliquer à relier les noms de domaines aux contenus<sup>11</sup>. Le dernier exemple en date a été la proposition d'introduire le domaine 'xxx' pour les sites web pornographiques. Le conseil d'administration de l'ICANN a rejeté cette proposition en mars 2007. La principale critique de cette décision a été que l'ICANN l'avait fait sous la pression du gouvernement américain, qui est fermement opposé à l'introduction du domaine 'xxx'<sup>12</sup>. Ce qui est intéressant, c'est que de nombreux autres gouvernements ont soutenu le gouvernement des États-Unis, y compris ceux qui sont généralement critiques de la position américaine en matière de gouvernance de l'Internet, comme le Brésil et la Chine. Cette question est revenue à l'ordre du jour en juin 2010 lors de la réunion de l'ICANN à Bruxelles où le Comité directeur de l'ICANN a positivement accepté la candidature pour le domaine .xxx et initia des négociations pour son introduction.

La décision prise par l'ICANN sur le cas 'xxx' a également rouvert le débat sur le rôle de l'ICANN sur les questions de politiques publiques.

### Les noms de domaine génériques pour les communautés culturelles et linguistiques

En 2003, l'ICANN a introduit un nouveau domaine '.cat' pour la langue catalane. Ceci est le premier domaine introduit pour une langue<sup>13</sup>. Le gouvernement espagnol ne s'était pas opposé à cette décision.

Lorsque ce problème de '.cat' a été évoqué, il a déclenché beaucoup d'inquiétudes, de sorte que cela pourrait constituer une espèce d'alibi pour d'autres langues, ou même amener plus de controverses au sein des communautés linguistiques et culturelles qui peuvent avoir des revendications à tendance nationalistes. Avec un regard rétrospectif, nous voyons que ceci ne s'est pas produit.

### La gestion des noms de domaines nationaux

La gestion des domaines de premier niveau pour les pays comprend trois questions importantes. La première concerne la décision souvent politiquement controversées de savoir exactement quel code appliquer à des pays ainsi qu'à des entités ayant un statut international non clarifié ou contesté (par exemple, les pays nouvellement indépendants et les mouvements de résistance). Une récente question controversée a été l'attribution d'un nom de domaine à l'Autorité palestinienne. En justifiant sa décision de céder le domaine de premier niveau '.ps', l'Internet Assigned Numbers Authority (IANA) a réaffirmé le principe de l'attribution des noms de domaine en conformité avec la norme ISO 3166, comme cela a été proposé par Jon Postel, l'un des pères fondateurs de l'Internet.<sup>14</sup>

Le deuxième problème concerne l'entité devant gérer les codes de pays. De nombreux pays ont essayé de prendre le contrôle de ces noms de domaines, qui sont considérés comme des ressources nationales. Les gouvernements nationaux ont choisi une grande variété d'approches stratégiques.<sup>15</sup> La transition ('re-délégation') vers une nouvelle institution qui se chargerait de gérer le ccTLD ('délégué') au sein de chaque pays est approuvée par l'ICANN si et seulement s'il existe un consensus de toutes les parties prenantes dans le pays. Étant donné l'importance de ce problème et la grande variété d'approches, il ya eu deux initiatives importantes au niveau international pour introduire un certain degré d'harmonisation. La première a été les 'principes du GAC', adoptés par le Comité Consultatif Gouvernemental de l'ICANN (CCG), qui propose des politiques et spécifie les procédures pour la re-délégation de l'administration des ccTLD.<sup>16</sup> La seconde constitue 'les meilleures pratiques', proposé par le *World Wide Alliance of Top Level Domains* (Juin 2001).

Le troisième problème est lié à la réticence des opérateurs de nombreux domaines de pays à devenir partie intégrante du système de l'ICANN. Jusqu'à présent, l'ICANN n'a pas réussi à rassembler les opérateurs des domaines des pays sous son égide. Les opérateurs des domaines de pays sont organisés au niveau régional (Europe – CENTR, l'Afrique – AFTLD, Asie – APTLD, Amérique du Nord – NATLD, l'Amérique du Sud – LACTLD). Au niveau

mondial, le principal forum est le *World Wide Alliance of Top level Domains*. L'ICANN est entrain de développer un 'Cadre de responsabilisation', comme une manière moins formelle d'établir des liens avec les opérateurs des domaines des pays.

### Les noms de domaine internationalisés

L'Internet a été initialement développé comme medium, et essentiellement en anglais. Grâce à une croissance rapide, l'Internet est devenu un outil de communication globale avec un nombre croissant d'utilisateurs non-anglophones. Pendant une longue période, le manque de fonctionnalités multilingues dans l'infrastructure d'Internet fut l'une des principales limites de son développement. En mai 2010, après une longue période d'essai et d'incertitudes politiques, l'ICANN commença à approuver de nouveaux noms de domaine en une large variété de scripts, incluant le Chinois, l'Arabe et le Cyrillique. L'introduction de noms de domaine internationalisés (Internationalized Domain Names – IDN) est considéré comme l'un des succès majeur du régime de la Gouvernance de l'Internet.

### Les serveurs racines

Au sommet de la structure hiérarchique du système des noms de domaine, les serveurs racine attirent beaucoup d'attention. Ils font partie de la plupart des débats politiques et académiques sur les problèmes de gouvernance de l'Internet.

### La situation actuelle

Le fonctionnement et la robustesse du DNS peuvent être illustrés par l'analyse du fait que l'Internet peut s'effondrer si jamais les serveurs racines étaient désactivés. Premièrement, il existe 13 serveurs racines distribués à travers le monde (10 aux Etats-Unis, un en Suède, un aux Pays Bas et un au Japon; des 10 aux Etats-Unis, plusieurs sont exploités par des organismes gouvernementaux américains), 13 étant le nombre maximal techniquement possible. Si un des serveurs tombe en panne, les 12 restants continueraient à fonctionner. Même si tous les 13 serveurs racines tombent en panne en même temps, la résolution de nom de domaine (la fonction principale de serveurs racines) se poursuivrait sur les autres serveurs de noms de domaines, réparties hiérarchiquement sur Internet<sup>17</sup>.

Par conséquent, des milliers de serveurs de noms de domaines contiennent des copies du fichier de la zone racine, et un effondrement immédiat et

catastrophique de l'Internet n'est pas envisageable. Il faudrait un certain temps avant que de graves conséquences fonctionnelles soient remarquées, temps pendant lequel il serait déjà possible de réactiver les serveurs d'origine ou d'en créer des nouveaux.

En outre, le système de serveurs racines s'est considérablement renforcé par le régime 'Anycast', qui reproduit des serveurs racines dans le monde entier. Ceci offre de nombreux avantages, notamment une robustesse accrue dans le système DNS et une résolution plus rapide des adresses Internet (avec le régime *Anycast*, les serveurs qui font des résolutions sont plus proches des utilisateurs finaux).

Les 13 serveurs racines sont gérés par une diversité d'organisations: institutions universitaires / institutions publiques, les sociétés commerciales et des institutions gouvernementales. Les institutions gérant des serveurs racines reçoivent un fichier de zone racine proposé par l'IANA (ICANN) et approuvé par le gouvernement des États-Unis (Département du commerce, *Department of Commerce – DoC*). Une fois que le contenu est approuvé par le Département du commerce, il entre dans le serveur racine principal géré par VeriSign sous contrat avec le Département.

Le fichier dans le serveur racine principal est automatiquement répliqué dans tous les autres serveurs racines. Ainsi, il est théoriquement possible pour le gouvernement des États-Unis d'introduire des changements unilatéraux à l'ensemble des DNS. C'est une source de préoccupation pour de nombreux gouvernements.

## Les problèmes

### L'internationalisation du contrôle des serveurs racines

Plusieurs pays ont exprimé leur préoccupation au sujet de la disposition actuelle par laquelle l'ultime décision concernant le contenu des serveurs racine demeure la responsabilité d'un pays (les États-Unis). Dans les négociations sur la gouvernance de l'internet, il y a eu des propositions diverses, y compris l'adoption d'une 'Root Convention', qui confierait à la communauté internationale la charge de surveiller la politique des serveurs racines ou, au moins des droits aux États sur la gestion de leurs propres noms de domaine nationaux. De nouvelles possibilités ont été ouvertes avec l'Affirmation of Commitments<sup>18</sup>, qui traite de la question de l'indépendance institutionnelle de l'ICANN vis à vis du Département du Commerce des États-Unis, y compris l'internationalisation à venir de l'ICANN. Le statut de

l'IANA sera renégocié en 2011. Quelques éléments pour la mise en place de solutions pratiques devraient se faire en deux étapes:

- 1 la réforme de l'ICANN, initiée par l'Affirmation of Commitments', conduisant à la création d'une organisation internationale *sui generis*, qui serait un cadre institutionnel acceptable pour tous les pays.
- 2 le transfert du contrôle des serveurs racines du Département américain du commerce à l'ICANN, comme cela a été initialement prévu.

### Serveurs racines alternatifs- faisabilité et risques

La mise en place d'un serveur racine alternatif est techniquement simple. La principale question est de savoir combien d'adeptes' un serveur alternatif pourrait avoir, ou, plus précisément, quel est le nombre d'ordinateurs sur Internet qui y pointeraient, au moment de la résolution des noms de domaine. Sans utilisateurs, tout DNS alternatif devient inutile. Quelques tentatives pour créer un DNS alternatif ont été réalisées: *Open NIC*, *New.net*, et *Name.space*. La plupart d'entre elles ont été infructueuses, ne comptant qu'un pourcentage négligeables d'utilisateurs.

### Le rôle des États-Unis dans la gestion des serveurs racines – Le paradoxe de la puissance

Depuis l'adoption de l'Affirmation of Commitment', la question du paradoxe de la puissance américaine sur les serveurs racines pouvait progressivement appartenir au passé. Le pouvoir potentiel de retirer un pays de l'Internet (par la suppression de son nom de domaine) peut difficilement être qualifié d'acte de puissance, puisqu'il n'a pas d'utilité effective. L'élément-clé dans l'exercice du pouvoir est de forcer l'autre à agir dans le sens voulu par le détenteur du pouvoir. L'utilisation du 'pouvoir' des États-Unis sur l'infrastructure de l'Internet pourrait générer des effets inattendus, y compris que des pays et des régions aillent jusqu'à établir leur propre 'internet'. Dans un tel scénario, l'Internet pourrait se désintégrer et les intérêts des États-Unis viendraient à disparaître (la prédominance des valeurs des États-Unis sur l'Internet, l'anglais comme langue franche de l'internet, la prédominance des sociétés américaines dans le domaine du e-commerce). Sur la base de ses premières initiatives politiques dans la gouvernance de l'internet (par exemple, l'Affirmation of Commitment), il semble que l'administration Obama soit consciente du paradoxe de puissance. Cela constitue un signe prometteur quant à l'évolution future du régime de la gouvernance de l'Internet au niveau mondial.

## **La neutralité du réseau**<sup>19</sup>

Que se serait-il produit si la concurrence avait limité l'accès à Google à ses débuts? Ou si les opérateurs de télécommunication avaient ralenti l'introduction de la téléphonie d'internet à Skype? Ou si le gouvernement des Etats-Unis avait restreint l'accès à l'Internet dans les pays ennemis?<sup>20</sup> Nous aurions très probablement eu un réseau informatique qui aurait été dans la logique des années 80, par exemple, du protocole réseau X.25 au lieu du TCP/IP, échangeant des données entre les réseaux informatiques nationaux aux frontières entre pays.

Le succès de l'Internet se situe dans sa conception qui est basée sur le principe de la neutralité du réseau. Tout trafic de données sur l'Internet à ce moment-là, qu'il vienne de nouvelles petites compagnies ou de grandes compagnies, a été traité sans discrimination. Les nouvelles compagnies et les innovateurs n'ont eu besoin ni de permission ni de puissance du marché pour innover sur l'Internet.

La neutralité de réseau, a été jusqu'à présent le point important du succès de l'Internet. C'est pourquoi la discussion sur la neutralité du réseau a attiré un éventail d'acteurs: du Président des États-Unis aux activistes de bases des droit de l'Homme. La neutralité de réseau est l'une des priorités les plus élevées du programme technologique du Président Obama et cette thématique a été discutée dans plusieurs instances politiques, y compris le Congrès américain. Dès le début, la neutralité du réseau était une discussion centrée aux Etats Unis; mais avec les nouveaux développements, la neutralité de réseau est de plus en plus discutée dans le monde entier.

### **Pourquoi la neutralité du réseau est-elle d'actualité aujourd'hui?**

Il n'y a pas de conspiration. L'internet est devenu une victime de son propre succès. Avec 2 milliards d'utilisateurs et un changement croissant de notre réalité économique et sociale quotidienne sur l'Internet, les enjeux prennent de plus en plus d'importance. L'Internet a un potentiel commercial et de développement très important. Pour certains de ces aspects commerciaux, particulièrement ceux en relation avec la diffusion des services vidéo et multimédia, la neutralité du réseau pourrait constituer un obstacle.

## La situation actuelle

Paradoxalement, la neutralité du réseau n'a jamais été strictement appliquée. Depuis les débuts des connexions par modems, il y a eu des rivalités entre bande passante disponible et les besoins des utilisateurs. Afin de relever ce défi et assurer la qualité de service, les opérateurs Internet (les entreprises de télécoms et les FAI) ont utilisé diverses techniques de gestion du réseau pour prioriser certains trafics. Par exemple, le trafic internet qui permet de véhiculer la conversation vocale sur Skype devrait avoir la priorité sur le trafic qui véhicule un simple e-mail: alors que nous pouvons percevoir un retard de voix dans la conversation sur Skype, nous ne remarquerons pas les petits retards dans les échanges d'e-mails. Le besoin de gestion du réseau est particulièrement important aujourd'hui avec l'accroissement du nombre d'utilisateurs de plus en plus demandeurs davantage de services tels que les téléchargements, les vidéos Haute Définition, la téléphonie sur Internet, les jeux en ligne, etc.

### La demande croissante en bande passante

En 2009, comme illustration de la demande croissante en bande passante, les téléspectateurs de YouTube observaient environ 1.2 milliards de vidéos par jour<sup>21</sup>, et téléchargeaient presque 20 heures de vidéo chaque minute!<sup>22</sup>

La gestion du réseau devient de plus en plus sophistiquée en routant de façon optimale le trafic Internet pour garantir un service de qualité: prévenant la congestion et éliminant latences et coups de nervosité.

La première discorde dans l'interprétation du principe de la neutralité du réseau se fonde sur la question de savoir si oui ou non n'importe quelle gestion de réseau serait permise. Les puristes de la neutralité du réseau soutiennent que 'tous les bits sont égaux' et que tout le trafic internet doit être traité de façon égale. Les sociétés de télécoms et les FAI estiment plutôt que ce sont les utilisateurs qui doivent avoir un accès égal à Internet, et si cela devait arriver, le trafic ne pourrait pas être traité de manière égale. Si les trafics de vidéos et d'e-mails sont traités de manière équitable, les utilisateurs n'auront pas un bon débit vidéo à la réception, par contre, ils ne remarqueront pas le retard de quelques secondes en recevant un e-mail. Même les défenseurs de la neutralité du réseau, ne peuvent remettre en question cette raison. Leur problème est que tout compromis sur la neutralité du réseau peut ouvrir une boîte de pandore, en soulevant le problème de la distinction entre la gestion justifiée du réseau et sa possible manipulation.

## Les problèmes

Dans le débat sur la neutralité du réseau, il y a un consensus qui se dégage sur le fait qu'il y a un besoin pour une gestion *appropriée* du réseau. La question principale est celle de savoir comment interpréter l'adjectif 'approprié'. En plus des problèmes techniques, il y a trois autres aspects – les problèmes économiques, juridiques et des droits humains – où le débat sur la neutralité du réseau est particulièrement houleux.

## Les problèmes économiques

Pendant les décennies passées, beaucoup d'opérateurs – Télécoms et FAI – ont étendu leurs activités commerciales à la fourniture des services:

A côté de la vente des connexions Internet et de la bande passante aux ménages et aux entreprises, ils ont introduit leurs propres VoIP (Voice-over Internet Protocol ; le téléphone via internet) ou IPTV (la télévision via Internet) services, la vidéo à la demande (une sorte de location de films), les portails de téléchargement de musique et de vidéos, etc. Ils sont maintenant en concurrence entre eux, non seulement pour des connexions moins chères, plus rapides et de meilleure qualité, mais également avec les fournisseurs de services et de contenus comme Skype, Google et Apple.

La gestion du réseau, quelque chose de disponible aux opérateurs mais pas aux autres peut s'avérer un outil important dans une compétition sur les services et les contenus en donnant la priorité aux paquets selon leur préférence commerciale.

Par exemple, un opérateur peut décider de ralentir la circulation des données ou carrément bloquer les données d'un concurrent (telle la téléphonie Skype ou Google) aux utilisateurs finaux à travers son réseau, ceci tout en donnant la priorité à ses propres données (telles que la téléphonie sur IP ou la télévision sur internet qu'il fournit à ses clients)<sup>23</sup>.

## Les problèmes juridiques

Une autre zone grise dans la gestion du réseau est le droit des opérateurs de bloquer les contenus qui peuvent enfreindre les droits d'auteurs. Les FAI ont-ils le droit et l'obligation d'arrêter le trafic, par exemple, sur les réseaux **peer-to-peer** (P2P) qui sont souvent utilisés pour le partage des éléments protégés par les droits d'auteurs? Ont-ils les prérogatives des corps juridiques et administratifs?

Certaines de ces questions ont été le point central d'une affaire entre la *Federal Communication Commission (FCC)* et l'opérateur Internet Comcast. En 2007, deux groupe-conseils publics ont porté plainte auprès de la FCC, l'autorité américaine de régulation, se plaignant du fait que Comcast, l'opérateur, avait violé le principe de la neutralité du réseau en ralentissant de façon significative l'application BitTorrent (Logiciel P2P pour le téléchargement des fichiers – très souvent de la musique, la vidéo et les jeux, bien que ne se limitant pas à cela) pour ses utilisateurs<sup>24</sup>.

### Les problèmes politiques

La capacité à gérer le trafic réseau basé sur l'origine et la destination, le service et le contenu, peut donner aux États l'occasion d'imposer de telles pratiques sur les opérateurs du trafic domestique et introduire par la même occasion les filtres pour les contenus sensibles et controversés en relation avec la politique, l'idéologie, la religion, la culture ou d'autres valeurs de ce pays. Ceci amène les risques d'abus dans la gestion du réseau pour permettre la censure, particulièrement dans des pays aux régimes autoritaires.

### Les risques

Si la gestion du réseau va au-delà d'un niveau *approprié* visant à fournir un service équitable à tous les utilisateurs internet, le principe de la neutralité du réseau serait en danger. Cela pourrait conduire à un Internet à plusieurs strates.

Selon les groupes d'utilisateurs tels que Save the Internet<sup>25</sup> et Internet Governance Caucus<sup>26</sup>, l'Internet deviendrait un ensemble de packages commerciaux offerts par les FAI dont les utilisateurs ne pourraient accéder qu'à une partie des services et contenus en ligne dans un certain package donné<sup>27</sup> – beaucoup plus comme la télévision par câble.

Par conséquent, ils préviennent que si les opérateurs de trafic commencent à taxer les fournisseurs de contenus et d'application, cela tuerait la concurrence entre opérateurs propriétaires des services, et mettrait en danger les petits commerces<sup>28</sup> et les offres non commerciales, telles que les applications pour des personnes vivant avec des handicaps qui demandent généralement une large bande passante.

### Qui sont les principaux acteurs et quels sont leurs arguments?

La position des principaux acteurs est en constant changement. Par exemple, la dernière indication selon laquelle Google signerait un accord spécial avec Verizon pour une approche intermédiaire à la neutralité du réseau changerait

le positionnement des principaux acteurs<sup>29</sup>. Jusqu'à maintenant, Google a été considéré comme l'un des fervents défenseurs de la neutralité du réseau ; les autres sont les associations des consommateurs, les entreprises en ligne, certaines entreprises du domaine des technologies, la plupart des grandes entreprises d'Internet comme Yahoo !, Vonage, Ebay, Amazon, Earthlink ainsi que les entreprises de logiciels telle que Microsoft.

	Les partisans	Les opposants
<b>L'argument à propos du futur</b>	La neutralité du réseau préservera l'architecture de l'Internet qui a permis un développement rapide et innovant de l'internet jusque-là. La plupart des défenseurs de la neutralité du réseau sont les nouvelles entreprises d'Internet qui se sont développés grâce à l'architecture ouverte de l'Internet.	Les entreprises en ligne doivent avoir l'opportunité de développer davantage l'Internet et offrir les services qui intéressent les clients. Ceci peut impliquer un internet plus rapide.
<b>Les arguments économiques</b>	Sans la neutralité du réseau l'Internet ressemblera à la Télévision par câble. Une poignée de sociétés contrôleraient l'accès et la distribution des contenus en décidant quel utilisateur a le droit de le regarder et combien cela doit coûter. Alors que cela profiterait à peu, la majorité en pâtirait et en fin de compte ruinerait le futur économique de l'Internet.	S'il n'y a pas la possibilité d'offrir de nouveaux services et des modèles économiques, ceci réduirait l'intérêt économique de l'Internet, stopper les investissements et même en fin de compte mettre en péril l'infrastructure de l'internet.
<b>Les arguments éthiques</b>	L'internet est le résultat de développements par plusieurs volontaires pendant de nombreuses décennies. Ils avaient investi leur temps et leur créativité en développant les aspects intrinsèques de l'internet, des protocoles techniques aux contenus. Il n'est donc pas juste de voir ce grand investissement profiter a une minorité de compagnies qui enfermeront l'internet dans des systèmes contraignants en violant le principe de la neutralité du réseau. L'Internet a été conçu de façon à être ouvert et public. L'intérêt du public doit être garanti. La neutralité du réseau est l'un des moyens de parvenir à cela.	La neutralité du réseau est éthiquement discutable parce que les opérateurs de l'internet doivent investir dans la maintenance de leur infrastructure et beaucoup de bénéfices sont réalisés par les compagnies des contenus telles que Google, Facebook et Amazon. Les opérateurs internet et télécoms estiment que le gâteau devrait être partagé un peu plus équitablement.
<b>Les arguments de régulation</b>	La neutralité du réseau doit être imposée par les Etats. Toute forme d'autorégulation ouvrira la voie aux opérateurs télécoms et Internet et les compagnies du câble à une violation de la neutralité du réseau.	L'Internet s'est développé à cause d'une régulation légère ou sans régulation du tout. Une régulation trop lourde de la part des Etats peut étouffer la créativité et une régulation sur la neutralité du réseau peut étouffer le développement futur de l'internet.

Les opposants à la neutralité du réseau y compris les principales compagnies de Télécoms, les FAI, les producteurs des équipements de réseau et matériel informatiques, ainsi que les producteurs du matériel vidéo et multimédia. Leurs arguments sont centrés sur le marché, en commençant par le besoin de fournir ce que les consommateurs demandent.

Il y a quatre arguments principaux dans le débat sur la neutralité du réseau.

### Les principes de base

Dans un passé récent, quelques régulateurs- tels que ceux de la Norvège, des Etats Unis ou de l'UE ont fait un pas et ont formulé les principes-clé de la neutralité du réseau en se basant sur les discussions en cours.<sup>30</sup>

- **Transparence:** Les opérateurs internet doivent fournir des informations complètes et actualisées sur leurs pratiques en matière de gestion du réseau, sur leur capacité, et sur la qualité des services offerts aux clients.
- **Accès:** Les utilisateurs devraient avoir un accès [équitable] à n'importe quel service contenu, service ou application [légale] [avec un minimum de la qualité de service garanti, tel que prescrit par le régulateur] ou bien connecter tout équipement qui ne gêne pas le réseau [sans distinction de leurs capacités financières ou statuts sociaux].
- **(Non) discrimination:** les opérateurs internet ne doivent faire aucune discrimination [ou une discrimination raisonnable] sur le trafic en se basant sur:
  - L'origine de l'expéditeur et du receveur
  - Le type du contenu, de l'application et du service [avec une concurrence saine – pas de discrimination contre les concurrents indésirables].
  - Là où "raisonnable" serait toute pratique pour le bénéfice public (assurer la qualité de service, la sécurité et la résilience du réseau, les innovations et les investissements supplémentaires, la baisse des prix, etc.).

Les autres principes souvent débattus dans les forums internationaux tels que les réunions du FGI et le dialogue *EuroDIG*<sup>31</sup> comprennent:

- La protection de la liberté d'expression, d'accès à l'information et de choix.
- Assurer la qualité du service, la sécurité et la résilience du réseau.
- Préserver un environnement favorable aux investissements.

## Utilisateurs ou clients?

Le débat sur la neutralité de réseau crée également une rhétorique linguistique. Les partisans de la neutralité de réseau se concentrent sur les 'utilisateurs' d'Internet, alors que les autres – principalement les acteurs commerciaux – les décrivent comme étant des 'clients'. Les internautes sont plus que de simples clients ; le terme 'utilisateur' implique la participation active au développement de l'Internet par le biais des réseaux sociaux, le blogging, et d'autres outils; et le rôle important qu'ils ont en décidant du futur d'Internet. Les clients, d'une part, comme tous les autres clients, peuvent décider si oui ou non il faut acheter les services offerts. Leur statut sur l'Internet est basé sur un contrat avec le FAI et sur des règles de protection des utilisateurs. Au delà, les clients sont supposés n'avoir aucun rôle dans la prise de décision sur le fonctionnement de l'Internet.

- Stimuler les innovations pour les investissements [y compris les opportunités pour de nouveaux modèles d'affaires et de nouvelles possibilités commerciales]. Définir les droits et rôles, et créer l'obligation de rendre des comptes pour toutes les parties engagées (fournisseurs, régulateurs, utilisateurs) incluant le droit de faire appel et d'obtenir réparation.
- Prévenir les pratiques de concurrence déloyale.
- Créer un environnement pour un marché qui permettrait à tous les utilisateurs de choisir ou de changer librement leur opérateur réseau.
- Protéger les intérêts des couches fragiles, telles que les personnes vivant avec un handicap ainsi que les utilisateurs et les entreprises des pays en développement.
- Maintenir la diversité des contenus et des services.

### Les approches politiques

Avec le débat sur la neutralité du réseau, il y a une autre question qui a surgi: quel est le rôle des régulateurs dans la politique en rapport avec la large bande et les pratiques des opérateurs?

### Les pays développés

En réponse à l'affaire Comcast, le FCC américain a adopté les lignes directrices sur la neutralité du réseau comme une mise à jour de son papier blanc de 2005,<sup>32</sup> lesquelles reflètent le besoin d'accès aux contenus et des équipements ainsi que le choix des ces derniers, cela a résolu les problèmes de discrimination et de transparence. Le Ministère Japonais des affaires intérieures et le Groupe de travail sur les communications ont fait un

rapport sur le choix et l'accès ainsi que sur la discrimination, mais ils se sont également penchés sur la répartition équitable des coûts et l'utilisation du réseau<sup>33</sup>. L'Agence suédoise des Postes et Télécoms (PTS) a soutenu que l'ouverture – soutenue par la concurrence et la non-discrimination est un pré requis pour l'innovation, mais qu'elle doit également être équilibrée entre les investissements et la sécurité du réseau.<sup>34</sup> Le cadre réglementaire des communications électroniques de l'UE vise à protéger la liberté d'expression, le choix des utilisateurs et les droits d'accès, ensemble avec le principe de transparence ; pourtant le cadre met également l'accent sur le besoin d'investissement, la concurrence saine sans discrimination, et des opportunités pour de nouveaux modèles économiques incluant les initiatives innovatrices.<sup>35</sup>

Le modèle le plus en vogue vient de L'autorité Norvégienne des Postes et Télécoms (NPT), qui cherche à assurer: la transparence dans les affaires et les pratiques, le choix de l'utilisateur et l'accès aux contenus, les services et les équipements, et la non discrimination basée sur les applications, les services, le contenu, l'expéditeur et le receveur.<sup>36</sup> Cependant, ce n'est pas seulement le contenu qui est en jeu mais également le processus pour parvenir à un consensus à propos de ces lignes directrices: adopter une approche largement basée sur l'implication de toutes les parties prenantes dans la mise en place d'un système souple de co-régulation basé sur la recherche d'un consensus à travers des accords d'engagement; dans ce sens, le NPT a rassuré les consommateurs et les entreprises sur le fait que le marché peut être régulé sans dispositif légal lourd.<sup>37</sup>

Toutefois, dans certains pays, il y a une pratique qui consiste à ne pas prévenir les discriminations à caractère commercial. Les défenseurs de la neutralité du réseau les qualifient de "paradis anti-neutralité" où, l'on peut voir ce que sont les perspectives d'un 'Internet véritablement non neutre'.

### Les pays en développement

A cause d'une infrastructure et une bande passante limitées, les régulateurs des pays en développement se basent plus sur des politiques de bon usage – prix abordables et accès équitable pour tous. D'autres soulèvent les problèmes relatifs à la non-discrimination transfrontalière, en avançant que le trafic de tous les pays doit être traité de la même manière sans référence aux coûts de terminaison. De plus, certains pays sont plus sensibles aux aspects culturels internes, politiques ou éthiques, entraînant de ce fait une compréhension de 'l'usage approprié' dans la perspective d'une gestion différente du réseau par rapport aux autres pays. On a évoqué les problèmes selon lesquels les modèles innovateurs du monde développé pourraient compromettre les marchés

des pays en développement: en donnant la priorité aux services des grandes compagnies internationales; les entreprises émergentes et la concurrence seraient menacées, mettant en péril la diversité et l'innovation. Toutefois, aucune politique formelle majeure ou pratique régulatrice sur la neutralité du réseau ne provient du monde en développement.

### Les organisations internationales et les ONG

Plusieurs organisations internationales et groupes d'utilisateurs ont ainsi développé des positions politiques par rapport à la neutralité du réseau. Le Conseil de l'Europe met l'accent sur les droits fondamentaux de la liberté d'expression et d'information; l'ISOC fait la promotion de son approche centrée sur l'utilisateur avec une prédominance sur les problèmes concernant l'accès, le choix, et la transparence à travers le débat sur l'"inter-réseautage ouvert" plutôt que celui sur la neutralité du réseau.<sup>38</sup> Le Trans Atlantic Consumer Dialogue (TACD), un forum des associations de consommateurs des Etats Unis et de l'UE met ainsi l'accent sur les demandes non-discriminatoires des opérateurs de trafic, appelant les régulateurs des Etats Unis et de l'UE à agir comme les défenseurs des droits des utilisateurs.<sup>39</sup> Beaucoup d'ONG se sentent particulièrement concernées par le futur des contenus non commerciaux et non concurrentiels des services en ligne, en demandant qu'ils soient diffusés à travers le réseau de transport de n'importe quel opérateur comme c'est le cas dans le cadre commercial. Ils mettent l'accent sur les droits des groupes marginaux – particulièrement les personnes handicapées – qui doivent utiliser les contenus, les services et les applications (y compris les applications requérant une grande bande passante) de leur choix sans aucune limite.

### Les questions ouvertes

Il y a un nombre important de questions ouvertes dans l'agenda du débat sur la neutralité du réseau.

- Où devrait se trouver l'équilibre entre les effets du bien public sur l'Internet et les droits de l'utilisateur (homme) d'un côté, et de l'autre les droits des opérateurs Internet à innover sur leurs propres réseaux?
- Un marché non régulé avec une concurrence ouverte comme évoqué par les opérateurs de trafic, peut-il fournir un choix illimité (ou suffisant) aux utilisateurs? Ou alors, les régulateurs doivent-ils inévitablement servir de garde fous, et avec quelle autorité?
- Comment les différentes méthodes des régulateurs peuvent-elles avoir un impact sur le marché de la bande passante et susciter plus d'investissement et d'innovation?

- Quelles sont les implications de la (non) neutralité du réseau pour les pays en développement?
- Le besoin de gestion du réseau pour des raisons techniques (qualité) sera-t-il obsolète dans l'avenir, à cause des évolutions dans la technologie de transport du trafic?
- Quelles sont les implications d'un Internet fragmenté pour la concurrence, l'innovation, l'investissement, et les droits de l'Homme?
- Comment l'ère du *cloud computing* (informatique en nuages) et la dépendance croissante vis-à-vis du nuage influenceront-ils le débat sur la neutralité du réseau et vice versa?
- Le débat devrait-il être étendu de la gestion du trafic au niveau de l'opérateur de transport, à la gestion des contenus et des applications au niveau du fournisseur de contenus et d'application, tels que Google, Apple ou Facebook?
- La protection du consommateur sera-t-elle toujours intrinsèquement liée à la neutralité du réseau? Si la neutralité du réseau était 'défaite', quels principes soutiendraient la protection du consommateur dans l'avenir?

## Les Fournisseurs d'Accès Internet (FAI)

Puisque les FAI connectent les utilisateurs finaux à l'Internet, ils fournissent l'option la plus directe de l'application des règles du droit sur l'Internet. Avec les problèmes de l'accroissement de l'aspect commercial de l'Internet et de l'importance grandissante des questions de cyber sécurité, beaucoup de pays ont commencé à concentrer tous leurs efforts sur l'application du droit aux FAI.

### Les enjeux

#### Les Monopoles de Télécom et les FAI

Il est courant de trouver que dans les pays avec des monopoles sur les télécommunications, ces monopoles fournissent également un accès à l'Internet. Ces monopoles prohibent les autres FAI d'entrer sur le marché, empêchant ainsi la concurrence.

Cela a pour conséquences les prix élevés, avec souvent une qualité de service médiocre, et un échec dans la réduction de la fracture numérique. Dans certains cas, ces monopoles dans les télécommunications tolèrent l'existence d'autres FAI, mais interfèrent au niveau opérationnel (par exemple en offrant une faible bande passante ou en causant des interruptions dans les services).

### La responsabilité des FAI en matière de droits d'auteurs

Il y a un principe commun dans tout système juridique: un FAI ne sera pas tenu pour responsable d'avoir hébergé des éléments qui enfreignent les droits d'auteurs (copyright) si le FAI n'est pas au courant de la violation. La différence principale se situe au niveau des actions légales entreprises après que le FAI ait été informé que l'élément qu'il héberge enfreint les droits d'auteur.

Les lois des Etats Unis et de l'UE emploient la procédure *Notice-Take-Down*, qui exige des FAI le retrait d'un tel élément pour éviter d'être poursuivi. La loi japonaise adopte une approche plus équilibrée, à travers la procédure *Notice-Take-Down*, qui donne à l'utilisateur de l'élément le droit de porter plainte contre la demande de suppression de l'élément.

L'approche qui consiste à placer une responsabilité limitée sur les FAI a généralement été dictée par la jurisprudence. Les cas les plus importants où les FAI ont été exemptés de toute responsabilité pour avoir hébergé des éléments qui sont en violation des droits d'auteur sont: le cas de la Scientologie (Pays-Bas), *RIAA vs Verizon* (Etats Unis), *SOCAN vs CAIP*(Canada), et *Sabam vs Tiscali* (Belgique).

### Le rôle des FAI en matière de contenus

Sous la pression publique croissante, les FAI, bien qu'à contrecœur, s'impliquent de plus en plus dans la politique du contenu. En le faisant, ils devraient suivre deux voies possibles. La première, consiste en l'application de mesures de régulation de l'Etat. La seconde, est basée sur l'autorégulation, et soutient qu'il appartient aux FAI de décider par eux-mêmes le contenu approprié. Ceci fait courir le risque de privatiser le contrôle du contenu, ce qui ferait que les FAI prendraient les responsabilités des Etats.

### Le rôle des FAI dans la politique anti-pollupostage

Les FAI sont en général considérés comme les premières structures impliquées dans les initiatives anti-pollupostage. Généralement, les FAI disposent de leur propre initiative de lutte contre le pollupostage, soit par un filtrage technique ou par la mise en place d'une politique anti-pollupostage. Le rapport de l'UIT sur le pollupostage déclare que les FAI devraient être responsables et proposer des code de conduite anti-pollupostage, qui doivent inclure deux dispositions importantes: un FAI doit interdire à ses utilisateurs d'envoyer des pollupostages et il ne doit pas entretenir des relations de peering avec un autre FAI qui refuse un tel code de conduite.<sup>40</sup>

Par exemple, le système de filtrage de Verizon a conduit à un procès car ayant également bloqué des messages légitimes, causant des préjudices aux utilisateurs qui n'ont pas pu recevoir leurs messages.<sup>41</sup>

## Les fournisseurs de bande passante internet (Internet Broadband Band Providers - IBP)

L'architecture de l'accès Internet a trois niveaux. Les FAI qui connectent les utilisateurs finaux constituent le *niveau 3* (niveau hiérarchique 3). Les niveaux hiérarchiques 1 et 2 sont constitués des IBP. Les fournisseurs du niveau 1 sont les IBP les plus importants. Ils ont toujours des arrangements de peering avec les autres IBP niveau 1.<sup>42</sup> La principale différence entre les IBP et ceux du Niveau 2 est que les IBP de Niveau 1 échangent leur trafic par peering alors que les IBP de Niveau 2 doivent payer les frais de transit aux IBP de Niveau 1.<sup>43</sup>

Le Niveau 1 est toujours constitué de grandes compagnies telles que MCI, AT&T, Câble Wireless et France Télécom.

### Les problèmes

#### L'infrastructure Internet doit-elle être un service public?

Les données internet peuvent circuler à travers n'importe quel média de télécommunications. En pratique, les équipements tels que ceux des dorsales de niveau 1 (Ex: Les principaux transits de données entre de larges réseaux stratégiquement interconnectés et les routeurs principaux de l'Internet), souvent constitués de fibres optiques ou de liaisons satellitaires sont devenus critiques dans le fonctionnement de l'Internet. Leurs positions stratégiques sur l'Internet donnent à leurs propriétaires le pouvoir d'imposer les prix et les conditions du marché. En fin de compte, le fonctionnement de l'Internet dépend des décisions des propriétaires de ces dorsales centrales.

Est-il possible à la communauté internet mondiale de demander des assurances et des garanties aux opérateurs télécoms majeurs pour un fonctionnement harmonieux de l'infrastructure critique de l'Internet? De nos jours, les discussions se focalisent sur une probable imposition de certaines exigences publiques sur les opérateurs privés de l'infrastructure de l'Internet.

### **IBP et l'infrastructure critique**

Au début de 2008, il y a eu une perturbation des câbles internet principaux dans les pays de la Méditerranée, proches de l'Égypte. Cet incident a mis en difficulté l'accès à l'Internet dans une grande partie du globe, jusqu'en Inde. Deux incidents similaires étaient survenus en 2007 (dérangement d'un câble internet proche de Taiwan et du câble principal du Pakistan) démontrant clairement que l'infrastructure est une composante nationale et mondiale de l'infrastructure critique. Une perturbation des services internet peut affecter toute l'économie et la vie sociale d'une région. L'éventualité d'une telle perturbation pousse à se poser un certain nombre de questions: les principaux câbles internet sont-ils bien protégés?

Quels sont les rôles respectifs des gouvernements nationaux, des organisations internationales et des compagnies privées dans la protection des câbles internet?

Comment pouvons-nous gérer les risques associés aux potentielles ruptures de ces câbles principaux de l'Internet?

### **La libéralisation des télécoms et le rôle des FAI et des IBP**

Il y a des vues qui divergent au sujet des modalités selon lesquelles les FAI et IBP devraient être soumis aux mécanismes des instruments internationaux existants. Les pays développés pensent que les règles libérales édictées par l'OMC aux opérateurs télécoms peuvent être également applicables aux FAI. Une interprétation restrictive met en lumière le fait que le régime des Télécoms de l'OMC s'applique seulement au marché des télécoms. La régulation du marché des FAI requiert de nouvelles règles de la part de l'OMC.

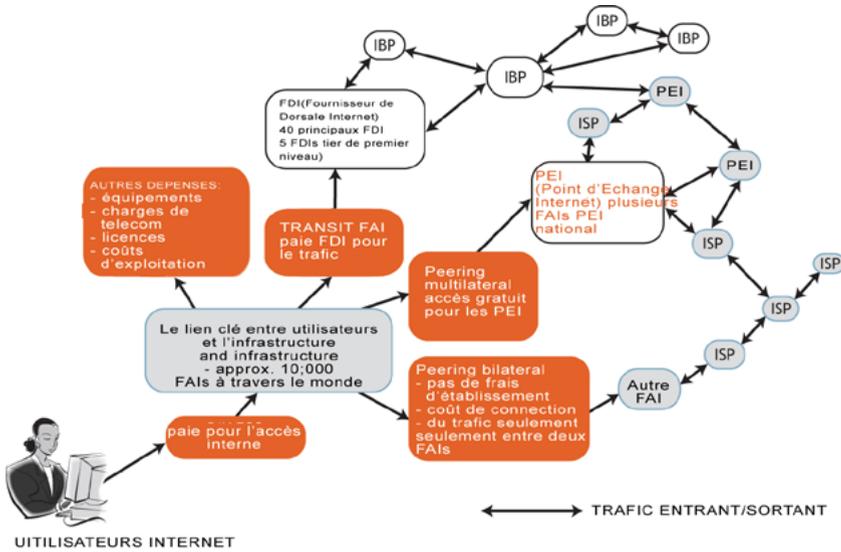
## **Un modèle économique de l'inter connectivité de l'Internet**

*Nous savons comment router les paquets, ce que nous ne savons pas faire c'est router les dollars.*

**David Clark**

### **La situation actuelle**

Souvent, toute discussion liée à des questions de gouvernance débouche sur analyse de distribution d'argent.<sup>44</sup> ' Qui paye pour l'Internet? ' Un nombre de transactions financières a lieu entre les parties impliquées dans l'Internet. Les abonnés individuels et les entreprises payent les FAI pour l'accès et les services Internet. Comment cet argent est-il distribué aux autres dans la



chaîne des services internet? Ou en d'autres termes comment le dollar de l'Internet circule-il?<sup>45</sup> Les dépenses qui devraient être couvertes à partir des frais collectées par les FAI incluent entre autres:

- Les FAI payent aux opérateurs télécoms et pour la bande passante.
- Les FAI payent aux 'RIR' ou 'LIR' desquels on obtient des pools d'adresses IP.
- Les FAI payent aux vendeurs d'équipements, de logiciels et pour la maintenance (ainsi que pour les outils de diagnostic et les autres frais de fonctionnement de leurs services).
- Les parties qui enregistrent un nom de domaine payent auprès d'un registrar et à l'IANA pour leurs services; et
- Les opérateurs télécoms payent auprès des fabricants des câbles, des satellites et des fournisseurs de services de télécoms pour leur fournir les liaisons nécessaires. (Comme les opérateurs sont souvent endettés, ils payent à leur tour de nombreux intérêts aux banques et aux consortiums).

La liste est longue et à vrai dire, 'il n'y a rien qui soit gratuit'. Finalement, les utilisateurs finaux de l'internet, qu'ils soient des individus ou des institutions, payent quelque chose dans cette chaîne.

## Les problèmes

### Le modèle économique de la connectivité d'internet a-t-il besoin de réforme?

Un des legs de l'internet c'est son modèle économique en cours qui a été développé à travers un certain nombre d'interactions. Le modèle économique d'internet est à présent considéré comme étant efficace grâce à la souplesse du fonctionnement de l'internet, et en général, son coût abordable. La principale critique du modèle économique en cours est centrée sur deux aspects:

- 1 Il n'évite pas un monopole des principaux acteurs dans le domaine de la connectivité de l'internet, et par conséquent une distorsion du marché est potentiellement possible.
- 2 Il n'alloue pas un partage équitable à la fois des revenus et des coûts entre tous ceux qui sont impliqués dans l'économie de l'internet.

Dans les milieux académiques, beaucoup de tentatives ont été faites afin de pourvoir à des politiques économiques adéquates pour l'Internet. Nguyen et Armitrage déclarent que l'Internet devrait avoir un équilibre optimal entre trois éléments: l'efficacité technique, l'efficacité économique et les effets sociaux.<sup>46</sup> D'autres soulignent les défis pour remplacer la structure de tarification existante, simple, une structure à taux-plat par une autre plus complexe, telle que la compatibilité basée sur le trafic des paquets. En rapport avec les changements pratiques, certains pensent que changer le modèle économique de l'internet actuel ouvrirait la boîte de Pandore.

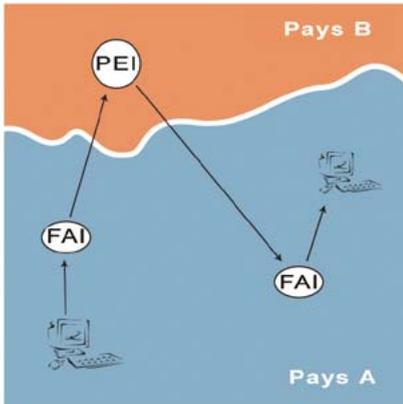
### Empêcher les monopoles possibles dans le marché des ressources de l'internet

Il est possible qu'à travers les changements, quelques monopoles pourraient dominer le marché entier du trafic de l'internet<sup>47</sup>. Ce problème existe à la fois dans les pays développés et ceux en développement. Certains considèrent que le processus de libéralisation des marchés des télécommunications résoudra le problème des monopoles (surtout en associant les opérateurs historiques). Cependant, la libéralisation conduirait au remplacement d'un monopole public par un monopole privé. Geoff Huston dit que l'installation des monopoles et la perte des diverses ressources du marché de l'internet pourraient inévitablement affecter le prix et la qualité des services de l'internet.<sup>48</sup>

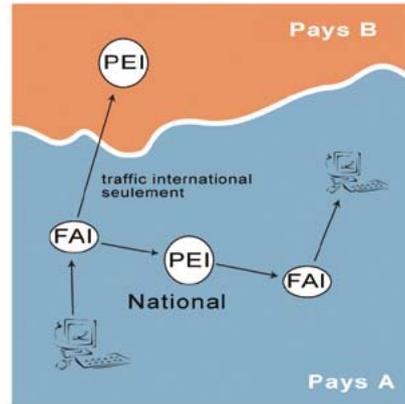
Qui supporterait le coût des liens entre les pays développés et les pays en développement?

*'Quand un utilisateur final au Kenya envoie un e-mail à un correspondant aux Etats Unis, c'est l'ISP Kenyan qui supporte le coût de connexion internationale du Kenya aux Etats Unis. Paradoxalement, quand un*

Trafic internet sans PEI



Trafic internet avec PEI



*utilisateur final américain envoie un e-mail au Kenya, c'est toujours l'ISP Kenyan qui supporte le coût de la connexion internationale, et en fin de compte c'est l'utilisateur final Kenyan qui supporte tout le poids en payant le coût le plus élevé des abonnements.*<sup>49</sup>

Actuellement, les pays en développement supportent le coût des liaisons entre les pays en développement et les pays développés<sup>50,51</sup>. Comparé au système de téléphonie traditionnelle, où deux pays partagent le prix de chaque appel international, le modèle Internet met la charge entière d'un côté: celui des pays en développement. Ces pays doivent supporter les coûts pour se connecter aux dorsales situées dans les pays développés. Comme résultat, les pays pauvres et les petits pays subventionnent l'Internet dans les pays riches.

L'argument principal dans les discussions sur les changements vers le système actuel de facturation de l'internet utilise l'analogie du système de règlement financier du téléphone, qui partage le coût et le revenu entre les points finaux de communication. Cependant, Geoff Huston stipule que cette analogie n'est pas à soutenir. Dans le système téléphonique, il n'y a qu'un produit clairement identifiable -un appel téléphonique établissant une conversation humaine entre deux postes téléphoniques – comme un prix<sup>52</sup>. L'internet n'a pas un équivalent, un seul produit, seulement les paquets, qui prennent différents itinéraires à travers le réseau. Cette différence fondamentale rend cette analogie inappropriée. C'est aussi la raison principale qui fait que le modèle de règlement financier téléphonique soit difficile à appliquer à l'Internet.

L'UIT a initié des discussions sur les améliorations qui pourraient être apportées au système actuel de règlement des dépenses liées à l'Internet, afin

d'aboutir à une distribution plus équilibrée des coûts d'accès à l'internet. A cause de l'opposition des pays développés et des opérateurs de télécoms, la résolution adoptée de l'UIT, la D.50, est restée pratiquement sans effet<sup>53</sup>. Des tentatives infructueuses ont également été faites soumettre ce problème aux négociations de l'OMC. Le besoin d'ajustements dans les facturations de l'interconnexion fut réitéré dans les documents finaux du Sommet Mondial de la Société de l'Information (SMSI) et dans le rapport du Groupe de travail sur la gouvernance de l'intérêt (GTGI).

## Les normes du web

Vers la fin des années 1980, la bataille sur les normes du réseau fut achevée. Le TCP/IP devenait progressivement le principal protocole du réseau, en marginalisant d'autres standards tels que X25 soutenu par l'UIT et beaucoup de standards propriétaires tel que le SNA d'IBM. Pendant que l'Internet a facilité la communication normale entre plusieurs réseaux à travers TCP/IP, le système manquait encore de standards pour des applications communes.

Une solution fut développée par Tim Berners-Lee et ses collègues au CERN (Centre Européen pour la recherche nucléaire) à Genève, un nouveau standard pour le partage de l'information sur l'Internet appelé HTML (qui n'était juste qu'une simplification d'un standard ISO existant appelé SGML – *Standard Generalized Markup Language*).

Le contenu affiché sur l'Internet devrait d'abord être organisé selon les standards du HTML. Le HTML, étant la base du World Wide Web (toile d'araignées mondiale), a préparé le chemin à la croissance exponentielle de l'Internet.

Depuis sa première version, le HTML a été constamment amélioré avec l'intégration de nouvelles fonctionnalités. La pertinence croissante de l'Internet a mis en exergue la question de la standardisation du HTML. Ceci était particulièrement pertinent pendant les 'guerres des navigateurs' entre Netscape et Microsoft, lorsque chaque société a essayé de renforcer sa position sur le marché en influençant les standards du HTML. Si le HTML de base ne gérait que les textes et les photos, les nouvelles applications d'Internet ont exigé des technologies plus sophistiquées capables de gérer les bases de données, la vidéo et les animations.

Une telle variété d'applications a exigé des efforts considérables de normalisation pour s'assurer que le contenu internet soit proprement visualisé par la majorité des explorateurs d'internet (*browsers*).

La standardisation d'application a intégré une nouvelle phase avec l'émergence de XML, qui a fourni une plus grande flexibilité dans l'établissement des standards du contenu Internet.

De nouvelles séries de standards XML ont également été introduites. Par exemple, le standard pour la distribution du contenu sans fil appelé *Wireless Markup Language* (WML).

La standardisation d'application est principalement menée dans le cadre du consortium du World Wide Web (W3C) sous le leadership de Tim Berners-Lee. Il est intéressant de remarquer que malgré sa grande pertinence à l'Internet, le W3C n'a pas encore attiré beaucoup d'attention dans le débat sur la gouvernance de l'Internet.

## Informatique en nuages

Le terme 'cloud computing – informatique en nuages' est utilisé pour décrire une tendance récente dans l'industrie informatique basée sur l'usage des applications informatiques en tant que services fournis à partir d'énormes groupes de serveurs (une collection de serveurs informatiques entretenus par une entreprise pour accomplir des tâches de serveurs largement au-delà de la capacité d'une seule machine). La première manifestation de l'informatique en nuages est déjà disponible avec le mouvement des e-mails, de nos disques durs vers les serveurs de messagerie (Gmail, Hotmail, Yahoo !) et l'utilisation des processeurs de traitement de texte en ligne (Wiki, services Google). Les applications des réseaux sociaux tels que Facebook et les blogs ont accentué la tendance vers l'informatique en nuages. De plus en plus, nos outils numériques sont déplacés des disques durs vers le nuage (cloud). Les principaux acteurs dans le cloud computing sont Google, Microsoft, Apple, Amazon, et Facebook ; tous ont soit déjà un gros serveur ou planifient d'en développer un de type 'cloud'.

Dès les premiers jours, il y avait de grands et puissants ordinateurs centraux ainsi que des stations de travail. La puissance était au centre. Après cela et pendant longtemps, avec les ordinateurs personnels et les applications Windows la puissance de l'ordinateur s'est déplacée vers la périphérie.

L'informatique en nuages fermera-t-il le cercle? Allons-nous avoir quelques gros ordinateurs centraux/serveurs et des milliards de stations de travail sous forme de 'bloc-notes', de moniteurs, et de téléphones mobiles? La réponse à cette question et à tant d'autres viendra avec le temps. Actuellement, nous pouvons identifier quelques sujets de la gouvernance de l'Internet qui vont probablement émerger en parallèle avec le développement de l'informatique en nuages.

- 1 Avec plus de services fournis en ligne, la société moderne accroîtra sa dépendance vis-à-vis de l'Internet. Dans le passé, lorsque l'Internet tombait en panne nous n'étions pas capables d'envoyer d'e-mail ou de naviguer sur le net. A l'ère de l'informatique en nuages nous ne pourrons même pas écrire de texte ou faire des calculs. Une plus grande dépendance envers l'Internet impliquera une plus grande pression sur sa robustesse et sa fiabilité. Cela conduira inévitablement à un régime de gouvernance de l'internet plus fort et une plus grande implication des gouvernements.
- 2 Avec plus de nos données personnelles emmagasinées dans les clouds (nuages), la question de la protection des données personnelles se posera avec plus d'acuité. Aurons-nous le contrôle de nos fichiers textes, e-mails et autres données? Les opérateurs de l'informatique en nuages pourront-ils les utiliser sans notre permission? Qui aura accès à nos données?
- 3 Avec un volume croissant d'outils sociaux passant au format numérique, les pays seront dans une position inconfortable car ayant des patrimoines nationaux hébergés hors des 'frontières' nationales. Ils pourront essayer de créer les clouds nationaux ou régionaux ou s'assurer que les clouds existants sont gérés avec une certaine supervision internationale. La nationalisation des 'nuages' pourra s'accélérer par le fait que tous les principaux opérateurs dans ce domaine sont basés aux Etats Unis. Certains disent que l'actuel débat centré sur l'ICANN peut être remplacé par un débat de gouvernance de l'Internet centré sur la régulation de cloud computing.
- 4 Avec les divers opérateurs du cloud computing, la question des standards devient très importante. L'adoption des standards communs assurera un transfert souple des données parmi les différents clouds (ex. de Google à Apple). Une possibilité en discussion est l'adoption de standards ouverts par les principaux opérateurs du cloud computing.

Lorsqu'il s'agit de cloud computing il y a plus de questions que des réponses. La Gouvernance de l'Internet du cloud computing risque d'émerger à travers l'interaction d'une diversité d'acteurs et de structures. Par exemple, l'UE se focalise sur la vie privée et la protection des données personnelles. Le 'Safe Harbor Agreement' qui était supposé résoudre le problème des différents régimes en matière de respect de la vie privée aux Etats Unis et dans l'UE ne fonctionne pas bien. Avec plus de données numériques qui traversent de

l'océan Atlantique, l'UE et les Etats Unis devront trouver une solution à la question de la protection de la vie privée selon les standards de l'UE par les sociétés Américaines, principaux opérateurs dans le cloud computing.

Lorsqu'il s'agit des standards, il est très probable que les principales sociétés puissent trouver un accord entre elles. Google a déjà commencé une forte poussée vers les standards ouverts en établissant un 'Front de libération des données' dont le but est d'assurer une transition souple des données entre les différents clouds. Ce sont ces premiers groupes qui traiteront la question de la gouvernance de l'internet de l'informatique en nuages. D'autres vont probablement émerger en tant que solution aux problèmes concrets de stratégie.

## Convergence internet-télécommunication-multimédia

Historiquement, la télécommunication, la radio diffusion et les autres domaines associés constituaient des secteurs différents de l'industrie; ils utilisaient des technologies différentes et étaient gouvernés par des régulations différentes. L'importance et la prédominance utilisation de l'IP a conduit à la convergence de ces technologies. Aujourd'hui, nous pouvons passer un coup de téléphone, regarder la télévision et partager la musique sur nos ordinateurs via Internet. Il y a seulement quelques années, cela aurait été fait en recourant à des systèmes différents.

Dans le champ de la communication traditionnelle, le principal point de convergence est la voix sur IP (VoIP). La popularité croissante des systèmes de VoIP tel que Skype est basé sur son faible coût, la possibilité d'intégrer les transferts de données et de la voix sur les mêmes lignes de communication, ainsi que l'utilisation des outils avancés par intermédiaire d'un ordinateur personnel. Avec *YouTube* et les services similaires, l'Internet fait également converger les services de multimédia et les divertissements traditionnels. Alors que la convergence technique progresse à un rythme rapide, ses implications économiques et juridiques exigeront du temps pour évoluer.

### Les enjeux

#### Les implications économiques de la convergence

A un niveau économique, la convergence a commencé à réorganiser les marchés traditionnels en mettant en compétition directe des sociétés qui auparavant fonctionnaient dans les domaines séparés. Les sociétés utilisent

des stratégies différentes. L'approche la plus fréquente est la fusion et l'acquisition. Par exemple, la fusion d'America Online et Time Warner visait à combiner la télécommunication avec les médias/divertissements. Actuellement, AOL/Time Warner a rassemblé les ISP, la télévision, la musique et le développement de logiciel sous le parapluie d'un seul consortium.

### Le besoin d'un cadre juridique

Le système juridique a été le plus lent pour s'ajuster aux changements causés par la convergence technologique et économique. Chaque segment – la télécommunication, la radio diffusion et l'information – a son propre cadre spécial de régulation. Cette convergence ouvre plusieurs questions de gouvernance et de régulation:

- Qu'est ce qui arrivera aux régimes nationaux et internationaux existant dans des domaines comme la téléphonie et la diffusion?
- Les nouveaux régimes seront-ils développés en se focalisant principalement sur l'Internet?
- La régulation de la convergence devrait-elle être conduite par les autorités publiques (organisations internationales et Etats) ou par autorégulation?

Certains pays, comme la Malaisie et la Suisse, aussi bien que ceux de l'UE, ont commencé à donner des réponses à ces questions. La Malaisie a adopté le 'Communication and Multimédia Act' en 1998, établissant un cadre général pour la régulation de la convergence. Les nouvelles directives du cadre de l'UE, maintenant transformées en lois nationales, constituent également un pas dans cette direction, comme c'est le cas des lois et régulations des télécommunications suisses.

### Le danger de convergence: fusion entre opérateurs par câble et ISPs

Dans beaucoup de pays, l'Internet à large bande a été introduit à travers les réseaux de câble. Ceci est surtout vrai pour les Etats Unis où l'Internet par câble est beaucoup plus répandu que l'ADSL (Asymmetric Digital Subscriber Line), l'autre principale option de l'Internet à large bande. Quelles sont les risques associés à cette convergence?

Certaines parties disent que les opérateurs de câbles qui opèrent entre utilisateurs et l'Internet pourraient défier le principe de la neutralité du réseau.

La différence majeure entre ADSL et le câble est que le câble n'est pas régulé par les soi-disantes règles du 'common carrier'. Ces règles, applicables au

système de téléphonie, spécifient que l'accès devrait être non-discriminatoire. Les opérateurs de câble ne sont pas soumis à ces règles, et ont ainsi le contrôle total sur l'accès à l'Internet de leurs abonnés. Ils peuvent bloquer l'utilisation de certaines applications et contrôler l'accès à certains matériels. Les possibilités de surveillance et par conséquent l'aptitude à violer l'intimité sont plus grandes avec l'Internet par câble puisque l'accès est contrôlé à travers un système semblable aux réseaux locaux qui fournissent un haut niveau de contrôle direct des utilisateurs.

Dans un article sur cette question, 'l'Américain Civil Liberties Union' donne l'exemple suivant sur les risques des monopoles de l'internet par câble:

*'Ceci est comme si la société de la téléphonie était autorisée à tenir des restaurants qui fournirait de bons services et des signaux efficace aux clients qui appellent Dominos et par contre des signaux souvent occupés, déconnectés et garderaient bloqués ceux qui appellent Pizza Hut.'*<sup>54</sup>

Ce problème de convergence sera résolu quand une décision sera prise, à savoir si l'internet par câble est 'un service d'information' ou un service de télécommunication. Si cette dernière option est prise, il devra être régulé à travers les règles du 'common carrier'.

## La cyber sécurité

### La situation actuelle

L'Internet était à l'origine conçu pour être utilisé par un cercle fermé, principalement des universitaires sans préoccupation concernant la sécurité. Ils communiquaient ouvertement et évoquaient les probables problèmes de sécurité de façon informelle.

La cyber sécurité a ravi la vedette du débat avec l'expansion rapide de la base des utilisateurs de l'Internet. L'Internet a réitéré le vieux paradoxe selon lequel la technologie peut être à la fois facilitatrice et obstacle en même temps. Ce qui peut être utilisé en faveur du bien être de la société peut aussi l'être à son désavantage.

Une des conséquences de l'intégration rapide de l'Internet dans presque tous les aspects de l'activité humaine est une vulnérabilité accrue de la société moderne. L'Internet est une partie de l'infrastructure critique globale. D'autres services au cœur de la société moderne tels que le réseau électrique,

les systèmes de transport et les services de santé dépendent de plus en plus de l'Internet. Ils sont des cibles fréquentes de cyber-attaques.

Les problèmes de cyber sécurité peuvent être classés en trois catégories:

- 1 **Le type d'action.** La classification basée sur le type d'action peut inclure l'interception des données, l'interférence des données, l'accès illégal, le spyware, la corruption des données, le sabotage, le déni de service et le vol d'identité.
- 2 **Le type d'auteurs.** Les malfaiteurs pourraient inclure les pirates, les cybercriminels, les cyber-guerriers et les cyber-terroristes.
- 3 **Le type de cible.** Les cibles potentielles sont nombreuses peuvent inclure des individus, des sociétés privées, et des institutions publiques aux infrastructures critiques, les gouvernements et les installations militaires.

### Les initiatives politiques pour la cyber sécurité

Beaucoup d'initiatives générales, régionales et nationales se focalisent sur la cyber sécurité. Au niveau national, un nombre croissant de juridictions et de jurisprudence traite de la cyber sécurité. Les initiatives juridiques les plus importantes sont celles des États Unies et sont liées à la lutte contre le terrorisme où le 'Department of Homeland Security' est la principale institution en charge des problèmes de cyber sécurité. Il est difficile de trouver un pays développé sans aucune initiative sur la cyber sécurité.

Au niveau international, l'UIT est l'organisation la plus active ; elle a produit un grand nombre de cadres de sécurité, des architectures, et des standards, y compris X.509, qui fournit la base pour l'infrastructure à clé publique (Public Key Infrastructure – PKI) utilisée, par exemple, dans la version sécurisée du HTTP(s) (Protocole de transfert hypertexte (sécurisé)). Récemment, l'UIT est allée au-delà des aspects strictement techniques et a lancé l'agenda global de cyber sécurité de l'UIT.<sup>55</sup> Cette initiative englobe les mesures juridiques, la coopération politique, et le renforcement des capacités.

Le G8 a également quelques initiatives dans le domaine de la cyber sécurité conçues pour améliorer la coopération entre les agences de mise en exécution de la loi. Il a formé un sous-groupe sur le crime par la haute technologie pour établir une communication 24/7 entre les centres de cyber sécurité des états membres, la formation du *staff*, et l'amélioration des systèmes légaux des états pour combattre la cybercriminalité et promouvoir une coopération entre l'industrie des TIC et les agences d'exécution de la loi.

L'Assemblée Générale des Nations Unies a voté plusieurs résolutions sur une base annuelle et sur les 'développements dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale', spécialement les résolutions 53/70(1998), 54/49(1999), 55/28(2000), 56/19(2001), 57/239(2002) et 58/199(2003). Depuis 1998, toutes les résolutions subséquentes ont un contenu similaire, sans améliorations significatives.

En dehors de ces résolutions de routine, la principale percée était le récent établissement des recommandations pour les négociations du traité sur la cyber sécurité, qui était soumis au Secrétaire général des Nations Unies par quinze Etats membres, y compris tous les membres permanents du Conseil de Sécurité des Nations Unies.

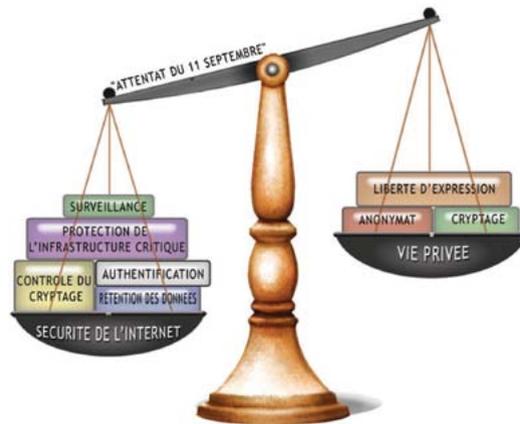
Comme instrument juridique international majeur lié à la cyber sécurité, l'on peut citer la Convention du Conseil de l'Europe sur la cyber sécurité qui entra en vigueur le 1<sup>er</sup> juillet 2004.<sup>56</sup> Certains pays ont établi des accords bilatéraux; par exemple, les Etats Unis ont signé des accords bilatéraux sur la coopération juridique en matière criminelle avec plus de 20 pays.<sup>57</sup> Ces accords s'appliquent aussi aux cas de cybercriminalité.

Comme tentative initiée par les universitaires et acteurs non-étatiques pour ébaucher un accord international, l'on peut mentionner le 'Stanford Draft Convention on Protection from Cyber Crime and Terrorism'. Ce projet recommande l'établissement d'une structure internationale: l'Agence pour la protection de l'infrastructure de l'information (Agency for Information Infrastructure Protection – AIIP).

## Les enjeux

### L'influence de l'architecture de l'Internet sur la cyber sécurité

La nature même de son organisation affecte la sécurité de l'Internet. Pourrions-nous garder l'approche actuelle qui consiste à bâtir l'Internet sur une base non-sécurisée ou modifier la base de l'infrastructure de l'Internet? Comment un tel changement affecterait-il d'autres caractéristiques de l'Internet, spécialement son caractère ouvert et sa transparence? La plupart des développements passés des standards de l'Internet visaient à améliorer la performance ou à introduire de nouvelles applications; la sécurité n'était pas une priorité.



Il n'est pas évident que l'IETF sera capable de changer les standards des e-mails pour fournir l'authentification appropriée, et en fin de compte, réduire les abus sur l'Internet (exemple: le pollupostage, le cyber crime). Etant donné la controverse autour des changements sur les fondements des standards d'Internet, il est probable que les améliorations liées à la sécurité dans les fondements du protocole Internet seront graduelles et lentes.

### Le futur développement du commerce en ligne exige un niveau élevé de cyber sécurité

La cyber sécurité est souvent mentionnée comme l'un des préalables pour la croissance rapide du commerce électronique. Sans un Internet sûr, les clients seront hésitants à fournir des informations confidentielles en ligne, telles que les numéros de carte de crédit. Il en est de même pour les services bancaires en ligne et l'usage de la monnaie électronique. Si la cyber sécurité générale ne s'améliore que lentement (avec, par exemple, un manque de standards), il est probable que le secteur des affaires fasse pression pour qu'il y ait des développements plus rapides. Cela peut conduire vers plus de défis dans le cadre du principe de la neutralité du réseau et le développement d'un 'nouvel Internet', qui faciliterait notamment, la sécurisation de la communication sur Internet.

### Le respect de la vie privée et la cyber sécurité

Un autre problème débattu est la relation entre la sécurité et le respect de la vie privée. Les mesures additionnelles de la cyber sécurité impliqueront-elles une certaine érosion dans le respect des droits à la vie privée? Quelle régulation s'appliquerait aux logiciels de cryptage, qui peuvent être utilisés à la fois pour la protection légitime de la communication privée et pour la protection des communications des terroristes et des criminels? Les réponses

à ces questions ainsi qu'à d'autres dépendent de l'équilibre, qui change constamment, entre la cyber sécurité et le respect de la vie privée.

Aussitôt après l'attaque terroriste à New York, en septembre 2001, la sécurité est devenue une priorité, et cela s'est reflété par l'adoption de plusieurs lois nationales qui stipulaient entre autre, des niveaux plus élevés de surveillance de l'Internet. La réaction de la société civile s'est centrée sur les dangers concernant le respect de la vie privée et sur le concept de la liberté d'expression.

Au niveau international, la question d'équilibre entre la cyber sécurité et la protection de la vie privée a été au centre des discussions sur l'extension de la Convention du Conseil de l'Europe sur le cyber crime au niveau global. La principale objection des activistes des droits de l'Homme est que la Convention traite des questions de cyber sécurité au détriment de la protection de la vie privée et d'autres droits humains.

## **Le cryptage**

Un des points au centre du débat sur la sécurité de l'Internet concerne le cryptage, qui a trait aux outils qui peuvent être utilisés pour la protection des échanges de données.

Un logiciel de cryptage brouille la communication électronique (e-mail, images) en texte illisible en utilisant des algorithmes mathématiques. L'équilibre entre le besoin de garder certaines informations confidentielles et le besoin des gouvernements de surveiller l'activité terroriste et potentiellement criminelle demeure un problème.

Les aspects internationaux de la politique du cryptage sont pertinents dans la discussion sur la Gouvernance de l'internet étant donné que la régulation du cryptage devrait être internationale, ou du moins, impliquer les pays capables de produire des outils de cryptage.

Ainsi par exemple, la politique des Etats Unis sur le contrôle de l'exportation de logiciels de cryptage n'avait guère bien réussi car elle ne contrôlait pas la distribution internationale de logiciels de chiffrement. Les éditeurs américains de ces logiciels ont initié une forte campagne de pression soutenant que les contrôles à l'exportation ne renforcent pas la sécurité nationale mais plutôt minent les intérêts du commerce américain.

### Régimes internationaux concernant les outils de cryptage

Le cryptage a été abordé dans deux contextes: l'engagement de Wassenaar et l'OCDE. L'engagement de Wassenaar est un régime international adopté par 33 pays industrialisés pour restreindre l'exportation des armes conventionnelles et les technologies à 'double usage' aux pays en guerre ou jugés être des 'Etats paria'. L'accord a mis en place un Secrétariat à Vienne. Le lobbying des Etats Unis, avec le groupe Wassenaar, visait à étendre l'*approche 'Clipper'*<sup>58</sup> au plan international, en contrôlant les logiciels de cryptage au moyen d'un système de tierce confiance. Cela engendra la résistance de nombreux pays, notamment le Japon et les pays scandinaves.

Un compromis fut trouvé en 1998 par l'introduction des directives de cryptographie, qui comprenaient la liste de contrôle à double-usage de produits – machines et logiciels – de cryptographie de plus de 56 bits. Cette extension comprenant des outils Internet tels que les navigateurs-web et l'e-mail. Il est intéressant de noter que cet accord ne couvre pas les transferts 'intangibles', comme les téléchargements. L'échec de l'adoption d'une version internationale de 'clipper' a contribué au retrait de cette proposition au sein des Etats Unis mêmes. Dans cet exemple de corrélation entre les arènes nationales et internationales, les développements internationaux ont eu un impact décisif sur l'évolution nationale.

L'OCDE est un autre forum pour la coopération internationale dans le domaine du cryptage. Quoique l'OCDE ne produise pas de documents juridiques ayant force de loi, ses directives sur des questions variées sont hautement respectées. Elles sont le résultat d'une approche d'experts et d'un processus de prise de décision basé sur le consensus. La plupart de ses directives sont éventuellement incorporées dans les lois nationales. La question du cryptage fut un sujet hautement controversée au cours des travaux de l'OCDE. Elle a été initiée en 1996 suite à une proposition américaine prônant l'adoption d'un système à tiers de confiance en guise de norme internationale. Comme dans le cas de Wassenaar, les négociations sur la proposition américaine firent l'objet d'une forte opposition du Japon et des pays scandinaves. Les pourparlers débouchèrent sur un compromis de spécification concernant les principaux éléments de la politique de cryptage.

Ces quelques tentatives pour développer un régime international de cryptage, principalement dans le contexte de l'Arrangement de Wassenaar n'a pas abouti au développement d'un régime international effectif. Il est encore possible d'obtenir un puissant logiciel de cryptage sur Internet.

## Pollupostage et 'mode politique'

Le pollupostage est un exemple flagrant des tendances et parfois de mode en matière d'orientation de politique générale. En 2005, le pollupostage était listé comme un problème significatif de Gouvernance de l'Internet dans le rapport du GTGI. Le spam était discuté lors du SMSI de Tunis et lors de nombreuses rencontres internationales. Il était aussi souvent à la une des médias.

Depuis 2005, le volume du pollupostage a augmenté de six fois, selon les estimations (2005: 30 milliards de messages par jour ; 2010: 183 milliards de messages par jour).

L'importance politique du pollupostage ne suit pas sa tendance. Le pollupostage a actuellement une très faible visibilité dans les processus de politique générale. Au FGI de 2009 à Sharm El Sheikh, il n'y avait aucun atelier ou session pour discuter du pollupostage. Toutefois, l'importance du pollupostage dans la politique globale reste encore à découvrir.

## Pollupostage

### La situation actuelle

Le pollupostage est souvent défini comme du courrier électronique non sollicité qui est envoyé à un grand nombre d'utilisateurs d'Internet. Tandis qu'il est principalement utilisé pour la promotion commerciale, ses autres usages incluent l'activisme social, la campagne politique et la distribution de matériels pornographiques. Le pollupostage est classé dans la corbeille infrastructure parce qu'il affecte le fonctionnement normal de l'Internet en empêchant le bon fonctionnement de l'une de ces applications centrales: le courrier électronique. Le pollupostage est l'un des problèmes de la Gouvernance de l'Internet qui affecte presque tout individu qui s'y connecte. Selon les statistiques de 2009, 81 % du trafic des messages électroniques étaient du pollupostage. Le volume du pollupostage entre 2008 et 2009 a augmenté de 24 %. En plus du fait qu'il soit ennuyeux pour les utilisateurs, le pollupostage cause aussi des pertes économiques considérables, à la fois en terme de bande passante utilisée et en terme de temps perdu pour sa vérification et sa suppression.



Le pollupostage peut être combattu à la fois à travers les moyens juridiques et techniques. Du point de vue technique, beaucoup d'applications pour filtrer les messages et détecter le pollupostage sont disponibles. Le problème fondamental avec les systèmes de filtrage est qu'ils sont connus pour également supprimer des messages non indésirables. L'industrie anti-pollupostage est un secteur en pleine croissance avec de plus en plus d'applications sophistiquées capables de distinguer les messages indésirables des messages réguliers. Les méthodes techniques n'ont qu'un effet limité et exigent les mesures juridiques complémentaires.

Sur le plan technique, beaucoup d'États-nations ont réagi en produisant de nouvelles lois anti-pollupostage. Aux États Unis, la loi 'Can-spam' tient compte d'un équilibre délicat entre, permettre la promotion basée sur le courrier électronique et la lutte contre le spam.<sup>59</sup> Bien que la loi prescrive les sanctions sévères pour la distribution de courriers indésirables, y compris l'emprisonnement pendant des années, certaines de ses dispositions, selon des critiques, tolèrent ou pourraient même encourager l'activité du pollupostage. Le point de départ 'par défaut' tel qu'énoncé dans la loi est que le pollupostage est permis jusqu'à ce que le réceptionneur des messages indésirables dise 'non' par intermédiaire d'une clause d'exclusion. Depuis l'adoption de la loi en décembre 2003, les statistiques n'ont pas mis en évidence une quelconque décroissance du nombre de messages indésirables.

En juillet 2003, l'UE a introduit sa propre législation anti-pollupostage comme faisant partie de sa Directive sur la vie privée et des communications électroniques. La loi de l'UE encourage l'autorégulation et les initiatives du secteur privé qui conduiraient à une réduction des courriers électroniques indésirables.<sup>60</sup>

En novembre 2006, la Commission Européenne a adopté sa Communication pour combattre le pollupostage, le *logiciel espion* et le logiciel malicieux. La Communication identifie un nombre d'actions pour promouvoir l'application de la loi existante comme souligné plus haut, étant donné que la non-exécution est considérée comme le problème majeur.<sup>61</sup>

### La réponse internationale

Les deux lois anti-pollupostage adoptées aux États Unis et dans l'UE ont une faiblesse: le manque de dispositions pour empêcher le pollupostage transfrontalier. Cette question est particulièrement pertinente dans certains pays tels que le Canada, qui, selon les dernières statistiques, reçoit 19 sur 20 des courriers indésirables depuis l'étranger.

La Ministre canadienne de l'industrie, Lucienne Robillard a dit que le problème ne peut pas être résolu sur une base 'pays-pays'. Une solution globale est nécessaire, renforcée à travers un traité international ou un mécanisme similaire.

Un Mémoire d'Entente signé par l'Australie, la Corée et le Royaume Uni est l'un des premiers exemples de la coopération internationale dans la campagne anti-pollupostage.

L'OCDE a établi un groupe de travail sur le pollupostage et a préparé une boîte à outil anti-pollupostage. L'UIT a également été proactive en organisant la rencontre thématique sur la lutte contre le pollupostage (2004) dans le but d'explorer les différentes possibilités d'établissement d'un Mémoire d'entente global pour combattre le pollupostage. Au niveau régional, l'UE a établi le réseau d'agences de lutte anti-pollupostage, l'APEC a préparé un dispositif de directives pour le consommateur.

Une autre approche possible d'anti-pollupostage a été entreprise par les grands groupes Internet qui hébergent les comptes de courrier électronique: American online, British Telecom, Comcast Earth Link, Microsoft et Yahoo ! Elles avaient établi l'Alliance technique anti-pollupostage (Anti-Spam Technical Alliance – ASTA) qui aurait pour tâche principale de coordonner les activités techniques et celles relatives à la politique anti-pollupostage.

## Les enjeux

### Les différentes définitions du pollupostage

Les différentes définitions du pollupostage affectent la campagne anti-pollupostage. Aux Etats Unis, une préoccupation générale au sujet de la protection de la liberté d'expression et du Premier Amendement affecte également la campagne anti pollupostage. Les législateurs américains considèrent comme pollupostage un courrier électronique commercial uniquement non sollicité, oubliant d'autres types de courriers indésirables qui comprennent l'activisme politique et la pornographie. Dans la plupart des autres pays, le pollupostage est considéré comme étant tout courrier électronique non sollicité en grande quantité quelque soit son contenu. Puisque la majeure partie des courriers électroniques indésirables sont produits aux Etats Unis, cette différence dans les définitions limite sérieusement toute possibilité d'introduire un mécanisme international effectif d'anti-pollupostage.

### **Le pollupostage et l'authentification du courrier électronique**

L'un des facteurs structurels favorisant le pollupostage est la possibilité d'envoyer des courriers électroniques avec une adresse d'expéditeur falsifiée. Il existe une solution technique à ce problème qui exigerait des changements dans les standards existants du courrier électronique sur l'Internet. L'IETF travaille à apporter les changements au protocole du courrier électronique qui assureraient l'authentification du courrier électronique. Ceci est un exemple de la manière dont les problèmes techniques peuvent affecter la politique. Un compromis possible serait que l'introduction de l'authentification du courrier électronique apporterait la restriction de l'anonymat sur l'Internet.

### **Le besoin d'une action globale**

La plupart des courriers électroniques indésirables envoyés vers un pays donné proviennent de l'étranger. C'est un problème mondial qui exige une solution mondiale. Il y a plusieurs initiatives qui pourraient conduire à une meilleure coopération globale. Certaines d'entre elles telles que les Mémoires d'entente bilatéraux ont déjà été mentionnés. D'autres incluent certaines actions comme le renforcement des capacités et l'échange d'informations. Une solution plus intégrée impliquerait une sorte d'instrument anti-pollupostage mondial. Jusqu'à présent, les pays développés préfèrent le renforcement des lois nationales couplées aux campagnes anti-pollupostage régionales ou bilatérales. Etant donné leur position défavorisée de recevoir un, 'mal public universel' provenant principalement des pays développés, la plupart des pays en développement sont intéressés à la formulation d'une réponse globale au problème du pollupostage.

## Notes de fin

- <sup>1</sup> Les termes ' Internet ' et toile d'araignée mondiale (World Wide Web) sont parfois utilisés de façon interchangeable; cependant, il ya une différence. L'Internet est un vaste réseau des réseaux; il couvre un nombre de services différents. Parfois le terme Internet est utilisé de manière globalisante, comprenant l'infrastructure, les applications (courrier électronique, ftp, la Toile) et le contenu. La toile d'araignée mondiale est juste l'une des nombreuses applications de l'internet, un système de documents liés et connectés à l'aide du protocole ' Hyper Text Transfer Protocol (HTTP) '.
- <sup>2</sup> La transmission de l'Internet à travers un réseau électrique est appelé Courant Porteur en Ligne. L'usage du réseau électrique rendrait l'Internet plus accessible à beaucoup d'utilisateurs. Pour une révision technique et organisationnelle de cette fonction, voir: Internet Society (2003) *Addressing the digital divide with IPv6-enabled broadband power line communications (Résoudre la fracture numérique par la technologie des connexions Internet haut débit utilisant le courant porteur en ligne avec le protocole IPv6* . ISOC Member Briefing No. 13. Disponible sur: <http://www.isoc.org/briefings/013/>
- <sup>3</sup> La libéralisation des marchés de télécommunication dans les pays membres de l'OMC a été rendue formelle en 1998 dans le ' Basic Telecommunication Agreement (BTA) ' . Après l'adoption du BTA, 100 pays ont commencé le processus de libéralisation, caractérisé par la privatisation des sociétés nationales de télécommunication qui avaient le monopole dans le domaine, l'introduction de la concurrence et l'établissement des régulateurs nationaux. L'accord est formellement appelé le ' The Fourth Protocol to the General Agreement on Trade in Services ' adoptés le 30 Avril 1996 et entré en vigueur le 5 février 1998. Disponible sur [www.wto.org/english/tratop\\_e/serv\\_e/4prote\\_e.htm](http://www.wto.org/english/tratop_e/serv_e/4prote_e.htm)
- <sup>4</sup> Pour plus d'information sur le rôle de l'OMC dans le domaine des télécommunications, voir: [http://www.wto.org/english/tratop\\_e/serv\\_e/telecom\\_e/telecom\\_e.htm](http://www.wto.org/english/tratop_e/serv_e/telecom_e/telecom_e.htm)
- <sup>5</sup> L'opinion commune est que les Etats peuvent collecter plus de recettes à partir du monopole du marché par les opérateurs nationaux ; les adversaires soutiennent qu'avec la libéralisation du marché, la valeur totale du marché a augmenté, apportant par conséquent plus de revenus à l'Etat par rapport à la situation du monopole.
- <sup>6</sup> Actuellement, les RIR sont l'ARIN (le registre américain des nombres d'Internet), l'APNIC (le réseau du centre d'information Asie -Pacifique), LACNIC (le registre régional de l'Amérique Latine et des Caraïbes pour les adresses IP), RIPE NCC (le centre de coordination du réseau des réseaux IP européens- couvrant l'Europe et le Moyen orient), et l'AFRINIC (le centre d'information du réseau africain). Une explication détaillée du système RIR est disponible à: <https://www.ripe.net/info/resource-admin/rir-system.html>
- <sup>7</sup> Pour un débat détaillé à propos de l'IPv6, voir: Kissangou JP, Guthrie M, Njiraini M (2005) *allocation des IPv4 et IPv6, dans le cadre du programme de renforcement de capacité de la GI*. Disponible sur: <http://textus.diplomacy.edu/Textusbin/portal/Ghome.asp?IDspace=84>
- <sup>8</sup> Pour une étude hautement technique et complète sur la sécurité du TCP/IP, voir: Chambers C, Dolske J, lyre J (ND) *TCP/IP Security, Department of Computer and Information Science, Ohio State University: Columbus, OH, USA*. Disponible sur: [http://www.linuxsecurity.com/resource\\_les/documentation/tcpip-security.html](http://www.linuxsecurity.com/resource_les/documentation/tcpip-security.html)
- <sup>9</sup> Abbate J (1999) *Inventing the Internet*. MIT Press: Cambridge, MA, USA.

- 10 Une vue d'ensemble des gTLD avec un lien à la liste de tous les TLDS est disponible sur: <http://www.icann.org/registries/about.htm>
- 11 Un exemple antérieur des domaines liés au contenu concernant les enfants est le domaine kids.us. Le Congrès des Etats-Unis d'Amérique a adopté une loi introduisant le domaine réservé au contenu convivial pour enfant. La principale difficulté avec cette proposition est de décider sur ce qui constitue le contenu convivial pour l'enfant. Une controverse conceptuelle et des problèmes pratiques liés au contrôle du contenu pourraient en résulter. Jusque-là, le domaine 'kids' n'a été utilisé que comme une partie du domaine américain.
- 12 Le gouvernement des Etats-Unis n'a pas suivi les procédures de prise de décision de l'ICANN pendant les discussions sur le domaine xxx. L'opposition des Etats-Unis s'est exprimée à travers une lettre envoyée par le ministre du commerce américain au Président d'ICANN.
- 13 Le formulaire d'enregistrement du domaine .cat est disponible sur: <http://www.icann.org/tlds/stdl-apps-19mar04/cat.htm>
- 14 Le rapport de l'IANA sur le ccTLD pour la Palestine est disponible sur: <http://www.iana.org/reports/ps-report-22mar00.htm>
- 15 Par exemple, l'Afrique du Sud a utilisé ses droits souverains comme un argument pour reprendre le contrôle de son domaine national. Une loi nouvellement promulguée spécifie que l'utilisation du domaine national hors des paramètres prescrits par le gouvernement Sud-Africain serait considéré comme un crime. Le modèle brésilien de gestion des domaines nationaux est souvent été montré comme un exemple réussi d'une approche multi parties-prenantes. Le corps national en charge des domaines brésiliens est ouvert à tous les protagonistes-clés, y compris les autorités gouvernementales, le secteur privé, et la société civile. Le transfert cambodgien de la gestion du domaine national du contrôle non gouvernemental au contrôle gouvernemental est souvent cité comme un exemple de transition échouée. Le gouvernement avait réduit la qualité des services et introduit des frais plus élevés qui ont rendu l'enregistrement des domaines cambodgiens beaucoup plus difficiles. Pour plus d'information, voir: Alfonso CA (2004) *BR: CCTLD An asset of the commons*, in *Internet Governance: A grand collaboration*. MacLean D (ed.). UNICT Task Force: New York, NY, USA, pp. 291–299; Klein N (2004) Internet governance: Perspectives from Cambodia, in *Internet Governance: A grand collaboration. op. cit.*
- 16 ICANN (2000) *Principles for the Delegation and Administration of Country Code Top-Level Domains*, currently being redrafted. Available at: <http://www.icann.org/committees/gac/gac-cctldprinciples-23feb00.htm>
- 17 La liste des serveurs racines de zone, leurs nœuds et positions, ainsi que les organisations en charge de leur gestion est disponible sur: <http://www.root-servers.org/>
- 18 ICANN (2009) Available at <http://www.icann.org/en/announcements/announcement-30sep09-en.htm>
- 19 La section sur la neutralité du serveur est basée sur les écrits de Vladimir Radunovic, coordonateur du projet sur la Gouvernance de l'Internet de DiploFoundation.
- 20 Durant toute l'histoire de l'Internet, les Etats-Unis n'ont jamais bloqué l'accès à un autre pays y compris les pays en conflit. Dans certains cas, comme durant la guerre du Kosovo de 1999, le régime des sanctions des NU donnait aux Etats-Unis le droit de rompre les communications avec la Serbie. N'ayant pas utilisé cette possibilité légale, ainsi la Serbie a gardé l'accès à l'Internet durant tout le conflit.

- <sup>21</sup> Arrington M (2009) You tube vidéo diffuse un maximum de 1,2 milliards de vidéo par jour. TechCrunch. Disponible à: <http://www.techcrunch.com/2009/06/09/youtume-strime-video-top-1-billionday/>
- <sup>22</sup> Faire la diffusion nous-même. Le bureau du blogue de YouTube (2009) Zoinks! 20 heures de vidéo mises en ligne chaque minute! Disponible sur: [http://youtube-global.blogspot.com/2009/05/zoinks-20-hours-of-video-uploaded-every\\_20.html](http://youtube-global.blogspot.com/2009/05/zoinks-20-hours-of-video-uploaded-every_20.html)
- <sup>23</sup> L'Amérique insiste sur la neutralité du net: The right of bits. *The Economist* 24 September 2009.
- <sup>24</sup> Ce cas a connu plusieurs bouleversements. Pour plus d'information sur l'historique de ce cas, voir: Broache A (2008) FCC veut savoir: le fait de dégrader le trafic Pair à Pair est-il raisonnable? Cent News Blog. Disponible sur [http://news.cnet.com/8301-10784\\_3-9850611-7.html?tag=mncol;txt](http://news.cnet.com/8301-10784_3-9850611-7.html?tag=mncol;txt)
- La mise à jour la plus récente fut la décision de la cour contre la réglementation antérieure de FCC, voir Kang C (2010), Court rules for Comcast over FCC in 'net neutrality' case. Le Washington Post, 7 avril. Disponible sur <http://www.washingtonpost.com/wp-dyn/content/article/2010/04/06/AR2010040600742.html>
- <sup>25</sup> ' Save the Internet ' est particulièrement actif en recommandant la neutralité du réseau comme moyen de préserver l'ouverture et la liberté sur l'Internet.
- <sup>26</sup> L' 'Internet Governance Caucus (IGC)' était à l'origine créé par les acteurs individuels et des organisations de la société civile qui se mirent ensemble dans le contexte du SMSI pour promouvoir les objectifs de l'intérêt public général dans la mise en place de la Gouvernance de l'Internet. Disponible sur: [www.igcaucus.org](http://www.igcaucus.org)
- <sup>27</sup> John Herman illustre les offres de packages souvent utilisés par les protagonistes de la neutralité du réseau. Disponible sur: <http://gizmodo.com/5391712/net-neutrality-worst-case>
- <sup>28</sup> La *quadrature du Net*, un groupe de défense qui fait la promotion des droits et libertés des citoyens sur l'internet, affirme dans sa lettre ouverte au parlement européen concernant la neutralité du réseau: *Everyone around the globe has access to the same Internet, and even the smallest entrepreneurs are on equal footing with the leading global enterprises (toute personne sur la terre a accès au même et unique Internet, et donc même le plus petit entrepreneur est sur le même pied d'égalité que les grands groupes mondiaux)*. Disponible sur: <http://www.laquadrature.net/en/we-must-protect-net-neutrality-in-europe-openletter-to-the-european-parliament#>
- <sup>29</sup> Ogg E (2010) *Report: Google, Verizon reach Net neutrality deal*. CNet 4 August. Disponible sur: [http://news.cnet.com/8301-31021\\_3-20012703-260.html?tag=mncol;mlt\\_related](http://news.cnet.com/8301-31021_3-20012703-260.html?tag=mncol;mlt_related)
- <sup>30</sup> Ces éléments qui sont encore controversés et négociés dans l'avenir sont entre parenthèses.
- <sup>31</sup> Les rapports de ces réunions aussi bien que d'autres éléments pertinents sur la neutralité du réseau, sont disponibles sur: [www.diplomacy.edu/ig/nn](http://www.diplomacy.edu/ig/nn)
- <sup>32</sup> Le journal de la politique de (FCC 2005) sur la gestion et la neutralité du réseau. Disponible sur: [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/FCC-05-151A1.pdf](http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf)
- <sup>33</sup> Ministère de l'intérieur et des communications, Japon (2007), Rapport sur la neutralité du réseau. Disponible sur: [www.soumu.go.jp/main\\_sosiki/joho\\_tsusin/eng/pdf/070900\\_1.pdf](http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pdf/070900_1.pdf)

- <sup>34</sup> PTS (2009) *Open Networks and Services*. Disponible sur: <http://www.pts.se/en-gb/Documents/Reports/Internet/2009/Open-Networks-and-Services---PTS-ER-200932/>
- <sup>35</sup> Kroes N (2010) *Net neutrality in Europe*. Discours prononcé par le Vice Président de la Commission Européenne pour l'Agenda Numérique. Disponible sur: <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/153&format=HTML&aged=0&language=EN&guiLanguage=en>
- <sup>36</sup> NPT (2009) *Net neutrality: Guidelines for Internet neutrality*. Disponible sur: <http://www.npt.no/ikbViewer/Content/109604/Guidelines%20for%20network%20neutrality.pdf>
- <sup>37</sup> Anderson N (2009) *Norway gets net neutrality – voluntary, but broadly supported. Ars Technica*. Disponible sur: <http://arstechnica.com/tech-policy/news/2009/02/norway-getsvoluntary-net-neutrality.ars>
- <sup>38</sup> ISOC considère le concept de la neutralité du réseau plutôt (comme) mal défini et discute plutôt de l'ouverture et de l'interopérabilité continue des réseaux. Disponible sur: <http://www.isoc.org/pubpolpillar/usercentricity/openinternetworking.shtml>. Sa consultation du 16 mai sur la neutralité du net affirme qu': ' *Au lieu de se focaliser simplement sur une gamme de définitions possibles de la neutralité du réseau, l'Internet Society croit qu'il est plus approprié de se focaliser plus ouvertement sur l'impératif de la préservation d'un modèle d'Internet ouvert, centré sur l'utilisateur, lequel a eu du succès jusqu'à ce jour* ' ( *Rather than focusing simply on the range of possible Network Neutrality definitions, the Internet Society believes it is more appropriate to concentrate more broadly on the imperative of preserving the open, user-centric Internet model that has been so successful to date*). Disponible sur: [http://www.isoc.org/regions/europe/docs/netneutrality\\_20100516\\_en.pdf](http://www.isoc.org/regions/europe/docs/netneutrality_20100516_en.pdf)
- <sup>39</sup> *TACD calls for Net Neutrality*. Disponible sur: [http://tacd.org/index.php?option=com\\_content&task=view&id=162&Itemid=43](http://tacd.org/index.php?option=com_content&task=view&id=162&Itemid=43)
- <sup>40</sup> Williams F (2006) *ISPs should be liable for spam*, souligne le rapport des Nations Unies. *Financial Times*, 8 Novembre. Disponible sur: <http://www.qlinks.net/quicklinks/spam.htm>
- <sup>41</sup> Shannon V (2006) *The end user: Junk payout in spam case. International Herald Tribune*, 13 Avril. Disponible sur: <http://www.iht.com/articles/2006/04/12/business/PTEND13.php>
- <sup>42</sup> Le ' Peering ' est un accord bi- latéral fait par les opérateurs de réseau pour garantir l'accès aux clients des uns et des autres sans coût pour toutes les parties; comme défini par le groupe HSC. ([www.hscgroup.co.uk](http://www.hscgroup.co.uk)). L'arrangement ' Peering ' est un bénéfice mutuel et il est aussi courant chez les FAI que chez les opérateurs de télécom.
- <sup>43</sup> Au niveau 2, se trouve des FBP (Fournisseurs de Bande Passante) généralement appelés Points de Connexion Internet (PCI) ou Passerelles d'Internet.
- <sup>44</sup> Andrew Odlyzko voit la question de fixation de prix et d'architecture sur l'internet dans une perspective historique. Identifiant l'évolution de la politique de fixation de prix pratiquée dans les systèmes de transport dans l'ancien monde, il en fait une liaison avec la politique actuelle de fixation des prix de l'internet. Odlyzko A (2004) *Pricing and architecture of the Internet: Historical perspectives from telecommunications and transportation*. University of Minnesota: Minneapolis, MN, USA. Disponible sur: [http://www.dtc.umn.edu/\\_odlyzko/doc/pricing.architecture.pdf](http://www.dtc.umn.edu/_odlyzko/doc/pricing.architecture.pdf)

- <sup>45</sup> Shawn O'donnell, dans l'article *An economic map of the Internet*, fournit une analyse de comment le dollar de l'internet est distribué, expliquant où va le dollar que le consommateur paye au FAI, disponible sur: [http://ebusiness.mit.edu/research/papers/162\\_ODonnell\\_Map.pdf](http://ebusiness.mit.edu/research/papers/162_ODonnell_Map.pdf)
- <sup>46</sup> Nguyen TT, Armitage GJ (2005) Evaluating Internet pricing schemes: A three-dimensional visual model. *ETRI Journal* 27: 64–74.
- <sup>47</sup> Le site web du marché de la bande passante est un marché en ligne des ressources de l'internet, offrant la bande passante, l'accès à l'Internet et d'autres ressources d'Internet. Disponible sur: <http://www.bandwidthmarket.net/>
- <sup>48</sup> Huston G (2005) 'Where's the money? – Internet interconnection and \_ financial settlements'. The ISP Column, Internet Society. Disponible sur: <http://ispcolumn.isoc.org/2005-01/interconns.pdf>
- <sup>49</sup> AfrISPA (2002) the half way proposition: Un article sur la subvention en sens inverse des pays du G8 par les FAI africains, présenté à la conférence des ministres africains des finances, de la planification et du développement économique, Johannesburg, Afrique du sud, 19 octobre 2002. Disponible sur: [http://www.wougnet.org/WSIS/ug/WSIS2005/docs/HalfwayProposition\\_Draft4.pdf](http://www.wougnet.org/WSIS/ug/WSIS2005/docs/HalfwayProposition_Draft4.pdf)
- <sup>50</sup> Pour une étude complète des coûts d'interconnexion, voir Esmat B., Fernandez J. (2006) 'International Internet Connections Costs', in Drake WJ (2006) *Reforming Internet Governance: Perspectives from the Working Group on Internet Governance* (WGIG). WGIG: New York, NY, USA, pp. 73–86. Disponible sur: <http://www.wgig.org/book-Launch.html>
- <sup>51</sup> Vous pouvez trouver une analyse complète du sujet dans Jensen M (2005) *Interconnection Costs*. APC: Melville, Afrique du Sud. Disponible sur: <http://www.apc.org/en/pubs/issue/accessibility/all/interconnection-costs>
- <sup>52</sup> Huston (2005) *op. cit.* pp. 7-9.
- <sup>53</sup> L'un des obstacles dans la négociation de cette question entre les gouvernements est que la plupart des accords d'interconnexion sont conclus entre les opérateurs de télécommunication privés. Ils sont souvent confidentiels.
- <sup>54</sup> ACLU White paper (ND) *No competition: How monopoly control of the broadband Internet threatens free speech*. ACLU: New York, NY, USA.
- <sup>55</sup> Pour plus d'informations à propos de l'Agenda mondial sur la cyber sécurité de l'UIT, voir: <http://www.itu.int/osg/csd/cybersecurity/gca/>
- <sup>56</sup> Le texte de la convention est disponible sur: <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>
- <sup>57</sup> Le nom officiel de ces instruments est le 'Mutual Legal Assistance in Criminal Matters Treaties' (MLATs): Traités de l'Assistance mutuelle juridique dans le domaine des affaires criminelles.
- <sup>58</sup> L'approche 'Clipper' fut déjà proposée par le gouvernement des Etats-Unis en 1993. Elle reposait sur l'usage de la puce de Clipper qui était supposée être utilisée dans tous les téléphones et autres outils de communication. La puce de Clipper avait une porte arrière qui serait utilisée par les gouvernements pour la surveillance légale. Après une forte opposition des activistes des droits de l'homme et du public en général, le gouvernement des Etats-Unis abandonna cette proposition en 1995. Voir: Denning D (1995) 'The case for

clipper'. *MIT Technology Review*. MIT: Cambridge, MA, USA. Disponible sur: [http://encryption\\_policies.tripod.com/us/denning\\_0795\\_clipper.htm](http://encryption_policies.tripod.com/us/denning_0795_clipper.htm)

- <sup>59</sup> Plus de référence au 'Can-Spam' sont disponibles sur: <http://www.ftc.gov/bcp/edu/pubs/business/e-commerce/bus61.shtm>
- <sup>60</sup> Le 'Contact Network of Spam Enforcement Authorities (CNSA)' a été mis en place en février 2005 par 13 pays de l'UE (France, Autriche, Belgique, Chypre, République Tchèque, Danemark, Grèce, Irlande, Italie, Lituanie, Malte, Royaume-Uni et Espagne). Il vise à promouvoir la coopération entre ces Etats, et la coordination avec les entités qui sont hors de l'UE, telles que l'OCDE et l'UIT.
- <sup>61</sup> Commission Européenne, Société de l'Information (2010). *Unsolicited communication: fighting spam*. Disponible sur: [http://ec.europa.eu/information\\_society/policy/ecommtodays\\_framework/privacy\\_protection/spam/index\\_en.htm](http://ec.europa.eu/information_society/policy/ecommtodays_framework/privacy_protection/spam/index_en.htm)



## Section 2

---

# La corbeille infrastructure et normalisation

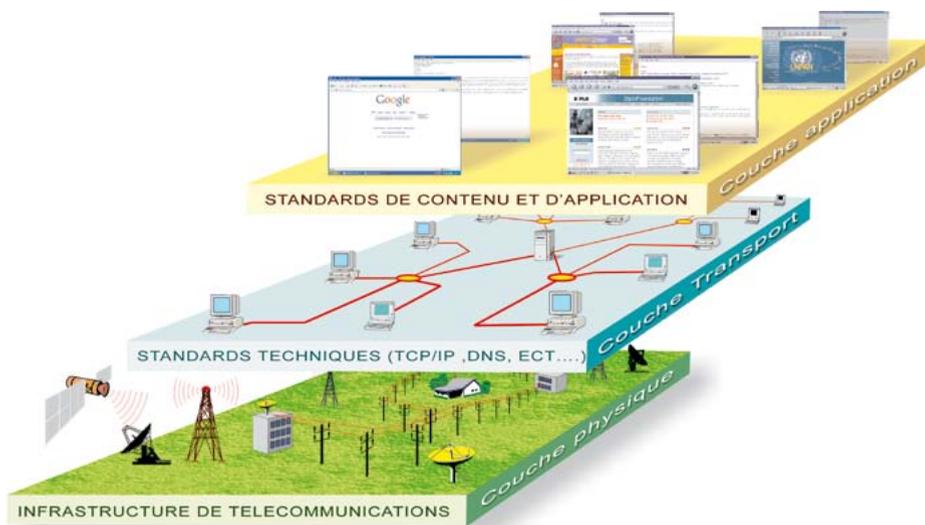




# La corbeille infrastructure et normalisation

La corbeille de l'infrastructure et de la normalisation contient les enjeux élémentaires, essentiellement techniques, liés au fonctionnement de l'Internet. Le principal critère pour placer un enjeu dans cette corbeille est sa pertinence dans le fonctionnement de base de l'Internet. Il ya ici deux groupes d'enjeux.

Le premier groupe se compose des questions essentielles sans lesquelles l'Internet et le World Wide Web ne pourraient pas exister<sup>1</sup>. Ces questions sont regroupées en trois couches:



- 1 l'infrastructure des télécommunications, à travers laquelle circule tout le trafic Internet ;
- 2 les normes (standards) et services techniques de l'Internet, l'infrastructure qui fait fonctionner l'Internet (par exemple TCP/IP: *Transmission Control Protocol/Internet Protocol*; DNS: *Domain Name Services*; SSL: *Secure Sockets Layer*).
- 3 les contenus et les normes régissant les applications (par exemple HTML: *HyperText Markup Language*, XML: *eXtensible Markup Language*).

Le second groupe comprend les questions relatives à la sauvegarde de la sécurité et de la stabilité opérationnelle de l'infrastructure de l'Internet et inclut la cyber sécurité, le cryptage et le pollupostage.

## Les infrastructures de télécommunications

### La situation actuelle

Les données Internet peuvent circuler sur une gamme variée de supports de communication: câble téléphoniques de cuivre, câbles à fibres optiques, satellites, micro-ondes, et des liaisons sans fil. Même le réseau électrique de base peut être utilisé pour relayer le trafic Internet en utilisant la technologie du courant porteur en ligne<sup>2</sup>.

Tenant compte du fait que la couche des télécommunications assure le trafic Internet, toute nouvelle réglementation liée aux télécommunications aura inévitablement un impact sur l'Internet. L'infrastructure de télécommunications est réglementée au niveau national et au niveau international par une variété d'organisations publiques et privées. Parmi les organisations internationales clés impliquées dans la régulation des télécommunications, il y a l'Union internationale des télécommunications (UIT), qui a développé et des règles détaillées pour gérer la relation entre opérateurs nationaux, l'allocation du spectre radio, et la gestion du

### La régulation internationale de l'UIT

La régulation internationale de l'IUT (ITR) de 1998 a facilité la libéralisation internationale de la tarification et des services et a permis une plus grande créativité dans l'usage des services au niveau de l'internet, tel que l'utilisation de lignes internationales louées dans le domaine de l'Internet. Elle a fourni l'une des bases palpable pour la croissance rapide de l'Internet dans les années 1990.

positionnement des satellites; et l'Organisation Mondiale du Commerce (OMC), qui a joué un rôle capital dans la libéralisation des marchés des télécommunications à travers le monde<sup>3</sup>.

Les rôles de l'OMC et l'UIT sont tout à fait différents. L'UIT définit des normes techniques détaillées non contraignantes, les réglementations internationales spécifiques des télécommunications, et fournit une assistance aux pays en développement. L'OMC en revanche offre un cadre pour les règles générales du marché<sup>4</sup>.

La libéralisation des marchés nationaux des télécommunications a donné aux grands groupes de télécommunications telles qu'AT & T, Câble and Wireless, France Telecom, Sprint, et WorldCom, l'opportunité d'étendre leur marché à l'échelle mondiale. Comme une grande partie du trafic Internet est transportée via les infrastructures de télécommunication de ces sociétés, ces dernières ont une influence importante sur le développement de l'Internet.

## Les enjeux

### Le 'dernier kilomètre' – 'la boucle locale'

La 'boucle locale' (ou 'dernier kilomètre') est le nom donné au lien de connexion existant entre les Fournisseurs d'accès Internet (FAI) et leur clients finaux. Les problèmes avec les 'boucles locales' résident dans le fait qu'elles constituent un obstacle à une utilisation plus répandue de l'Internet dans de nombreux pays, particulièrement ceux en développement. La communication sans fils est l'une des solutions peu coûteuse au problème de la boucle locale. En dehors des options techniques de plus en plus accessibles, la solution au problème de la 'boucle locale' dépend également de la libéralisation de ce segment du marché des télécommunications.

### La libéralisation des marchés des télécommunications

Un nombre considérable de pays ont libéralisé leurs marchés des télécommunications. Cependant, beaucoup de pays en développement sont confrontés à un choix difficile: libéraliser et rendre le marché des télécommunications plus efficace, ou préserver une importante source de revenus budgétaires des monopoles de télécommunications existants<sup>5</sup>. L'assistance étrangère, la transition progressive, et le fait de lier le processus de libéralisation à la protection de l'intérêt public pourraient être des voies de sorti de ce dilemme.

### La création de normes techniques d'infrastructure

Les normes techniques sont de plus en plus fixées par les institutions privées et professionnelles. Par exemple, la norme WiFi, IEEE 802.11b, a été développée par 'the Institute of Electric and Electronic Engineers' (IEEE). La certification des équipements WiFi compatibles est faite par l'Alliance WiFi. La fonction même de la création ou de la mise en œuvre des normes dans un marché qui se développe rapidement confère une influence considérable à ces institutions.

## Le 'Transport Control Protocol/ Internet Protocol' (TCP/IP)

### La situation actuelle

Le TCP/IP est la norme technique principale de l'Internet, précisant comment les données sont transférées par Internet, il est basé sur trois principes: commutation des paquets, la mise en réseau de bout en bout et la robustesse. La gouvernance de l'Internet en rapport avec le protocole TCP/IP a deux aspects importants: l'introduction de nouvelles normes et l'attribution des adresses IP.

Les normes TCP/IP sont fixées par l'Internet Engineering Task Force (IETF). Etant donné la pertinence de ces protocoles pour l'Internet, ces derniers sont soigneusement gardés par l'IETF. Toute modification du protocole TCP/IP requiert au préalable une grande discussion et la preuve que la solution en question soit réellement efficace (principe du 'code fonctionnel').

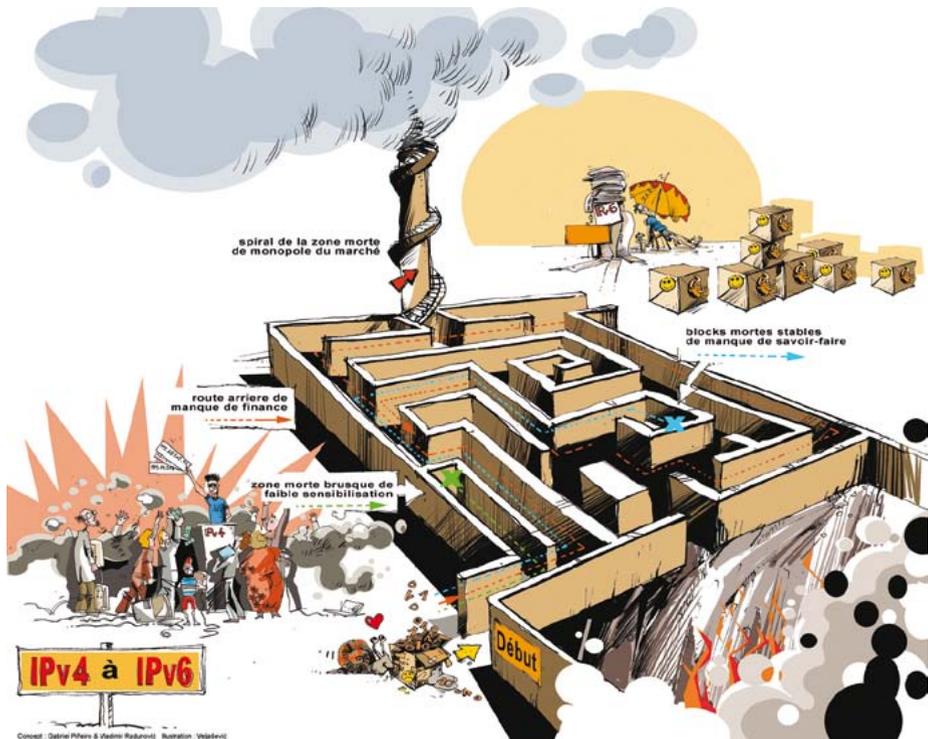
Les adresses IP sont des adresses numériques que tout ordinateur connecté à Internet doit avoir. Les adresses IP sont uniques, deux ordinateurs connectés à l'Internet ne peuvent pas avoir la même adresse IP. Cela fait des adresses IP une ressource potentiellement rare. Le système d'attribution des adresses IP est hiérarchiquement organisé. Au sommet, il y a l'Internet Assigned Numbers Authority (IANA) – une filiale de l'ICANN, qui distribue des blocs d'adresses IP aux cinq Registres internet régionaux (*RIR*)<sup>6</sup>. Les RIR distribuent les adresses IP aux Registres Internet Locaux (Local Internet Registries-LIR) et dans les Registres Internet Nationaux (National Internet Registries-NIRS), qui à leur tour, distribuent les adresses IP aux petits fournisseurs de services Internet, aux entreprises et aux individus au plus bas de l'échelle.

## Les enjeux

### Comment faire face au nombre limité d'adresses IP (Transition vers IPv6)

Le pool actuel des adresses IP sous la forme IPv4 (Internet Protocol, version 4) contient quelque quatre milliards d'adresses et pourrait arriver à épuisement dans quelques années face à l'introduction de gadgets/terminaux-Internet, tels que les téléphones mobiles, les organisateurs personnels, les consoles de jeu, et les appareils ménagers. La préoccupation liée au fait que les adresses IP risqueraient de s'épuiser et inhiberait éventuellement le développement de l'Internet a conduit la communauté technique à prendre les mesures suivantes:

- Rationaliser l'utilisation du pool existant d'adresses IP par le biais de l'introduction du Network Address Translation (NAT);
- Répondre au gaspillage des algorithmes d'attribution d'adresses utilisés par le RIR, en introduisant le routage inter-domaines sans classe (*Classless Inter-Domain Routing*: CIDR);
- Introduire une nouvelle version du protocole TCP/IP – IPv6 – qui prévoit un nombre beaucoup plus élevé d'adresses IP (340,000,000,000,000,000).



La réponse de la communauté Internet au problème du risque de pénurie d'adresses IP est un exemple de gestion rapide et proactive. Bien que le NAT et le CIDR aient fourni une solution rapide au problème, une solution à long terme est la transition vers l'IPv6.

Bien qu'introduit en 1996, le déploiement d'IPv6 a été très lent. Avec l'épuisement prochain du pool d'adresses de l'IPv4 en 2011, la lenteur du déploiement de l'IPv6 renforce les éléments d'une crise en gestation. L'un des principaux défis à relever pour le déploiement de l'IPv6 est le manque de compatibilité entre l'IPv4 et l'IPv6. Les réseaux utilisant l'IPv6 ne peuvent pas communiquer directement avec ceux qui, encore en nombre dominant aujourd'hui, utilisent l'IPv4. Comme il est très probable que les réseaux utilisant l'IPv4 et l'IPv6 coexistent à l'avenir, il est important de s'assurer que les nouveaux réseaux – basés sur l'IPv6 – ne restent pas isolés. Une solution technique comprendra un tunnel spécial entre les deux types de réseaux, ce qui entraînera un routage plus complexe sur l'Internet et quelques autres problèmes 'collatéraux'.

Le déploiement est également retardé par le faible intérêt de la part des Fournisseurs d'accès Internet (FAI) et des utilisateurs. Bien qu'ils soient conscients du risque d'épuisement d'adresses IP, ils préfèrent la tactique de 'attendre et voir'. Par exemple, une enquête récente au Japon a montré que si plus de 70% des FAI sont conscients du risque d'épuisement de l'IPv4, seulement 30% d'entre eux se préparent à la transition vers l'IPv6. Dans une telle situation, lorsque la motivation du marché ne peut pas fournir de solution, il y a une pression croissante sur les gouvernements et les autres autorités publiques pour qu'ils jouent un rôle de premier plan dans le pilotage de la transition vers l'IPv6 à travers la sensibilisation sur les risques d'épuisement d'adresses IPv4, et dans le soutien financier pour la transition vers IPv6 et l'utilisation d'IPv6 pour les réseaux des gouvernements.

Étant donné la complexité de la transition vers IPv6, les pays en développement, essentiellement les pays d'Afrique, pourraient être avantagés par le retard pris dans l'acquisition des réseaux et de la possibilité de l'introduction directe des réseaux basés sur IPv6. Dans ce processus, les pays en développement vont avoir besoin d'une assistance technique<sup>7</sup>.

Outre le problème de la transition, le cadre politique pour l'attribution de l'IPv6 a besoin d'une bonne répartition d'adresses IP, exigeant ainsi l'introduction de mécanismes ouverts et concurrentiels de façon à répondre de la manière la plus optimale aux besoins des utilisateurs finaux.

### Les changements dans le protocole TCP/IP et la cybersécurité

À l'origine, la sécurité n'était pas un enjeu majeur pour les développeurs de l'Internet puisqu'à cette époque l'Internet n'était qu'un réseau fermé d'institutions de recherche. Avec l'expansion de l'Internet à plus de deux milliards d'utilisateurs dans le monde et de son importance croissante comme outil commercial, la question de la sécurité fut placée au devant de la scène des problèmes de gouvernance de l'Internet.

Etant donné que l'architecture de l'Internet n'a pas été conçue en ayant à l'esprit la sécurité, incorporer la cyber sécurité de façon intrinsèque nécessite d'apporter des changements substantiels au fondement même de l'Internet, c'est-à-dire au protocole TCP/IP. Le nouveau protocole IPv6 offre certaines améliorations de sécurité, mais ceci reste en deçà d'une solution globale. Cette protection va demander des modifications considérables sur le TCP/IP.<sup>8</sup>

### Les changements dans le protocole TCP/IP et le problème de la bande passante limitée

Afin de faciliter la fourniture de contenus multimédia (par exemple la téléphonie sur Internet, ou vidéo à la demande), il est nécessaire de garantir une qualité de service (Quality of Service – QoS) capable de garantir un niveau minimal de performance. La QoS est particulièrement importante pour les applications sensibles aux délais (temps de réponse), telle que la diffusion d'événements en direct; et il est souvent difficile de la réaliser en raison des contraintes de la bande passante. L'introduction de la QoS peut nécessiter des changements dans le protocole Internet, sans écarter un risque potentiel pour le principe de la neutralité du réseau.

## Le système des noms de domaine (DNS)

### La situation actuelle

Le DNS gère les adresses Internet (telle que [www.google.com](http://www.google.com)) et les convertit en adresses IP (une illustration simplifiée de ce processus est présenté dans le dessin qui suit). Le DNS est constitué de serveurs racine, serveurs de premier niveau (Top-Level Domain – TLD) et un grand nombre de serveurs DNS sont placés à travers le monde. La gestion du DNS a été un des sujets brûlants dans le débat sur la gouvernance de l'internet. L'une des principales controverses concerne l'autorité du gouvernement des États-Unis (via le ministère du Commerce, Department of Commerce – DOC) sur les serveurs racine, le niveau supérieur hiérarchiquement organisé du système du

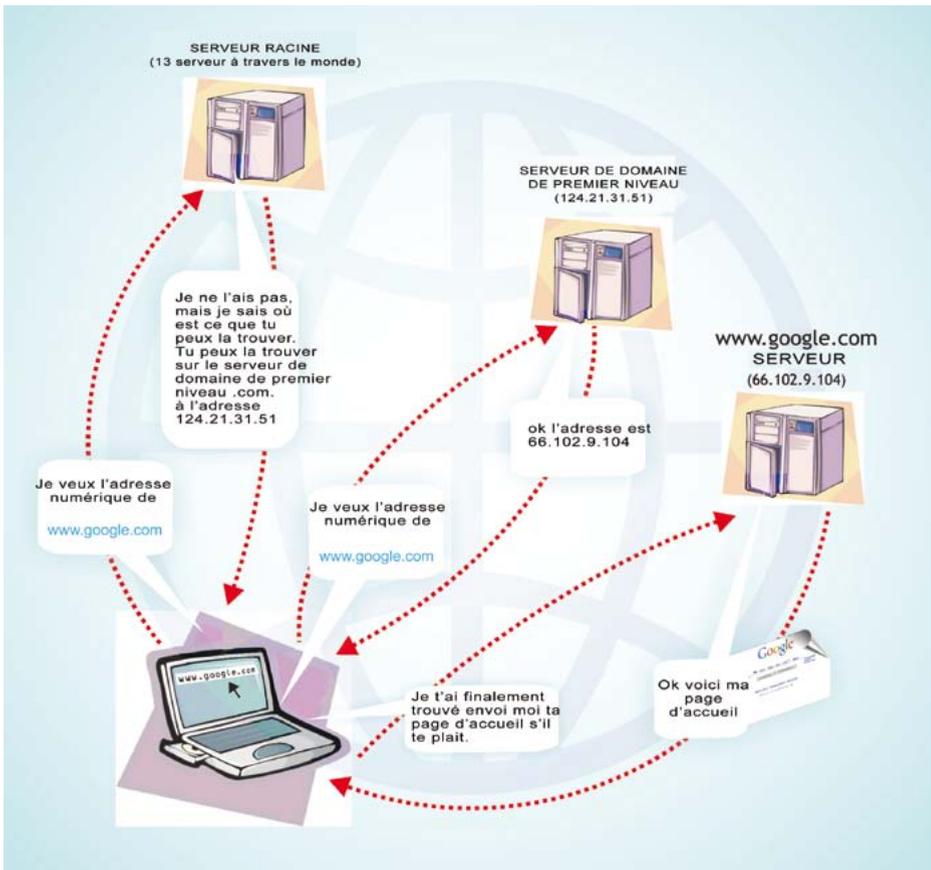
## Technologie, standards, politiques

Le débat sur les protocoles réseau illustre comment les normes peuvent être considérées comme des politiques en ayant une autre perspective. En considérant que l'intervention gouvernementale dans la technologie et les affaires (telle que la régulation de la sécurité et les actions anti-trust) est aisément considérée comme ayant une signification politique et sociale; les normes techniques sont généralement reconnues comme socialement neutres et donc jouissant d'un intérêt historique très faible. Mais les décisions techniques peuvent avoir des conséquences économiques et sociales de grande envergure, changeant l'équilibre des forces entre les entreprises ou les nations en concurrence et rendant contraignante la liberté des utilisateurs. Des efforts pour créer des normes formelles poussent à des décisions techniques privées des constructeurs de systèmes dans le domaine public; de cette façon, les batailles de normes peuvent mettre en lumière des acceptations tacites et des conflits d'intérêt. La grande passion avec laquelle les parties prenantes contestent des décisions sur les normes devrait nous alerter quant à la signification plus profonde sous les écrous et les boulons.<sup>9</sup>

nom de domaine. La situation s'est encore aggravée par le fait que 10 des 13 serveurs racine existants sont aux États-Unis (avec trois autres en Europe et en Asie). Pour résoudre ce problème et améliorer l'évolutivité du système de serveurs racine, le 'régime *Anycast*' a été élaboré, en incluant désormais une centaine de serveurs dans le monde entier et dans tous les continents.

Le DNS est fondé sur trois types de domaines de premier niveau: générique (gTLD), codes pays (ccTLD), et sponsorisés (sTLD). Les gTLD sont des domaines que n'importe qui peut obtenir (.com., .info, .net et .org). Les sTLD sont limités à des groupes spécifiques. Par exemple, les sTLD '.aero' n'ont pas été ouverts à l'enregistrement que pour l'industrie du transport aérien. Les ccTLD sont réservés à des pays spécifiques (.uk, .cn, .in).

Pour chaque domaine générique de premier niveau (gTLD) Il y a un registre qui maintient une liste d'adresses. Par exemple, le gTLD '.com' est géré par VeriSign. La fonction de 'vendeur' est assurée par les registraires. L'ICANN assure la coordination globale du système DNS en concluant des accords avec des registres d'accréditation et d'enregistrement. L'ICANN définit également les prix de gros auxquels le registre (VeriSign) 'loue' les noms de domaine aux bureaux d'enregistrement, et impose des conditions sur les services offerts par le registre ainsi qu'aux structures travaillant avec ce dernier. C'est pour dire que l'ICANN agit en tant que régulateur économique et juridique du *business* des noms de domaine pour les gTLD.



Une partie importante de la gestion du système des noms de domaine est la protection des marques et le règlement des différends. Le principe du 'premier arrivé, premier servi' dans l'attribution des noms de domaine a été utilisé dès les premiers jours où l'Internet a vu se déclencher le phénomène connu sous le nom de *cyber-squatting*, la pratique d'enregistrer des noms de domaine qui sont revendus par la suite. Les politiques uniformes de règlement des litiges *Uniform Disputes Resolution Policy (UDRP)*, développées par l'ICANN et l'Organisation Mondiale de la Propriété Intellectuelle (OMPI) prévoient des mécanismes qui ont considérablement réduit le *cyber-squatting*.

Un autre élément important dans l'enquête sur l'organisation actuelle de la gouvernance du système DNS est la gestion des codes de pays de niveau supérieur (*Top-Level Domains*) (ccTLD). Actuellement, certains codes de pays sont encore gérés par une variété d'institutions ou des personnes qui ont reçu l'accréditation dans les tous premiers jours de l'Internet, lorsque certains gouvernements n'étaient pas tous intéressés à la question.

## Les problèmes

### La création des nouveaux domaines génériques

Techniquement, la création de nouveaux domaines de premier niveau est presque illimitée. Cependant, l'introduction de nouveaux domaines génériques de premier niveau (gTLD) a été très lente, avec un certain nombre de nouveaux TLD génériques introduits que récemment. Actuellement, 20 gTLD sont actifs et trois autres sont à l'étude.<sup>10</sup> La principale opposition à la création de nouveaux TLD génériques provient du secteur privé, dont le souci est que l'augmentation du nombre de domaines compliquerait la protection de leurs marques.

Sous la pression d'introduire de nouveaux gTLD, l'ICANN a entamé des consultations pour concevoir une nouvelle politique dans ce domaine. La nouvelle politique devrait traiter de la manière de résoudre les demandes concurrentes pour les gTLDs, les questions de moralité publique, et les frais d'inscription, entre autres.

### Les contenus en relation avec des noms de domaine génériques

Une autre question politique de l'ICANN est de décider de la création de nouveaux domaines, qui pourrait s'impliquer à relier les noms de domaines aux contenus<sup>11</sup>. Le dernier exemple en date a été la proposition d'introduire le domaine 'xxx' pour les sites web pornographiques. Le conseil d'administration de l'ICANN a rejeté cette proposition en mars 2007. La principale critique de cette décision a été que l'ICANN l'avait fait sous la pression du gouvernement américain, qui est fermement opposé à l'introduction du domaine 'xxx'<sup>12</sup>. Ce qui est intéressant, c'est que de nombreux autres gouvernements ont soutenu le gouvernement des États-Unis, y compris ceux qui sont généralement critiques de la position américaine en matière de gouvernance de l'Internet, comme le Brésil et la Chine. Cette question est revenue à l'ordre du jour en juin 2010 lors de la réunion de l'ICANN à Bruxelles où le Comité directeur de l'ICANN a positivement accepté la candidature pour le domaine .xxx et initia des négociations pour son introduction.

La décision prise par l'ICANN sur le cas 'xxx' a également rouvert le débat sur le rôle de l'ICANN sur les questions de politiques publiques.

### Les noms de domaine génériques pour les communautés culturelles et linguistiques

En 2003, l'ICANN a introduit un nouveau domaine '.cat' pour la langue catalane. Ceci est le premier domaine introduit pour une langue<sup>13</sup>. Le gouvernement espagnol ne s'était pas opposé à cette décision.

Lorsque ce problème de '.cat' a été évoqué, il a déclenché beaucoup d'inquiétudes, de sorte que cela pourrait constituer une espèce d'alibi pour d'autres langues, ou même amener plus de controverses au sein des communautés linguistiques et culturelles qui peuvent avoir des revendications à tendance nationalistes. Avec un regard rétrospectif, nous voyons que ceci ne s'est pas produit.

### La gestion des noms de domaines nationaux

La gestion des domaines de premier niveau pour les pays comprend trois questions importantes. La première concerne la décision souvent politiquement controversées de savoir exactement quel code appliquer à des pays ainsi qu'à des entités ayant un statut international non clarifié ou contesté (par exemple, les pays nouvellement indépendants et les mouvements de résistance). Une récente question controversée a été l'attribution d'un nom de domaine à l'Autorité palestinienne. En justifiant sa décision de céder le domaine de premier niveau '.ps', l'Internet Assigned Numbers Authority (IANA) a réaffirmé le principe de l'attribution des noms de domaine en conformité avec la norme ISO 3166, comme cela a été proposé par Jon Postel, l'un des pères fondateurs de l'Internet.<sup>14</sup>

Le deuxième problème concerne l'entité devant gérer les codes de pays. De nombreux pays ont essayé de prendre le contrôle de ces noms de domaines, qui sont considérés comme des ressources nationales. Les gouvernements nationaux ont choisi une grande variété d'approches stratégiques.<sup>15</sup> La transition ('re-délégation') vers une nouvelle institution qui se chargerait de gérer le ccTLD ('délégué') au sein de chaque pays est approuvée par l'ICANN si et seulement s'il existe un consensus de toutes les parties prenantes dans le pays. Étant donné l'importance de ce problème et la grande variété d'approches, il ya eu deux initiatives importantes au niveau international pour introduire un certain degré d'harmonisation. La première a été les 'principes du GAC', adoptés par le Comité Consultatif Gouvernemental de l'ICANN (CCG), qui propose des politiques et spécifie les procédures pour la re-délégation de l'administration des ccTLD.<sup>16</sup> La seconde constitue 'les meilleures pratiques', proposé par le *World Wide Alliance of Top Level Domains* (Juin 2001).

Le troisième problème est lié à la réticence des opérateurs de nombreux domaines de pays à devenir partie intégrante du système de l'ICANN. Jusqu'à présent, l'ICANN n'a pas réussi à rassembler les opérateurs des domaines des pays sous son égide. Les opérateurs des domaines de pays sont organisés au niveau régional (Europe – CENTR, l'Afrique – AFTLD, Asie – APTLD, Amérique du Nord – NATLD, l'Amérique du Sud – LACTLD). Au niveau

mondial, le principal forum est le *World Wide Alliance of Top level Domains*. L'ICANN est entrain de développer un 'Cadre de responsabilisation', comme une manière moins formelle d'établir des liens avec les opérateurs des domaines des pays.

### Les noms de domaine internationalisés

L'Internet a été initialement développé comme medium, et essentiellement en anglais. Grâce à une croissance rapide, l'Internet est devenu un outil de communication globale avec un nombre croissant d'utilisateurs non-anglophones. Pendant une longue période, le manque de fonctionnalités multilingues dans l'infrastructure d'Internet fut l'une des principales limites de son développement. En mai 2010, après une longue période d'essai et d'incertitudes politiques, l'ICANN commença à approuver de nouveaux noms de domaine en une large variété de scripts, incluant le Chinois, l'Arabe et le Cyrillique. L'introduction de noms de domaine internationalisés (Internationalized Domain Names – IDN) est considéré comme l'un des succès majeur du régime de la Gouvernance de l'Internet.

### Les serveurs racines

Au sommet de la structure hiérarchique du système des noms de domaine, les serveurs racine attirent beaucoup d'attention. Ils font partie de la plupart des débats politiques et académiques sur les problèmes de gouvernance de l'Internet.

### La situation actuelle

Le fonctionnement et la robustesse du DNS peuvent être illustrés par l'analyse du fait que l'Internet peut s'effondrer si jamais les serveurs racines étaient désactivés. Premièrement, il existe 13 serveurs racines distribués à travers le monde (10 aux Etats-Unis, un en Suède, un aux Pays Bas et un au Japon; des 10 aux Etats-Unis, plusieurs sont exploités par des organismes gouvernementaux américains), 13 étant le nombre maximal techniquement possible. Si un des serveurs tombe en panne, les 12 restants continueraient à fonctionner. Même si tous les 13 serveurs racines tombent en panne en même temps, la résolution de nom de domaine (la fonction principale de serveurs racines) se poursuivrait sur les autres serveurs de noms de domaines, réparties hiérarchiquement sur Internet<sup>17</sup>.

Par conséquent, des milliers de serveurs de noms de domaines contiennent des copies du fichier de la zone racine, et un effondrement immédiat et

catastrophique de l'Internet n'est pas envisageable. Il faudrait un certain temps avant que de graves conséquences fonctionnelles soient remarquées, temps pendant lequel il serait déjà possible de réactiver les serveurs d'origine ou d'en créer des nouveaux.

En outre, le système de serveurs racines s'est considérablement renforcé par le régime 'Anycast', qui reproduit des serveurs racines dans le monde entier. Ceci offre de nombreux avantages, notamment une robustesse accrue dans le système DNS et une résolution plus rapide des adresses Internet (avec le régime *Anycast*, les serveurs qui font des résolutions sont plus proches des utilisateurs finaux).

Les 13 serveurs racines sont gérés par une diversité d'organisations: institutions universitaires / institutions publiques, les sociétés commerciales et des institutions gouvernementales. Les institutions gérant des serveurs racines reçoivent un fichier de zone racine proposé par l'IANA (ICANN) et approuvé par le gouvernement des États-Unis (Département du commerce, *Department of Commerce – DoC*). Une fois que le contenu est approuvé par le Département du commerce, il entre dans le serveur racine principal géré par VeriSign sous contrat avec le Département.

Le fichier dans le serveur racine principal est automatiquement répliqué dans tous les autres serveurs racines. Ainsi, il est théoriquement possible pour le gouvernement des États-Unis d'introduire des changements unilatéraux à l'ensemble des DNS. C'est une source de préoccupation pour de nombreux gouvernements.

## Les problèmes

### L'internationalisation du contrôle des serveurs racines

Plusieurs pays ont exprimé leur préoccupation au sujet de la disposition actuelle par laquelle l'ultime décision concernant le contenu des serveurs racine demeure la responsabilité d'un pays (les États-Unis). Dans les négociations sur la gouvernance de l'internet, il y a eu des propositions diverses, y compris l'adoption d'une 'Root Convention', qui confierait à la communauté internationale la charge de surveiller la politique des serveurs racines ou, au moins des droits aux États sur la gestion de leurs propres noms de domaine nationaux. De nouvelles possibilités ont été ouvertes avec l'Affirmation of Commitments<sup>18</sup>, qui traite de la question de l'indépendance institutionnelle de l'ICANN vis à vis du Département du Commerce des États-Unis, y compris l'internationalisation à venir de l'ICANN. Le statut de

l'IANA sera renégocié en 2011. Quelques éléments pour la mise en place de solutions pratiques devraient se faire en deux étapes:

- 1 la réforme de l'ICANN, initiée par l'Affirmation of Commitments', conduisant à la création d'une organisation internationale *sui generis*, qui serait un cadre institutionnel acceptable pour tous les pays.
- 2 le transfert du contrôle des serveurs racines du Département américain du commerce à l'ICANN, comme cela a été initialement prévu.

### Serveurs racines alternatifs- faisabilité et risques

La mise en place d'un serveur racine alternatif est techniquement simple. La principale question est de savoir combien d'adeptes' un serveur alternatif pourrait avoir, ou, plus précisément, quel est le nombre d'ordinateurs sur Internet qui y pointeraient, au moment de la résolution des noms de domaine. Sans utilisateurs, tout DNS alternatif devient inutile. Quelques tentatives pour créer un DNS alternatif ont été réalisées: *Open NIC*, *New.net*, et *Name.space*. La plupart d'entre elles ont été infructueuses, ne comptant qu'un pourcentage négligeables d'utilisateurs.

### Le rôle des États-Unis dans la gestion des serveurs racines – Le paradoxe de la puissance

Depuis l'adoption de l'Affirmation of Commitment', la question du paradoxe de la puissance américaine sur les serveurs racines pouvait progressivement appartenir au passé. Le pouvoir potentiel de retirer un pays de l'Internet (par la suppression de son nom de domaine) peut difficilement être qualifié d'acte de puissance, puisqu'il n'a pas d'utilité effective. L'élément-clé dans l'exercice du pouvoir est de forcer l'autre à agir dans le sens voulu par le détenteur du pouvoir. L'utilisation du 'pouvoir' des États-Unis sur l'infrastructure de l'Internet pourrait générer des effets inattendus, y compris que des pays et des régions aillent jusqu'à établir leur propre 'internet'. Dans un tel scénario, l'Internet pourrait se désintégrer et les intérêts des États-Unis viendraient à disparaître (la prédominance des valeurs des États-Unis sur l'Internet, l'anglais comme langue franche de l'internet, la prédominance des sociétés américaines dans le domaine du e-commerce). Sur la base de ses premières initiatives politiques dans la gouvernance de l'internet (par exemple, l'Affirmation of Commitment), il semble que l'administration Obama soit consciente du paradoxe de puissance. Cela constitue un signe prometteur quant à l'évolution future du régime de la gouvernance de l'Internet au niveau mondial.

## **La neutralité du réseau**<sup>19</sup>

Que se serait-il produit si la concurrence avait limité l'accès à Google à ses débuts? Ou si les opérateurs de télécommunication avaient ralenti l'introduction de la téléphonie d'internet à Skype? Ou si le gouvernement des Etats-Unis avait restreint l'accès à l'Internet dans les pays ennemis?<sup>20</sup> Nous aurions très probablement eu un réseau informatique qui aurait été dans la logique des années 80, par exemple, du protocole réseau X.25 au lieu du TCP/IP, échangeant des données entre les réseaux informatiques nationaux aux frontières entre pays.

Le succès de l'Internet se situe dans sa conception qui est basée sur le principe de la neutralité du réseau. Tout trafic de données sur l'Internet à ce moment-là, qu'il vienne de nouvelles petites compagnies ou de grandes compagnies, a été traité sans discrimination. Les nouvelles compagnies et les innovateurs n'ont eu besoin ni de permission ni de puissance du marché pour innover sur l'Internet.

La neutralité de réseau, a été jusqu'à présent le point important du succès de l'Internet. C'est pourquoi la discussion sur la neutralité du réseau a attiré un éventail d'acteurs: du Président des États-Unis aux activistes de bases des droit de l'Homme. La neutralité de réseau est l'une des priorités les plus élevées du programme technologique du Président Obama et cette thématique a été discutée dans plusieurs instances politiques, y compris le Congrès américain. Dès le début, la neutralité du réseau était une discussion centrée aux Etats Unis; mais avec les nouveaux développements, la neutralité de réseau est de plus en plus discutée dans le monde entier.

### **Pourquoi la neutralité du réseau est-elle d'actualité aujourd'hui?**

Il n'y a pas de conspiration. L'Internet est devenu une victime de son propre succès. Avec 2 milliards d'utilisateurs et un changement croissant de notre réalité économique et sociale quotidienne sur l'Internet, les enjeux prennent de plus en plus d'importance. L'Internet a un potentiel commercial et de développement très important. Pour certains de ces aspects commerciaux, particulièrement ceux en relation avec la diffusion des services vidéo et multimédia, la neutralité du réseau pourrait constituer un obstacle.

## La situation actuelle

Paradoxalement, la neutralité du réseau n'a jamais été strictement appliquée. Depuis les débuts des connexions par modems, il y a eu des rivalités entre bande passante disponible et les besoins des utilisateurs. Afin de relever ce défi et assurer la qualité de service, les opérateurs Internet (les entreprises de télécoms et les FAI) ont utilisé diverses techniques de gestion du réseau pour prioriser certains trafics. Par exemple, le trafic internet qui permet de véhiculer la conversation vocale sur Skype devrait avoir la priorité sur le trafic qui véhicule un simple e-mail: alors que nous pouvons percevoir un retard de voix dans la conversation sur Skype, nous ne remarquerons pas les petits retards dans les échanges d'e-mails. Le besoin de gestion du réseau est particulièrement important aujourd'hui avec l'accroissement du nombre d'utilisateurs de plus en plus demandeurs davantage de services tels que les téléchargements, les vidéos Haute Définition, la téléphonie sur Internet, les jeux en ligne, etc.

### La demande croissante en bande passante

En 2009, comme illustration de la demande croissante en bande passante, les téléspectateurs de YouTube observaient environ 1.2 milliards de vidéos par jour<sup>21</sup>, et téléchargeaient presque 20 heures de vidéo chaque minute!<sup>22</sup>

La gestion du réseau devient de plus en plus sophistiquée en routant de façon optimale le trafic Internet pour garantir un service de qualité: prévenant la congestion et éliminant latences et coups de nervosité.

La première discorde dans l'interprétation du principe de la neutralité du réseau se fonde sur la question de savoir si oui ou non n'importe quelle gestion de réseau serait permise. Les puristes de la neutralité du réseau soutiennent que 'tous les bits sont égaux' et que tout le trafic internet doit être traité de façon égale. Les sociétés de télécoms et les FAI estiment plutôt que ce sont les utilisateurs qui doivent avoir un accès égal à Internet, et si cela devait arriver, le trafic ne pourrait pas être traité de manière égale. Si les trafics de vidéos et d'e-mails sont traités de manière équitable, les utilisateurs n'auront pas un bon débit vidéo à la réception, par contre, ils ne remarqueront pas le retard de quelques secondes en recevant un e-mail. Même les défenseurs de la neutralité du réseau, ne peuvent remettre en question cette raison. Leur problème est que tout compromis sur la neutralité du réseau peut ouvrir une boîte de pandore, en soulevant le problème de la distinction entre la gestion justifiée du réseau et sa possible manipulation.

## Les problèmes

Dans le débat sur la neutralité du réseau, il y a un consensus qui se dégage sur le fait qu'il y a un besoin pour une gestion *appropriée* du réseau. La question principale est celle de savoir comment interpréter l'adjectif 'approprié'. En plus des problèmes techniques, il y a trois autres aspects – les problèmes économiques, juridiques et des droits humains – où le débat sur la neutralité du réseau est particulièrement houleux.

## Les problèmes économiques

Pendant les décennies passées, beaucoup d'opérateurs – Télécoms et FAI – ont étendu leurs activités commerciales à la fourniture des services:

A côté de la vente des connexions Internet et de la bande passante aux ménages et aux entreprises, ils ont introduit leurs propres VoIP (Voice-over Internet Protocol ; le téléphone via internet) ou IPTV (la télévision via Internet) services, la vidéo à la demande (une sorte de location de films), les portails de téléchargement de musique et de vidéos, etc. Ils sont maintenant en concurrence entre eux, non seulement pour des connexions moins chères, plus rapides et de meilleure qualité, mais également avec les fournisseurs de services et de contenus comme Skype, Google et Apple.

La gestion du réseau, quelque chose de disponible aux opérateurs mais pas aux autres peut s'avérer un outil important dans une compétition sur les services et les contenus en donnant la priorité aux paquets selon leur préférence commerciale.

Par exemple, un opérateur peut décider de ralentir la circulation des données ou carrément bloquer les données d'un concurrent (telle la téléphonie Skype ou Google) aux utilisateurs finaux à travers son réseau, ceci tout en donnant la priorité à ses propres données (telles que la téléphonie sur IP ou la télévision sur internet qu'il fournit à ses clients)<sup>23</sup>.

## Les problèmes juridiques

Une autre zone grise dans la gestion du réseau est le droit des opérateurs de bloquer les contenus qui peuvent enfreindre les droits d'auteurs. Les FAI ont-ils le droit et l'obligation d'arrêter le trafic, par exemple, sur les réseaux **peer-to-peer** (P2P) qui sont souvent utilisés pour le partage des éléments protégés par les droits d'auteurs? Ont-ils les prérogatives des corps juridiques et administratifs?

Certaines de ces questions ont été le point central d'une affaire entre la *Federal Communication Commission (FCC)* et l'opérateur Internet Comcast. En 2007, deux groupe-conseils publics ont porté plainte auprès de la FCC, l'autorité américaine de régulation, se plaignant du fait que Comcast, l'opérateur, avait violé le principe de la neutralité du réseau en ralentissant de façon significative l'application BitTorrent (Logiciel P2P pour le téléchargement des fichiers – très souvent de la musique, la vidéo et les jeux, bien que ne se limitant pas à cela) pour ses utilisateurs<sup>24</sup>.

### Les problèmes politiques

La capacité à gérer le trafic réseau basé sur l'origine et la destination, le service et le contenu, peut donner aux États l'occasion d'imposer de telles pratiques sur les opérateurs du trafic domestique et introduire par la même occasion les filtres pour les contenus sensibles et controversés en relation avec la politique, l'idéologie, la religion, la culture ou d'autres valeurs de ce pays. Ceci amène les risques d'abus dans la gestion du réseau pour permettre la censure, particulièrement dans des pays aux régimes autoritaires.

### Les risques

Si la gestion du réseau va au-delà d'un niveau *approprié* visant à fournir un service équitable à tous les utilisateurs internet, le principe de la neutralité du réseau serait en danger. Cela pourrait conduire à un Internet à plusieurs strates.

Selon les groupes d'utilisateurs tels que Save the Internet<sup>25</sup> et Internet Governance Caucus<sup>26</sup>, l'Internet deviendrait un ensemble de packages commerciaux offerts par les FAI dont les utilisateurs ne pourraient accéder qu'à une partie des services et contenus en ligne dans un certain package donné<sup>27</sup> – beaucoup plus comme la télévision par câble.

Par conséquent, ils préviennent que si les opérateurs de trafic commencent à taxer les fournisseurs de contenus et d'application, cela tuerait la concurrence entre opérateurs propriétaires des services, et mettrait en danger les petits commerces<sup>28</sup> et les offres non commerciales, telles que les applications pour des personnes vivant avec des handicaps qui demandent généralement une large bande passante.

### Qui sont les principaux acteurs et quels sont leurs arguments?

La position des principaux acteurs est en constant changement. Par exemple, la dernière indication selon laquelle Google signerait un accord spécial avec Verizon pour une approche intermédiaire à la neutralité du réseau changerait

le positionnement des principaux acteurs<sup>29</sup>. Jusqu'à maintenant, Google a été considéré comme l'un des fervents défenseurs de la neutralité du réseau ; les autres sont les associations des consommateurs, les entreprises en ligne, certaines entreprises du domaine des technologies, la plupart des grandes entreprises d'Internet comme Yahoo !, Vonage, Ebay, Amazon, Earthlink ainsi que les entreprises de logiciels telle que Microsoft.

	Les partisans	Les opposants
<b>L'argument à propos du futur</b>	La neutralité du réseau préservera l'architecture de l'Internet qui a permis un développement rapide et innovant de l'internet jusque-là. La plupart des défenseurs de la neutralité du réseau sont les nouvelles entreprises d'Internet qui se sont développés grâce à l'architecture ouverte de l'Internet.	Les entreprises en ligne doivent avoir l'opportunité de développer davantage l'Internet et offrir les services qui intéressent les clients. Ceci peut impliquer un internet plus rapide.
<b>Les arguments économiques</b>	Sans la neutralité du réseau l'Internet ressemblera à la Télévision par câble. Une poignée de sociétés contrôleraient l'accès et la distribution des contenus en décidant quel utilisateur a le droit de le regarder et combien cela doit coûter. Alors que cela profiterait à peu, la majorité en pâtirait et en fin de compte ruinerait le futur économique de l'Internet.	S'il n'y a pas la possibilité d'offrir de nouveaux services et des modèles économiques, ceci réduirait l'intérêt économique de l'Internet, stopper les investissements et même en fin de compte mettre en péril l'infrastructure de l'internet.
<b>Les arguments éthiques</b>	L'internet est le résultat de développements par plusieurs volontaires pendant de nombreuses décennies. Ils avaient investi leur temps et leur créativité en développant les aspects intrinsèques de l'internet, des protocoles techniques aux contenus. Il n'est donc pas juste de voir ce grand investissement profiter a une minorité de compagnies qui enfermeront l'internet dans des systèmes contraignants en violant le principe de la neutralité du réseau. L'Internet a été conçu de façon à être ouvert et public. L'intérêt du public doit être garanti. La neutralité du réseau est l'un des moyens de parvenir à cela.	La neutralité du réseau est éthiquement discutable parce que les opérateurs de l'internet doivent investir dans la maintenance de leur infrastructure et beaucoup de bénéfices sont réalisés par les compagnies des contenus telles que Google, Facebook et Amazon. Les opérateurs internet et télécoms estiment que le gâteau devrait être partagé un peu plus équitablement.
<b>Les arguments de régulation</b>	La neutralité du réseau doit être imposée par les Etats. Toute forme d'autorégulation ouvrira la voie aux opérateurs télécoms et Internet et les compagnies du câble à une violation de la neutralité du réseau.	L'Internet s'est développé à cause d'une régulation légère ou sans régulation du tout. Une régulation trop lourde de la part des Etats peut étouffer la créativité et une régulation sur la neutralité du réseau peut étouffer le développement futur de l'internet.

Les opposants à la neutralité du réseau y compris les principales compagnies de Télécoms, les FAI, les producteurs des équipements de réseau et matériel informatiques, ainsi que les producteurs du matériel vidéo et multimédia. Leurs arguments sont centrés sur le marché, en commençant par le besoin de fournir ce que les consommateurs demandent.

Il y a quatre arguments principaux dans le débat sur la neutralité du réseau.

### Les principes de base

Dans un passé récent, quelques régulateurs- tels que ceux de la Norvège, des Etats Unis ou de l'UE ont fait un pas et ont formulé les principes-clé de la neutralité du réseau en se basant sur les discussions en cours.<sup>30</sup>

- **Transparence:** Les opérateurs internet doivent fournir des informations complètes et actualisées sur leurs pratiques en matière de gestion du réseau, sur leur capacité, et sur la qualité des services offerts aux clients.
- **Accès:** Les utilisateurs devraient avoir un accès [équitable] à n'importe quel service contenu, service ou application [légale] [avec un minimum de la qualité de service garanti, tel que prescrit par le régulateur] ou bien connecter tout équipement qui ne gêne pas le réseau [sans distinction de leurs capacités financières ou statuts sociaux].
- **(Non) discrimination:** les opérateurs internet ne doivent faire aucune discrimination [ou une discrimination raisonnable] sur le trafic en se basant sur:
  - L'origine de l'expéditeur et du receveur
  - Le type du contenu, de l'application et du service [avec une concurrence saine – pas de discrimination contre les concurrents indésirables].
  - Là où "raisonnable" serait toute pratique pour le bénéfice public (assurer la qualité de service, la sécurité et la résilience du réseau, les innovations et les investissements supplémentaires, la baisse des prix, etc.).

Les autres principes souvent débattus dans les forums internationaux tels que les réunions du FGI et le dialogue *EuroDIG*<sup>31</sup> comprennent:

- La protection de la liberté d'expression, d'accès à l'information et de choix.
- Assurer la qualité du service, la sécurité et la résilience du réseau.
- Préserver un environnement favorable aux investissements.

## Utilisateurs ou clients?

Le débat sur la neutralité de réseau crée également une rhétorique linguistique. Les partisans de la neutralité de réseau se concentrent sur les 'utilisateurs' d'Internet, alors que les autres – principalement les acteurs commerciaux – les décrivent comme étant des 'clients'. Les internautes sont plus que de simples clients ; le terme 'utilisateur' implique la participation active au développement de l'Internet par le biais des réseaux sociaux, le blogging, et d'autres outils; et le rôle important qu'ils ont en décidant du futur d'Internet. Les clients, d'une part, comme tous les autres clients, peuvent décider si oui ou non il faut acheter les services offerts. Leur statut sur l'Internet est basé sur un contrat avec le FAI et sur des règles de protection des utilisateurs. Au delà, les clients sont supposés n'avoir aucun rôle dans la prise de décision sur le fonctionnement de l'Internet.

- Stimuler les innovations pour les investissements [y compris les opportunités pour de nouveaux modèles d'affaires et de nouvelles possibilités commerciales]. Définir les droits et rôles, et créer l'obligation de rendre des comptes pour toutes les parties engagées (fournisseurs, régulateurs, utilisateurs) incluant le droit de faire appel et d'obtenir réparation.
- Prévenir les pratiques de concurrence déloyale.
- Créer un environnement pour un marché qui permettrait à tous les utilisateurs de choisir ou de changer librement leur opérateur réseau.
- Protéger les intérêts des couches fragiles, telles que les personnes vivant avec un handicap ainsi que les utilisateurs et les entreprises des pays en développement.
- Maintenir la diversité des contenus et des services.

### Les approches politiques

Avec le débat sur la neutralité du réseau, il y a une autre question qui a surgi: quel est le rôle des régulateurs dans la politique en rapport avec la large bande et les pratiques des opérateurs?

### Les pays développés

En réponse à l'affaire Comcast, le FCC américain a adopté les lignes directrices sur la neutralité du réseau comme une mise à jour de son papier blanc de 2005,<sup>32</sup> lesquelles reflètent le besoin d'accès aux contenus et des équipements ainsi que le choix des ces derniers, cela a résolu les problèmes de discrimination et de transparence. Le Ministère Japonais des affaires intérieures et le Groupe de travail sur les communications ont fait un

rapport sur le choix et l'accès ainsi que sur la discrimination, mais ils se sont également penchés sur la répartition équitable des coûts et l'utilisation du réseau<sup>33</sup>. L'Agence suédoise des Postes et Télécoms (PTS) a soutenu que l'ouverture – soutenue par la concurrence et la non-discrimination est un pré requis pour l'innovation, mais qu'elle doit également être équilibrée entre les investissements et la sécurité du réseau.<sup>34</sup> Le cadre réglementaire des communications électroniques de l'UE vise à protéger la liberté d'expression, le choix des utilisateurs et les droits d'accès, ensemble avec le principe de transparence ; pourtant le cadre met également l'accent sur le besoin d'investissement, la concurrence saine sans discrimination, et des opportunités pour de nouveaux modèles économiques incluant les initiatives innovatrices.<sup>35</sup>

Le modèle le plus en vogue vient de L'autorité Norvégienne des Postes et Télécoms (NPT), qui cherche à assurer: la transparence dans les affaires et les pratiques, le choix de l'utilisateur et l'accès aux contenus, les services et les équipements, et la non discrimination basée sur les applications, les services, le contenu, l'expéditeur et le receveur.<sup>36</sup> Cependant, ce n'est pas seulement le contenu qui est en jeu mais également le processus pour parvenir à un consensus à propos de ces lignes directrices: adopter une approche largement basée sur l'implication de toutes les parties prenantes dans la mise en place d'un système souple de co-régulation basé sur la recherche d'un consensus à travers des accords d'engagement; dans ce sens, le NPT a rassuré les consommateurs et les entreprises sur le fait que le marché peut être régulé sans dispositif légal lourd.<sup>37</sup>

Toutefois, dans certains pays, il y a une pratique qui consiste à ne pas prévenir les discriminations à caractère commercial. Les défenseurs de la neutralité du réseau les qualifient de "paradis anti-neutralité" où, l'on peut voir ce que sont les perspectives d'un 'Internet véritablement non neutre'.

### Les pays en développement

A cause d'une infrastructure et une bande passante limitées, les régulateurs des pays en développement se basent plus sur des politiques de bon usage – prix abordables et accès équitable pour tous. D'autres soulèvent les problèmes relatifs à la non-discrimination transfrontalière, en avançant que le trafic de tous les pays doit être traité de la même manière sans référence aux coûts de terminaison. De plus, certains pays sont plus sensibles aux aspects culturels internes, politiques ou éthiques, entraînant de ce fait une compréhension de 'l'usage approprié' dans la perspective d'une gestion différente du réseau par rapport aux autres pays. On a évoqué les problèmes selon lesquels les modèles innovateurs du monde développé pourraient compromettre les marchés

des pays en développement: en donnant la priorité aux services des grandes compagnies internationales; les entreprises émergentes et la concurrence seraient menacées, mettant en péril la diversité et l'innovation. Toutefois, aucune politique formelle majeure ou pratique régulatrice sur la neutralité du réseau ne provient du monde en développement.

### Les organisations internationales et les ONG

Plusieurs organisations internationales et groupes d'utilisateurs ont ainsi développé des positions politiques par rapport à la neutralité du réseau. Le Conseil de l'Europe met l'accent sur les droits fondamentaux de la liberté d'expression et d'information; l'ISOC fait la promotion de son approche centrée sur l'utilisateur avec une prédominance sur les problèmes concernant l'accès, le choix, et la transparence à travers le débat sur l'"inter-réseautage ouvert" plutôt que celui sur la neutralité du réseau.<sup>38</sup> Le Trans Atlantic Consumer Dialogue (TACD), un forum des associations de consommateurs des Etats Unis et de l'UE met ainsi l'accent sur les demandes non-discriminatoires des opérateurs de trafic, appelant les régulateurs des Etats Unis et de l'UE à agir comme les défenseurs des droits des utilisateurs.<sup>39</sup> Beaucoup d'ONG se sentent particulièrement concernées par le futur des contenus non commerciaux et non concurrentiels des services en ligne, en demandant qu'ils soient diffusés à travers le réseau de transport de n'importe quel opérateur comme c'est le cas dans le cadre commercial. Ils mettent l'accent sur les droits des groupes marginaux – particulièrement les personnes handicapées – qui doivent utiliser les contenus, les services et les applications (y compris les applications requérant une grande bande passante) de leur choix sans aucune limite.

### Les questions ouvertes

Il y a un nombre important de questions ouvertes dans l'agenda du débat sur la neutralité du réseau.

- Où devrait se trouver l'équilibre entre les effets du bien public sur l'Internet et les droits de l'utilisateur (homme) d'un côté, et de l'autre les droits des opérateurs Internet à innover sur leurs propres réseaux?
- Un marché non régulé avec une concurrence ouverte comme évoqué par les opérateurs de trafic, peut-il fournir un choix illimité (ou suffisant) aux utilisateurs? Ou alors, les régulateurs doivent-ils inévitablement servir de garde fous, et avec quelle autorité?
- Comment les différentes méthodes des régulateurs peuvent-elles avoir un impact sur le marché de la bande passante et susciter plus d'investissement et d'innovation?

- Quelles sont les implications de la (non) neutralité du réseau pour les pays en développement?
- Le besoin de gestion du réseau pour des raisons techniques (qualité) sera-t-il obsolète dans l'avenir, à cause des évolutions dans la technologie de transport du trafic?
- Quelles sont les implications d'un Internet fragmenté pour la concurrence, l'innovation, l'investissement, et les droits de l'Homme?
- Comment l'ère du *cloud computing* (informatique en nuages) et la dépendance croissante vis-à-vis du nuage influenceront-ils le débat sur la neutralité du réseau et vice versa?
- Le débat devrait-il être étendu de la gestion du trafic au niveau de l'opérateur de transport, à la gestion des contenus et des applications au niveau du fournisseur de contenus et d'application, tels que Google, Apple ou Facebook?
- La protection du consommateur sera-t-elle toujours intrinsèquement liée à la neutralité du réseau? Si la neutralité du réseau était 'défaite', quels principes soutiendraient la protection du consommateur dans l'avenir?

## Les Fournisseurs d'Accès Internet (FAI)

Puisque les FAI connectent les utilisateurs finaux à l'Internet, ils fournissent l'option la plus directe de l'application des règles du droit sur l'Internet. Avec les problèmes de l'accroissement de l'aspect commercial de l'Internet et de l'importance grandissante des questions de cyber sécurité, beaucoup de pays ont commencé à concentrer tous leurs efforts sur l'application du droit aux FAI.

### Les enjeux

#### Les Monopoles de Télécom et les FAI

Il est courant de trouver que dans les pays avec des monopoles sur les télécommunications, ces monopoles fournissent également un accès à l'Internet. Ces monopoles prohibent les autres FAI d'entrer sur le marché, empêchant ainsi la concurrence.

Cela a pour conséquences les prix élevés, avec souvent une qualité de service médiocre, et un échec dans la réduction de la fracture numérique. Dans certains cas, ces monopoles dans les télécommunications tolèrent l'existence d'autres FAI, mais interfèrent au niveau opérationnel (par exemple en offrant une faible bande passante ou en causant des interruptions dans les services).

### La responsabilité des FAI en matière de droits d'auteurs

Il y a un principe commun dans tout système juridique: un FAI ne sera pas tenu pour responsable d'avoir hébergé des éléments qui enfreignent les droits d'auteurs (copyright) si le FAI n'est pas au courant de la violation. La différence principale se situe au niveau des actions légales entreprises après que le FAI ait été informé que l'élément qu'il héberge enfreint les droits d'auteur.

Les lois des Etats Unis et de l'UE emploient la procédure *Notice-Take-Down*, qui exige des FAI le retrait d'un tel élément pour éviter d'être poursuivi. La loi japonaise adopte une approche plus équilibrée, à travers la procédure *Notice-Take-Down*, qui donne à l'utilisateur de l'élément le droit de porter plainte contre la demande de suppression de l'élément.

L'approche qui consiste à placer une responsabilité limitée sur les FAI a généralement été dictée par la jurisprudence. Les cas les plus importants où les FAI ont été exemptés de toute responsabilité pour avoir hébergé des éléments qui sont en violation des droits d'auteur sont: le cas de la Scientologie (Pays-Bas), *RIAA vs Verizon* (Etats Unis), *SOCAN vs CAIP*(Canada), et *Sabam vs Tiscali* (Belgique).

### Le rôle des FAI en matière de contenus

Sous la pression publique croissante, les FAI, bien qu'à contrecœur, s'impliquent de plus en plus dans la politique du contenu. En le faisant, ils devraient suivre deux voies possibles. La première, consiste en l'application de mesures de régulation de l'Etat. La seconde, est basée sur l'autorégulation, et soutient qu'il appartient aux FAI de décider par eux-mêmes le contenu approprié. Ceci fait courir le risque de privatiser le contrôle du contenu, ce qui ferait que les FAI prendraient les responsabilités des Etats.

### Le rôle des FAI dans la politique anti-pollupostage

Les FAI sont en général considérés comme les premières structures impliquées dans les initiatives anti-pollupostage. Généralement, les FAI disposent de leur propre initiative de lutte contre le pollupostage, soit par un filtrage technique ou par la mise en place d'une politique anti-pollupostage. Le rapport de l'UIT sur le pollupostage déclare que les FAI devraient être responsables et proposer des code de conduite anti-pollupostage, qui doivent inclure deux dispositions importantes: un FAI doit interdire à ses utilisateurs d'envoyer des pollupostages et il ne doit pas entretenir des relations de peering avec un autre FAI qui refuse un tel code de conduite.<sup>40</sup>

Par exemple, le système de filtrage de Verizon a conduit à un procès car ayant également bloqué des messages légitimes, causant des préjudices aux utilisateurs qui n'ont pas pu recevoir leurs messages.<sup>41</sup>

## Les fournisseurs de bande passante internet (Internet Broadband Band Providers - IBP)

L'architecture de l'accès Internet a trois niveaux. Les FAI qui connectent les utilisateurs finaux constituent le *niveau 3* (niveau hiérarchique 3). Les niveaux hiérarchiques 1 et 2 sont constitués des IBP. Les fournisseurs du niveau 1 sont les IBP les plus importants. Ils ont toujours des arrangements de peering avec les autres IBP niveau 1.<sup>42</sup> La principale différence entre les IBP et ceux du Niveau 2 est que les IBP de Niveau 1 échangent leur trafic par peering alors que les IBP de Niveau 2 doivent payer les frais de transit aux IBP de Niveau 1.<sup>43</sup>

Le Niveau 1 est toujours constitué de grandes compagnies telles que MCI, AT&T, Câble Wireless et France Télécom.

### Les problèmes

#### L'infrastructure Internet doit-elle être un service public?

Les données internet peuvent circuler à travers n'importe quel média de télécommunications. En pratique, les équipements tels que ceux des dorsales de niveau 1 (Ex: Les principaux transits de données entre de larges réseaux stratégiquement interconnectés et les routeurs principaux de l'Internet), souvent constitués de fibres optiques ou de liaisons satellitaires sont devenus critiques dans le fonctionnement de l'Internet. Leurs positions stratégiques sur l'Internet donnent à leurs propriétaires le pouvoir d'imposer les prix et les conditions du marché. En fin de compte, le fonctionnement de l'Internet dépend des décisions des propriétaires de ces dorsales centrales.

Est-il possible à la communauté internet mondiale de demander des assurances et des garanties aux opérateurs télécoms majeurs pour un fonctionnement harmonieux de l'infrastructure critique de l'Internet? De nos jours, les discussions se focalisent sur une probable imposition de certaines exigences publiques sur les opérateurs privés de l'infrastructure de l'Internet.

### **IBP et l'infrastructure critique**

Au début de 2008, il y a eu une perturbation des câbles internet principaux dans les pays de la Méditerranée, proches de l'Égypte. Cet incident a mis en difficulté l'accès à l'Internet dans une grande partie du globe, jusqu'en Inde. Deux incidents similaires étaient survenus en 2007 (dérangement d'un câble internet proche de Taiwan et du câble principal du Pakistan) démontrant clairement que l'infrastructure est une composante nationale et mondiale de l'infrastructure critique. Une perturbation des services internet peut affecter toute l'économie et la vie sociale d'une région. L'éventualité d'une telle perturbation pousse à se poser un certain nombre de questions: les principaux câbles internet sont-ils bien protégés?

Quels sont les rôles respectifs des gouvernements nationaux, des organisations internationales et des compagnies privées dans la protection des câbles internet?

Comment pouvons-nous gérer les risques associés aux potentielles ruptures de ces câbles principaux de l'Internet?

### **La libéralisation des télécoms et le rôle des FAI et des IBP**

Il y a des vues qui divergent au sujet des modalités selon lesquelles les FAI et IBP devraient être soumis aux mécanismes des instruments internationaux existants. Les pays développés pensent que les règles libérales édictées par l'OMC aux opérateurs télécoms peuvent être également applicables aux FAI. Une interprétation restrictive met en lumière le fait que le régime des Télécoms de l'OMC s'applique seulement au marché des télécoms. La régulation du marché des FAI requiert de nouvelles règles de la part de l'OMC.

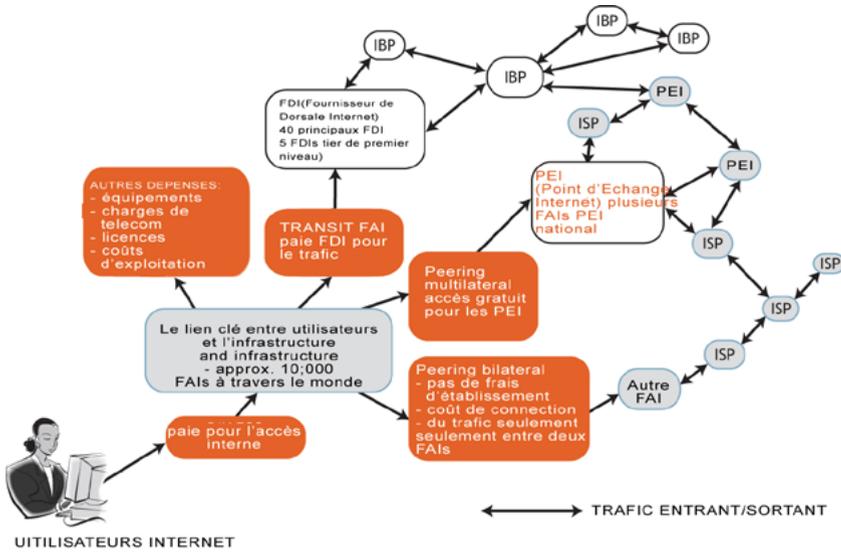
## **Un modèle économique de l'inter connectivité de l'Internet**

*Nous savons comment router les paquets, ce que nous ne savons pas faire c'est router les dollars.*

**David Clark**

### **La situation actuelle**

Souvent, toute discussion liée à des questions de gouvernance débouche sur analyse de distribution d'argent.<sup>44</sup> ' Qui paye pour l'Internet? ' Un nombre de transactions financières a lieu entre les parties impliquées dans l'Internet. Les abonnés individuels et les entreprises payent les FAI pour l'accès et les services Internet. Comment cet argent est-il distribué aux autres dans la



chaîne des services internet? Ou en d'autres termes comment le dollar de l'Internet circule-il?<sup>45</sup> Les dépenses qui devraient être couvertes à partir des frais collectées par les FAI incluent entre autres:

- Les FAI payent aux opérateurs télécoms et pour la bande passante.
- Les FAI payent aux 'RIR' ou 'LIR' desquels on obtient des pools d'adresses IP.
- Les FAI payent aux vendeurs d'équipements, de logiciels et pour la maintenance (ainsi que pour les outils de diagnostic et les autres frais de fonctionnement de leurs services).
- Les parties qui enregistrent un nom de domaine payent auprès d'un registrar et à l'IANA pour leurs services; et
- Les opérateurs télécoms payent auprès des fabricants des câbles, des satellites et des fournisseurs de services de télécoms pour leur fournir les liaisons nécessaires. (Comme les opérateurs sont souvent endettés, ils payent à leur tour de nombreux intérêts aux banques et aux consortiums).

La liste est longue et à vrai dire, 'il n'y a rien qui soit gratuit'. Finalement, les utilisateurs finaux de l'internet, qu'ils soient des individus ou des institutions, payent quelque chose dans cette chaîne.

## Les problèmes

### Le modèle économique de la connectivité d'internet a-t-il besoin de réforme?

Un des legs de l'internet c'est son modèle économique en cours qui a été développé à travers un certain nombre d'interactions. Le modèle économique d'internet est à présent considéré comme étant efficace grâce à la souplesse du fonctionnement de l'internet, et en général, son coût abordable. La principale critique du modèle économique en cours est centrée sur deux aspects:

- 1 Il n'évite pas un monopole des principaux acteurs dans le domaine de la connectivité de l'internet, et par conséquent une distorsion du marché est potentiellement possible.
- 2 Il n'alloue pas un partage équitable à la fois des revenus et des coûts entre tous ceux qui sont impliqués dans l'économie de l'internet.

Dans les milieux académiques, beaucoup de tentatives ont été faites afin de pourvoir à des politiques économiques adéquates pour l'Internet. Nguyen et Armitrage déclarent que l'Internet devrait avoir un équilibre optimal entre trois éléments: l'efficacité technique, l'efficacité économique et les effets sociaux.<sup>46</sup> D'autres soulignent les défis pour remplacer la structure de tarification existante, simple, une structure à taux-plat par une autre plus complexe, telle que la compatibilité basée sur le trafic des paquets. En rapport avec les changements pratiques, certains pensent que changer le modèle économique de l'internet actuel ouvrirait la boîte de Pandore.

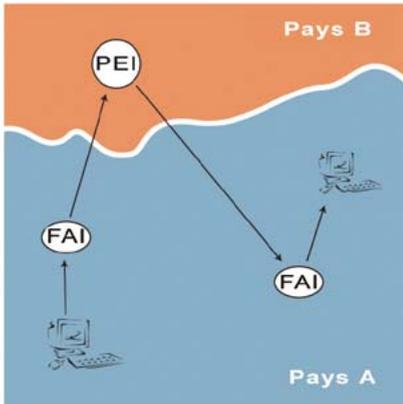
### Empêcher les monopoles possibles dans le marché des ressources de l'internet

Il est possible qu'à travers les changements, quelques monopoles pourraient dominer le marché entier du trafic de l'internet<sup>47</sup>. Ce problème existe à la fois dans les pays développés et ceux en développement. Certains considèrent que le processus de libéralisation des marchés des télécommunications résoudra le problème des monopoles (surtout en associant les opérateurs historiques). Cependant, la libéralisation conduirait au remplacement d'un monopole public par un monopole privé. Geoff Huston dit que l'installation des monopoles et la perte des diverses ressources du marché de l'internet pourraient inévitablement affecter le prix et la qualité des services de l'internet.<sup>48</sup>

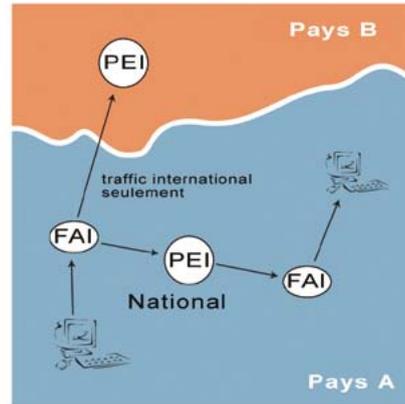
Qui supporterait le coût des liens entre les pays développés et les pays en développement?

*'Quand un utilisateur final au Kenya envoie un e-mail à un correspondant aux Etats Unis, c'est l'ISP Kenyan qui supporte le coût de connexion internationale du Kenya aux Etats Unis. Paradoxalement, quand un*

### Trafic internet sans PEI



### Trafic internet avec PEI



*utilisateur final américain envoie un e-mail au Kenya, c'est toujours l'ISP Kenyan qui supporte le coût de la connexion internationale, et en fin de compte c'est l'utilisateur final Kenyan qui supporte tout le poids en payant le coût le plus élevé des abonnements.*<sup>49</sup>

Actuellement, les pays en développement supportent le coût des liaisons entre les pays en développement et les pays développés<sup>50,51</sup>. Comparé au système de téléphonie traditionnelle, où deux pays partagent le prix de chaque appel international, le modèle Internet met la charge entière d'un côté: celui des pays en développement. Ces pays doivent supporter les coûts pour se connecter aux dorsales situées dans les pays développés. Comme résultat, les pays pauvres et les petits pays subventionnent l'Internet dans les pays riches.

L'argument principal dans les discussions sur les changements vers le système actuel de facturation de l'internet utilise l'analogie du système de règlement financier du téléphone, qui partage le coût et le revenu entre les points finaux de communication. Cependant, Geoff Huston stipule que cette analogie n'est pas à soutenir. Dans le système téléphonique, il n'y a qu'un produit clairement identifiable -un appel téléphonique établissant une conversation humaine entre deux postes téléphoniques - comme un prix<sup>52</sup>. L'internet n'a pas un équivalent, un seul produit, seulement les paquets, qui prennent différents itinéraires à travers le réseau. Cette différence fondamentale rend cette analogie inappropriée. C'est aussi la raison principale qui fait que le modèle de règlement financier téléphonique soit difficile à appliquer à l'Internet.

L'UIT a initié des discussions sur les améliorations qui pourraient être apportées au système actuel de règlement des dépenses liées à l'Internet, afin

d'aboutir à une distribution plus équilibrée des coûts d'accès à l'internet. A cause de l'opposition des pays développés et des opérateurs de télécoms, la résolution adoptée de l'UIT, la D.50, est restée pratiquement sans effet<sup>53</sup>. Des tentatives infructueuses ont également été faites soumettre ce problème aux négociations de l'OMC. Le besoin d'ajustements dans les facturations de l'interconnexion fut réitéré dans les documents finaux du Sommet Mondial de la Société de l'Information (SMSI) et dans le rapport du Groupe de travail sur la gouvernance de l'intérêt (GTGI).

## **Les normes du web**

Vers la fin des années 1980, la bataille sur les normes du réseau fut achevée. Le TCP/IP devenait progressivement le principal protocole du réseau, en marginalisant d'autres standards tels que X25 soutenu par l'UIT et beaucoup de standards propriétaires tel que le SNA d'IBM. Pendant que l'Internet a facilité la communication normale entre plusieurs réseaux à travers TCP/IP, le système manquait encore de standards pour des applications communes.

Une solution fut développée par Tim Berners-Lee et ses collègues au CERN (Centre Européen pour la recherche nucléaire) à Genève, un nouveau standard pour le partage de l'information sur l'Internet appelé HTML (qui n'était juste qu'une simplification d'un standard ISO existant appelé SGML – *Standard Generalized Markup Language*).

Le contenu affiché sur l'Internet devrait d'abord être organisé selon les standards du HTML. Le HTML, étant la base du World Wide Web (toile d'araignées mondiale), a préparé le chemin à la croissance exponentielle de l'Internet.

Depuis sa première version, le HTML a été constamment amélioré avec l'intégration de nouvelles fonctionnalités. La pertinence croissante de l'Internet a mis en exergue la question de la standardisation du HTML. Ceci était particulièrement pertinent pendant les 'guerres des navigateurs' entre Netscape et Microsoft, lorsque chaque société a essayé de renforcer sa position sur le marché en influençant les standards du HTML. Si le HTML de base ne gérait que les textes et les photos, les nouvelles applications d'Internet ont exigé des technologies plus sophistiquées capables de gérer les bases de données, la vidéo et les animations.

Une telle variété d'applications a exigé des efforts considérables de normalisation pour s'assurer que le contenu internet soit proprement visualisé par la majorité des explorateurs d'internet (*browsers*).

La standardisation d'application a intégré une nouvelle phase avec l'émergence de XML, qui a fourni une plus grande flexibilité dans l'établissement des standards du contenu Internet.

De nouvelles séries de standards XML ont également été introduites. Par exemple, le standard pour la distribution du contenu sans fil appelé *Wireless Markup Language* (WML).

La standardisation d'application est principalement menée dans le cadre du consortium du World Wide Web (W3C) sous le leadership de Tim Berners-Lee. Il est intéressant de remarquer que malgré sa grande pertinence à l'Internet, le W3C n'a pas encore attiré beaucoup d'attention dans le débat sur la gouvernance de l'Internet.

## Informatique en nuages

Le terme 'cloud computing – informatique en nuages' est utilisé pour décrire une tendance récente dans l'industrie informatique basée sur l'usage des applications informatiques en tant que services fournis à partir d'énormes groupes de serveurs (une collection de serveurs informatiques entretenus par une entreprise pour accomplir des tâches de serveurs largement au-delà de la capacité d'une seule machine). La première manifestation de l'informatique en nuages est déjà disponible avec le mouvement des e-mails, de nos disques durs vers les serveurs de messagerie (Gmail, Hotmail, Yahoo !) et l'utilisation des processeurs de traitement de texte en ligne (Wiki, services Google). Les applications des réseaux sociaux tels que Facebook et les blogs ont accentué la tendance vers l'informatique en nuages. De plus en plus, nos outils numériques sont déplacés des disques durs vers le nuage (cloud). Les principaux acteurs dans le cloud computing sont Google, Microsoft, Apple, Amazon, et Facebook ; tous ont soit déjà un gros serveur ou planifient d'en développer un de type 'cloud'.

Dès les premiers jours, il y avait de grands et puissants ordinateurs centraux ainsi que des stations de travail. La puissance était au centre. Après cela et pendant longtemps, avec les ordinateurs personnels et les applications Windows la puissance de l'ordinateur s'est déplacée vers la périphérie.

L'informatique en nuages fermera-t-elle le cercle? Allons-nous avoir quelques gros ordinateurs centraux/serveurs et des milliards de stations de travail sous forme de 'bloc-notes', de moniteurs, et de téléphones mobiles? La réponse à cette question et à tant d'autres viendra avec le temps. Actuellement, nous pouvons identifier quelques sujets de la gouvernance de l'Internet qui vont probablement émerger en parallèle avec le développement de l'informatique en nuages.

- 1 Avec plus de services fournis en ligne, la société moderne accroîtra sa dépendance vis-à-vis de l'Internet. Dans le passé, lorsque l'Internet tombait en panne nous n'étions pas capables d'envoyer d'e-mail ou de naviguer sur le net. A l'ère de l'informatique en nuages nous ne pourrions même pas écrire de texte ou faire des calculs. Une plus grande dépendance envers l'Internet impliquera une plus grande pression sur sa robustesse et sa fiabilité. Cela conduira inévitablement à un régime de gouvernance de l'Internet plus fort et une plus grande implication des gouvernements.
- 2 Avec plus de nos données personnelles emmagasinées dans les clouds (nuages), la question de la protection des données personnelles se posera avec plus d'acuité. Aurons-nous le contrôle de nos fichiers textes, e-mails et autres données? Les opérateurs de l'informatique en nuages pourront-ils les utiliser sans notre permission? Qui aura accès à nos données?
- 3 Avec un volume croissant d'outils sociaux passant au format numérique, les pays seront dans une position inconfortable car ayant des patrimoines nationaux hébergés hors des 'frontières' nationales. Ils pourront essayer de créer les clouds nationaux ou régionaux ou s'assurer que les clouds existants sont gérés avec une certaine supervision internationale. La nationalisation des 'nuages' pourra s'accélérer par le fait que tous les principaux opérateurs dans ce domaine sont basés aux Etats Unis. Certains disent que l'actuel débat centré sur l'ICANN peut être remplacé par un débat de gouvernance de l'Internet centré sur la régulation de cloud computing.
- 4 Avec les divers opérateurs du cloud computing, la question des standards devient très importante. L'adoption des standards communs assurera un transfert souple des données parmi les différents clouds (ex. de Google à Apple). Une possibilité en discussion est l'adoption de standards ouverts par les principaux opérateurs du cloud computing.

Lorsqu'il s'agit de cloud computing il y a plus de questions que des réponses. La Gouvernance de l'Internet du cloud computing risque d'émerger à travers l'interaction d'une diversité d'acteurs et de structures. Par exemple, l'UE se focalise sur la vie privée et la protection des données personnelles. Le 'Safe Harbor Agreement' qui était supposé résoudre le problème des différents régimes en matière de respect de la vie privée aux Etats Unis et dans l'UE ne fonctionne pas bien. Avec plus de données numériques qui traversent de

l'océan Atlantique, l'UE et les Etats Unis devront trouver une solution à la question de la protection de la vie privée selon les standards de l'UE par les sociétés Américaines, principaux opérateurs dans le cloud computing.

Lorsqu'il s'agit des standards, il est très probable que les principales sociétés puissent trouver un accord entre elles. Google a déjà commencé une forte poussée vers les standards ouverts en établissant un 'Front de libération des données' dont le but est d'assurer une transition souple des données entre les différents clouds. Ce sont ces premiers groupes qui traiteront la question de la gouvernance de l'internet de l'informatique en nuages. D'autres vont probablement émerger en tant que solution aux problèmes concrets de stratégie.

## Convergence internet-télécommunication-multimédia

Historiquement, la télécommunication, la radio diffusion et les autres domaines associés constituaient des secteurs différents de l'industrie; ils utilisaient des technologies différentes et étaient gouvernés par des régulations différentes. L'importance et la prédominance utilisation de l'IP a conduit à la convergence de ces technologies. Aujourd'hui, nous pouvons passer un coup de téléphone, regarder la télévision et partager la musique sur nos ordinateurs via Internet. Il y a seulement quelques années, cela aurait été fait en recourant à des systèmes différents.

Dans le champ de la communication traditionnelle, le principal point de convergence est la voix sur IP (VoIP). La popularité croissante des systèmes de VoIP tel que Skype est basé sur son faible coût, la possibilité d'intégrer les transferts de données et de la voix sur les mêmes lignes de communication, ainsi que l'utilisation des outils avancés par intermédiaire d'un ordinateur personnel. Avec *YouTube* et les services similaires, l'Internet fait également converger les services de multimédia et les divertissements traditionnels. Alors que la convergence technique progresse à un rythme rapide, ses implications économiques et juridiques exigeront du temps pour évoluer.

### Les enjeux

#### Les implications économiques de la convergence

A un niveau économique, la convergence a commencé à réorganiser les marchés traditionnels en mettant en compétition directe des sociétés qui auparavant fonctionnaient dans les domaines séparés. Les sociétés utilisent

des stratégies différentes. L'approche la plus fréquente est la fusion et l'acquisition. Par exemple, la fusion d'America Online et Time Warner visait à combiner la télécommunication avec les médias/divertissements. Actuellement, AOL/Time Warner a rassemblé les ISP, la télévision, la musique et le développement de logiciel sous le parapluie d'un seul consortium.

### Le besoin d'un cadre juridique

Le système juridique a été le plus lent pour s'ajuster aux changements causés par la convergence technologique et économique. Chaque segment – la télécommunication, la radio diffusion et l'information – a son propre cadre spécial de régulation. Cette convergence ouvre plusieurs questions de gouvernance et de régulation:

- Qu'est ce qui arrivera aux régimes nationaux et internationaux existant dans des domaines comme la téléphonie et la diffusion?
- Les nouveaux régimes seront-ils développés en se focalisant principalement sur l'Internet?
- La régulation de la convergence devrait-elle être conduite par les autorités publiques (organisations internationales et Etats) ou par autorégulation?

Certains pays, comme la Malaisie et la Suisse, aussi bien que ceux de l'UE, ont commencé à donner des réponses à ces questions. La Malaisie a adopté le 'Communication and Multimédia Act' en 1998, établissant un cadre général pour la régulation de la convergence. Les nouvelles directives du cadre de l'UE, maintenant transformées en lois nationales, constituent également un pas dans cette direction, comme c'est le cas des lois et régulations des télécommunications suisses.

### Le danger de convergence: fusion entre opérateurs par câble et ISPs

Dans beaucoup de pays, l'Internet à large bande a été introduit à travers les réseaux de câble. Ceci est surtout vrai pour les Etats Unis où l'Internet par câble est beaucoup plus répandu que l'ADSL (Asymmetric Digital Subscriber Line), l'autre principale option de l'Internet à large bande. Quelles sont les risques associés à cette convergence?

Certaines parties disent que les opérateurs de câbles qui opèrent entre utilisateurs et l'Internet pourraient défier le principe de la neutralité du réseau.

La différence majeure entre ADSL et le câble est que le câble n'est pas régulé par les soi-disantes règles du 'common carrier'. Ces règles, applicables au

système de téléphonie, spécifient que l'accès devrait être non-discriminatoire. Les opérateurs de câble ne sont pas soumis à ces règles, et ont ainsi le contrôle total sur l'accès à l'Internet de leurs abonnés. Ils peuvent bloquer l'utilisation de certaines applications et contrôler l'accès à certains matériels. Les possibilités de surveillance et par conséquent l'aptitude à violer l'intimité sont plus grandes avec l'Internet par câble puisque l'accès est contrôlé à travers un système semblable aux réseaux locaux qui fournissent un haut niveau de contrôle direct des utilisateurs.

Dans un article sur cette question, 'l'Américain Civil Liberties Union' donne l'exemple suivant sur les risques des monopoles de l'internet par câble:

*'Ceci est comme si la société de la téléphonie était autorisée à tenir des restaurants qui fournirait de bons services et des signaux efficace aux clients qui appellent Dominos et par contre des signaux souvent occupés, déconnectés et garderaient bloqués ceux qui appellent Pizza Hut.'*<sup>54</sup>

Ce problème de convergence sera résolu quand une décision sera prise, à savoir si l'internet par câble est 'un service d'information' ou un service de télécommunication. Si cette dernière option est prise, il devra être régulé à travers les règles du 'common carrier'.

## La cyber sécurité

### La situation actuelle

L'Internet était à l'origine conçu pour être utilisé par un cercle fermé, principalement des universitaires sans préoccupation concernant la sécurité. Ils communiquaient ouvertement et évoquaient les probables problèmes de sécurité de façon informelle.

La cyber sécurité a ravi la vedette du débat avec l'expansion rapide de la base des utilisateurs de l'Internet. L'Internet a réitéré le vieux paradoxe selon lequel la technologie peut être à la fois facilitatrice et obstacle en même temps. Ce qui peut être utilisé en faveur du bien être de la société peut aussi l'être à son désavantage.

Une des conséquences de l'intégration rapide de l'Internet dans presque tous les aspects de l'activité humaine est une vulnérabilité accrue de la société moderne. L'Internet est une partie de l'infrastructure critique globale. D'autres services au cœur de la société moderne tels que le réseau électrique,

les systèmes de transport et les services de santé dépendent de plus en plus de l'Internet. Ils sont des cibles fréquentes de cyber-attaques.

Les problèmes de cyber sécurité peuvent être classés en trois catégories:

- 1 Le type d'action.** La classification basée sur le type d'action peut inclure l'interception des données, l'interférence des données, l'accès illégal, le spyware, la corruption des données, le sabotage, le déni de service et le vol d'identité.
- 2 Le type d'auteurs.** Les malfaiteurs pourraient inclure les pirates, les cybercriminels, les cyber-guerriers et les cyber-terroristes.
- 3 Le type de cible.** Les cibles potentielles sont nombreuses peuvent inclure des individus, des sociétés privées, et des institutions publiques aux infrastructures critiques, les gouvernements et les installations militaires.

### Les initiatives politiques pour la cyber sécurité

Beaucoup d'initiatives générales, régionales et nationales se focalisent sur la cyber sécurité. Au niveau national, un nombre croissant de juridictions et de jurisprudence traite de la cyber sécurité. Les initiatives juridiques les plus importantes sont celles des États Unies et sont liées à la lutte contre le terrorisme où le 'Department of Homeland Security' est la principale institution en charge des problèmes de cyber sécurité. Il est difficile de trouver un pays développé sans aucune initiative sur la cyber sécurité.

Au niveau international, l'UIT est l'organisation la plus active ; elle a produit un grand nombre de cadres de sécurité, des architectures, et des standards, y compris X.509, qui fournit la base pour l'infrastructure à clé publique (Public Key Infrastructure – PKI) utilisée, par exemple, dans la version sécurisée du HTTP(s) (Protocole de transfert hypertexte (sécurisé)). Récemment, l'UIT est allée au-delà des aspects strictement techniques et a lancé l'agenda global de cyber sécurité de l'UIT.<sup>55</sup> Cette initiative englobe les mesures juridiques, la coopération politique, et le renforcement des capacités.

Le G8 a également quelques initiatives dans le domaine de la cyber sécurité conçues pour améliorer la coopération entre les agences de mise en exécution de la loi. Il a formé un sous-groupe sur le crime par la haute technologie pour établir une communication 24/7 entre les centres de cyber sécurité des états membres, la formation du *staff*, et l'amélioration des systèmes légaux des états pour combattre la cybercriminalité et promouvoir une coopération entre l'industrie des TIC et les agences d'exécution de la loi.

L'Assemblée Générale des Nations Unies a voté plusieurs résolutions sur une base annuelle et sur les 'développements dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale', spécialement les résolutions 53/70(1998), 54/49(1999), 55/28(2000), 56/19(2001), 57/239(2002) et 58/199(2003). Depuis 1998, toutes les résolutions subséquentes ont un contenu similaire, sans améliorations significatives.

En dehors de ces résolutions de routine, la principale percée était le récent établissement des recommandations pour les négociations du traité sur la cyber sécurité, qui était soumis au Secrétaire général des Nations Unies par quinze Etats membres, y compris tous les membres permanents du Conseil de Sécurité des Nations Unies.

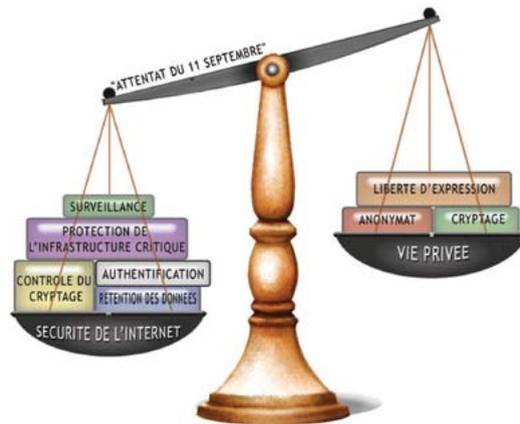
Comme instrument juridique international majeur lié à la cyber sécurité, l'on peut citer la Convention du Conseil de l'Europe sur la cyber sécurité qui entra en vigueur le 1<sup>er</sup> juillet 2004.<sup>56</sup> Certains pays ont établi des accords bilatéraux; par exemple, les Etats Unis ont signé des accords bilatéraux sur la coopération juridique en matière criminelle avec plus de 20 pays.<sup>57</sup> Ces accords s'appliquent aussi aux cas de cybercriminalité.

Comme tentative initiée par les universitaires et acteurs non-étatiques pour ébaucher un accord international, l'on peut mentionner le 'Stanford Draft Convention on Protection from Cyber Crime and Terrorism'. Ce projet recommande l'établissement d'une structure internationale: l'Agence pour la protection de l'infrastructure de l'information (Agency for Information Infrastructure Protection – AIIP).

## Les enjeux

### L'influence de l'architecture de l'Internet sur la cyber sécurité

La nature même de son organisation affecte la sécurité de l'Internet. Pourrions-nous garder l'approche actuelle qui consiste à bâtir l'Internet sur une base non-sécurisée ou modifier la base de l'infrastructure de l'Internet? Comment un tel changement affecterait-il d'autres caractéristiques de l'Internet, spécialement son caractère ouvert et sa transparence? La plupart des développements passés des standards de l'Internet visaient à améliorer la performance ou à introduire de nouvelles applications; la sécurité n'était pas une priorité.



Il n'est pas évident que l'IETF sera capable de changer les standards des e-mails pour fournir l'authentification appropriée, et en fin de compte, réduire les abus sur l'Internet (exemple: le pollupostage, le cyber crime). Etant donné la controverse autour des changements sur les fondements des standards d'Internet, il est probable que les améliorations liées à la sécurité dans les fondements du protocole Internet seront graduelles et lentes.

### Le futur développement du commerce en ligne exige un niveau élevé de cyber sécurité

La cyber sécurité est souvent mentionnée comme l'un des préalables pour la croissance rapide du commerce électronique. Sans un Internet sûr, les clients seront hésitants à fournir des informations confidentielles en ligne, telles que les numéros de carte de crédit. Il en est de même pour les services bancaires en ligne et l'usage de la monnaie électronique. Si la cyber sécurité générale ne s'améliore que lentement (avec, par exemple, un manque de standards), il est probable que le secteur des affaires fasse pression pour qu'il y ait des développements plus rapides. Cela peut conduire vers plus de défis dans le cadre du principe de la neutralité du réseau et le développement d'un 'nouvel Internet', qui faciliterait notamment, la sécurisation de la communication sur Internet.

### Le respect de la vie privée et la cyber sécurité

Un autre problème débattu est la relation entre la sécurité et le respect de la vie privée. Les mesures additionnelles de la cyber sécurité impliqueront-elles une certaine érosion dans le respect des droits à la vie privée? Quelle régulation s'appliquerait aux logiciels de cryptage, qui peuvent être utilisés à la fois pour la protection légitime de la communication privée et pour la protection des communications des terroristes et des criminels? Les réponses

à ces questions ainsi qu'à d'autres dépendent de l'équilibre, qui change constamment, entre la cyber sécurité et le respect de la vie privée.

Aussitôt après l'attaque terroriste à New York, en septembre 2001, la sécurité est devenue une priorité, et cela s'est reflété par l'adoption de plusieurs lois nationales qui stipulaient entre autre, des niveaux plus élevés de surveillance de l'Internet. La réaction de la société civile s'est centrée sur les dangers concernant le respect de la vie privée et sur le concept de la liberté d'expression.

Au niveau international, la question d'équilibre entre la cyber sécurité et la protection de la vie privée a été au centre des discussions sur l'extension de la Convention du Conseil de l'Europe sur le cyber crime au niveau global. La principale objection des activistes des droits de l'Homme est que la Convention traite des questions de cyber sécurité au détriment de la protection de la vie privée et d'autres droits humains.

## **Le cryptage**

Un des points au centre du débat sur la sécurité de l'Internet concerne le cryptage, qui a trait aux outils qui peuvent être utilisés pour la protection des échanges de données.

Un logiciel de cryptage brouille la communication électronique (e-mail, images) en texte illisible en utilisant des algorithmes mathématiques. L'équilibre entre le besoin de garder certaines informations confidentielles et le besoin des gouvernements de surveiller l'activité terroriste et potentiellement criminelle demeure un problème.

Les aspects internationaux de la politique du cryptage sont pertinents dans la discussion sur la Gouvernance de l'internet étant donné que la régulation du cryptage devrait être internationale, ou du moins, impliquer les pays capables de produire des outils de cryptage.

Ainsi par exemple, la politique des Etats Unis sur le contrôle de l'exportation de logiciels de cryptage n'avait guère bien réussi car elle ne contrôlait pas la distribution internationale de logiciels de chiffrement. Les éditeurs américains de ces logiciels ont initié une forte campagne de pression soutenant que les contrôles à l'exportation ne renforcent pas la sécurité nationale mais plutôt minent les intérêts du commerce américain.

### Régimes internationaux concernant les outils de cryptage

Le cryptage a été abordé dans deux contextes: l'engagement de Wassenaar et l'OCDE. L'engagement de Wassenaar est un régime international adopté par 33 pays industrialisés pour restreindre l'exportation des armes conventionnelles et les technologies à 'double usage' aux pays en guerre ou jugés être des 'Etats paria'. L'accord a mis en place un Secrétariat à Vienne. Le lobbying des Etats Unis, avec le groupe Wassenaar, visait à étendre l'*approche 'Clipper'*<sup>58</sup> au plan international, en contrôlant les logiciels de cryptage au moyen d'un système de tierce confiance. Cela engendra la résistance de nombreux pays, notamment le Japon et les pays scandinaves.

Un compromis fut trouvé en 1998 par l'introduction des directives de cryptographie, qui comprenaient la liste de contrôle à double-usage de produits – machines et logiciels – de cryptographie de plus de 56 bits. Cette extension comprenant des outils Internet tels que les navigateurs-web et l'e-mail. Il est intéressant de noter que cet accord ne couvre pas les transferts 'intangibles', comme les téléchargements. L'échec de l'adoption d'une version internationale de 'clipper' a contribué au retrait de cette proposition au sein des Etats Unis mêmes. Dans cet exemple de corrélation entre les arènes nationales et internationales, les développements internationaux ont eu un impact décisif sur l'évolution nationale.

L'OCDE est un autre forum pour la coopération internationale dans le domaine du cryptage. Quoique l'OCDE ne produise pas de documents juridiques ayant force de loi, ses directives sur des questions variées sont hautement respectées. Elles sont le résultat d'une approche d'experts et d'un processus de prise de décision basé sur le consensus. La plupart de ses directives sont éventuellement incorporées dans les lois nationales. La question du cryptage fut un sujet hautement controversée au cours des travaux de l'OCDE. Elle a été initiée en 1996 suite à une proposition américaine prônant l'adoption d'un système à tiers de confiance en guise de norme internationale. Comme dans le cas de Wassenaar, les négociations sur la proposition américaine firent l'objet d'une forte opposition du Japon et des pays scandinaves. Les pourparlers débouchèrent sur un compromis de spécification concernant les principaux éléments de la politique de cryptage.

Ces quelques tentatives pour développer un régime international de cryptage, principalement dans le contexte de l'Arrangement de Wassenaar n'a pas abouti au développement d'un régime international effectif. Il est encore possible d'obtenir un puissant logiciel de cryptage sur Internet.

## Pollupostage et 'mode politique'

Le pollupostage est un exemple flagrant des tendances et parfois de mode en matière d'orientation de politique générale. En 2005, le pollupostage était listé comme un problème significatif de Gouvernance de l'Internet dans le rapport du GTGI. Le spam était discuté lors du SMSI de Tunis et lors de nombreuses rencontres internationales. Il était aussi souvent à la une des médias.

Depuis 2005, le volume du pollupostage a augmenté de six fois, selon les estimations (2005: 30 milliards de messages par jour ; 2010: 183 milliards de messages par jour).

L'importance politique du pollupostage ne suit pas sa tendance. Le pollupostage a actuellement une très faible visibilité dans les processus de politique générale. Au FGI de 2009 à Sharm El Sheikh, il n'y avait aucun atelier ou session pour discuter du pollupostage. Toutefois, l'importance du pollupostage dans la politique globale reste encore à découvrir.

## Pollupostage

### La situation actuelle

Le pollupostage est souvent défini comme du courrier électronique non sollicité qui est envoyé à un grand nombre d'utilisateurs d'Internet. Tandis qu'il est principalement utilisé pour la promotion commerciale, ses autres usages incluent l'activisme social, la campagne politique et la distribution de matériels pornographiques. Le pollupostage est classé dans la corbeille infrastructure parce qu'il affecte le fonctionnement normal de l'Internet en empêchant le bon fonctionnement de l'une de ces applications centrales: le courrier électronique. Le pollupostage est l'un des problèmes de la Gouvernance de l'Internet qui affecte presque tout individu qui s'y connecte. Selon les statistiques de 2009, 81 % du trafic des messages électroniques étaient du pollupostage. Le volume du pollupostage entre 2008 et 2009 a augmenté de 24 %. En plus du fait qu'il soit ennuyeux pour les utilisateurs, le pollupostage cause aussi des pertes économiques considérables, à la fois en terme de bande passante utilisée et en terme de temps perdu pour sa vérification et sa suppression.



Le pollupostage peut être combattu à la fois à travers les moyens juridiques et techniques. Du point de vue technique, beaucoup d'applications pour filtrer les messages et détecter le pollupostage sont disponibles. Le problème fondamental avec les systèmes de filtrage est qu'ils sont connus pour également supprimer des messages non indésirables. L'industrie anti-pollupostage est un secteur en pleine croissance avec de plus en plus d'applications sophistiquées capables de distinguer les messages indésirables des messages réguliers. Les méthodes techniques n'ont qu'un effet limité et exigent les mesures juridiques complémentaires.

Sur le plan technique, beaucoup d'États-nations ont réagi en produisant de nouvelles lois anti-pollupostage. Aux États Unis, la loi 'Can-spam' tient compte d'un équilibre délicat entre, permettre la promotion basée sur le courrier électronique et la lutte contre le spam.<sup>59</sup> Bien que la loi prescrive les sanctions sévères pour la distribution de courriers indésirables, y compris l'emprisonnement pendant des années, certaines de ses dispositions, selon des critiques, tolèrent ou pourraient même encourager l'activité du pollupostage. Le point de départ 'par défaut' tel qu'énoncé dans la loi est que le pollupostage est permis jusqu'à ce que le réceptionneur des messages indésirables dise 'non' par intermédiaire d'une clause d'exclusion. Depuis l'adoption de la loi en décembre 2003, les statistiques n'ont pas mis en évidence une quelconque décroissance du nombre de messages indésirables.

En juillet 2003, l'UE a introduit sa propre législation anti-pollupostage comme faisant partie de sa Directive sur la vie privée et des communications électroniques. La loi de l'UE encourage l'autorégulation et les initiatives du secteur privé qui conduiraient à une réduction des courriers électroniques indésirables.<sup>60</sup>

En novembre 2006, la Commission Européenne a adopté sa Communication pour combattre le pollupostage, le *logiciel espion* et le logiciel malicieux. La Communication identifie un nombre d'actions pour promouvoir l'application de la loi existante comme souligné plus haut, étant donné que la non-exécution est considérée comme le problème majeur.<sup>61</sup>

### La réponse internationale

Les deux lois anti-pollupostage adoptées aux États Unis et dans l'UE ont une faiblesse: le manque de dispositions pour empêcher le pollupostage transfrontalier. Cette question est particulièrement pertinente dans certains pays tels que le Canada, qui, selon les dernières statistiques, reçoit 19 sur 20 des courriers indésirables depuis l'étranger.

La Ministre canadienne de l'industrie, Lucienne Robillard a dit que le problème ne peut pas être résolu sur une base 'pays-pays'. Une solution globale est nécessaire, renforcée à travers un traité international ou un mécanisme similaire.

Un Mémoire d'Entente signé par l'Australie, la Corée et le Royaume Uni est l'un des premiers exemples de la coopération internationale dans la campagne anti-pollupostage.

L'OCDE a établi un groupe de travail sur le pollupostage et a préparé une boîte à outil anti-pollupostage. L'UIT a également été proactive en organisant la rencontre thématique sur la lutte contre le pollupostage (2004) dans le but d'explorer les différentes possibilités d'établissement d'un Mémoire d'entente global pour combattre le pollupostage. Au niveau régional, l'UE a établi le réseau d'agences de lutte anti-pollupostage, l'APEC a préparé un dispositif de directives pour le consommateur.

Une autre approche possible d'anti-pollupostage a été entreprise par les grands groupes Internet qui hébergent les comptes de courrier électronique: American online, British Telecom, Comcast Earth Link, Microsoft et Yahoo ! Elles avaient établi l'Alliance technique anti-pollupostage (Anti-Spam Technical Alliance – ASTA) qui aurait pour tâche principale de coordonner les activités techniques et celles relatives à la politique anti-pollupostage.

## Les enjeux

### Les différentes définitions du pollupostage

Les différentes définitions du pollupostage affectent la campagne anti-pollupostage. Aux Etats Unis, une préoccupation générale au sujet de la protection de la liberté d'expression et du Premier Amendement affecte également la campagne anti pollupostage. Les législateurs américains considèrent comme pollupostage un courrier électronique commercial uniquement non sollicité, oubliant d'autres types de courriers indésirables qui comprennent l'activisme politique et la pornographie. Dans la plupart des autres pays, le pollupostage est considéré comme étant tout courrier électronique non sollicité en grande quantité quelque soit son contenu. Puisque la majeure partie des courriers électroniques indésirables sont produits aux Etats Unis, cette différence dans les définitions limite sérieusement toute possibilité d'introduire un mécanisme international effectif d'anti-pollupostage.

### **Le pollupostage et l'authentification du courrier électronique**

L'un des facteurs structurels favorisant le pollupostage est la possibilité d'envoyer des courriers électroniques avec une adresse d'expéditeur falsifiée. Il existe une solution technique à ce problème qui exigerait des changements dans les standards existants du courrier électronique sur l'Internet. L'IETF travaille à apporter les changements au protocole du courrier électronique qui assureraient l'authentification du courrier électronique. Ceci est un exemple de la manière dont les problèmes techniques peuvent affecter la politique. Un compromis possible serait que l'introduction de l'authentification du courrier électronique apporterait la restriction de l'anonymat sur l'Internet.

### **Le besoin d'une action globale**

La plupart des courriers électroniques indésirables envoyés vers un pays donné proviennent de l'étranger. C'est un problème mondial qui exige une solution mondiale. Il y a plusieurs initiatives qui pourraient conduire à une meilleure coopération globale. Certaines d'entre elles telles que les Mémoires d'entente bilatéraux ont déjà été mentionnés. D'autres incluent certaines actions comme le renforcement des capacités et l'échange d'informations. Une solution plus intégrée impliquerait une sorte d'instrument anti-pollupostage mondial. Jusqu'à présent, les pays développés préfèrent le renforcement des lois nationales couplées aux campagnes anti-pollupostage régionales ou bilatérales. Etant donné leur position défavorisée de recevoir un, 'mal public universel' provenant principalement des pays développés, la plupart des pays en développement sont intéressés à la formulation d'une réponse globale au problème du pollupostage.

## Notes de fin

- <sup>1</sup> Les termes ' Internet ' et toile d'araignée mondiale (World Wide Web) sont parfois utilisés de façon interchangeable; cependant, il ya une différence. L'Internet est un vaste réseau des réseaux; il couvre un nombre de services différents. Parfois le terme Internet est utilisé de manière globalisante, comprenant l'infrastructure, les applications (courrier électronique, ftp, la Toile) et le contenu. La toile d'araignée mondiale est juste l'une des nombreuses applications de l'internet, un système de documents liés et connectés à l'aide du protocole ' Hyper Text Transfer Protocol (HTTP) '.
- <sup>2</sup> La transmission de l'Internet à travers un réseau électrique est appelé Courant Porteur en Ligne. L'usage du réseau électrique rendrait l'Internet plus accessible à beaucoup d'utilisateurs. Pour une révision technique et organisationnelle de cette fonction, voir: Internet Society (2003) *Addressing the digital divide with IPv6-enabled broadband power line communications (Résoudre la fracture numérique par la technologie des connexions Internet haut débit utilisant le courant porteur en ligne avec le protocole IPv6* . ISOC Member Briefing No. 13. Disponible sur: <http://www.isoc.org/briefings/013/>
- <sup>3</sup> La libéralisation des marchés de télécommunication dans les pays membres de l'OMC a été rendue formelle en 1998 dans le ' Basic Telecommunication Agreement (BTA) ' . Après l'adoption du BTA, 100 pays ont commencé le processus de libéralisation, caractérisé par la privatisation des sociétés nationales de télécommunication qui avaient le monopole dans le domaine, l'introduction de la concurrence et l'établissement des régulateurs nationaux. L'accord est formellement appelé le ' The Fourth Protocol to the General Agreement on Trade in Services ' adoptés le 30 Avril 1996 et entré en vigueur le 5 février 1998. Disponible sur [www.wto.org/english/tratop\\_e/serv\\_e/4prote\\_e.htm](http://www.wto.org/english/tratop_e/serv_e/4prote_e.htm)
- <sup>4</sup> Pour plus d'information sur le rôle de l'OMC dans le domaine des télécommunications, voir: [http://www.wto.org/english/tratop\\_e/serv\\_e/telecom\\_e/telecom\\_e.htm](http://www.wto.org/english/tratop_e/serv_e/telecom_e/telecom_e.htm)
- <sup>5</sup> L'opinion commune est que les Etats peuvent collecter plus de recettes à partir du monopole du marché par les opérateurs nationaux ; les adversaires soutiennent qu'avec la libéralisation du marché, la valeur totale du marché a augmenté, apportant par conséquent plus de revenus à l'Etat par rapport à la situation du monopole.
- <sup>6</sup> Actuellement, les RIR sont l'ARIN (le registre américain des nombres d'Internet), l'APNIC (le réseau du centre d'information Asie -Pacifique), LACNIC (le registre régional de l'Amérique Latine et des Caraïbes pour les adresses IP), RIPE NCC (le centre de coordination du réseau des réseaux IP européens- couvrant l'Europe et le Moyen orient), et l'AFRINIC (le centre d'information du réseau africain). Une explication détaillée du système RIR est disponible à: <https://www.ripe.net/info/resource-admin/rir-system.html>
- <sup>7</sup> Pour un débat détaillé à propos de l'IPv6, voir: Kissangou JP, Guthrie M, Njiraini M (2005) *allocation des IPv4 et IPv6, dans le cadre du programme de renforcement de capacité de la GI*. Disponible sur: <http://textus.diplomacy.edu/Textusbin/portal/Ghome.asp?IDspace=84>
- <sup>8</sup> Pour une étude hautement technique et complète sur la sécurité du TCP/IP, voir: Chambers C, Dolske J, lyre J (ND) *TCP/IP Security, Department of Computer and Information Science, Ohio State University: Columbus, OH, USA*. Disponible sur: [http://www.linuxsecurity.com/resource\\_les/documentation/tcpip-security.html](http://www.linuxsecurity.com/resource_les/documentation/tcpip-security.html)
- <sup>9</sup> Abbate J (1999) *Inventing the Internet*. MIT Press: Cambridge, MA, USA.

- 10 Une vue d'ensemble des gTLD avec un lien à la liste de tous les TLDS est disponible sur: <http://www.icann.org/registries/about.htm>
- 11 Un exemple antérieur des domaines liés au contenu concernant les enfants est le domaine kids.us. Le Congrès des Etats-Unis d'Amérique a adopté une loi introduisant le domaine réservé au contenu convivial pour enfant. La principale difficulté avec cette proposition est de décider sur ce qui constitue le contenu convivial pour l'enfant. Une controverse conceptuelle et des problèmes pratiques liés au contrôle du contenu pourraient en résulter. Jusque-là, le domaine 'kids' n'a été utilisé que comme une partie du domaine américain.
- 12 Le gouvernement des Etats-Unis n'a pas suivi les procédures de prise de décision de l'ICANN pendant les discussions sur le domaine xxx. L'opposition des Etats-Unis s'est exprimée à travers une lettre envoyée par le ministre du commerce américain au Président d'ICANN.
- 13 Le formulaire d'enregistrement du domaine .cat est disponible sur: <http://www.icann.org/tlds/stdl-apps-19mar04/cat.htm>
- 14 Le rapport de l'IANA sur le ccTLD pour la Palestine est disponible sur: <http://www.iana.org/reports/ps-report-22mar00.htm>
- 15 Par exemple, l'Afrique du Sud a utilisé ses droits souverains comme un argument pour reprendre le contrôle de son domaine national. Une loi nouvellement promulguée spécifie que l'utilisation du domaine national hors des paramètres prescrits par le gouvernement Sud-Africain serait considéré comme un crime. Le modèle brésilien de gestion des domaines nationaux est souvent été montré comme un exemple réussi d'une approche multi parties-prenantes. Le corps national en charge des domaines brésiliens est ouvert à tous les protagonistes-clés, y compris les autorités gouvernementales, le secteur privé, et la société civile. Le transfert cambodgien de la gestion du domaine national du contrôle non gouvernemental au contrôle gouvernemental est souvent cité comme un exemple de transition échouée. Le gouvernement avait réduit la qualité des services et introduit des frais plus élevés qui ont rendu l'enregistrement des domaines cambodgiens beaucoup plus difficiles. Pour plus d'information, voir: Alfonso CA (2004) *BR: CCTLD An asset of the commons*, in *Internet Governance: A grand collaboration*. MacLean D (ed.). UNICT Task Force: New York, NY, USA, pp. 291–299; Klein N (2004) Internet governance: Perspectives from Cambodia, in *Internet Governance: A grand collaboration. op. cit.*
- 16 ICANN (2000) *Principles for the Delegation and Administration of Country Code Top-Level Domains*, currently being redrafted. Available at: <http://www.icann.org/committees/gac/gac-cctldprinciples-23feb00.htm>
- 17 La liste des serveurs racines de zone, leurs nœuds et positions, ainsi que les organisations en charge de leur gestion est disponible sur: <http://www.root-servers.org/>
- 18 ICANN (2009) Available at <http://www.icann.org/en/announcements/announcement-30sep09-en.htm>
- 19 La section sur la neutralité du serveur est basée sur les écrits de Vladimir Radunovic, coordonateur du projet sur la Gouvernance de l'Internet de DiploFoundation.
- 20 Durant toute l'histoire de l'Internet, les Etats-Unis n'ont jamais bloqué l'accès à un autre pays y compris les pays en conflit. Dans certains cas, comme durant la guerre du Kosovo de 1999, le régime des sanctions des NU donnait aux Etats-Unis le droit de rompre les communications avec la Serbie. N'ayant pas utilisé cette possibilité légale, ainsi la Serbie a gardé l'accès à l'Internet durant tout le conflit.

- <sup>21</sup> Arrington M (2009) You tube vidéo diffuse un maximum de 1,2 milliards de vidéo par jour. TechCrunch. Disponible à: <http://www.techcrunch.com/2009/06/09/youtume-strime-video-top-1-billionday/>
- <sup>22</sup> Faire la diffusion nous-même. Le bureau du blogue de YouTube (2009) Zoinks! 20 heures de vidéo mises en ligne chaque minute! Disponible sur: [http://youtube-global.blogspot.com/2009/05/zoinks-20-hours-of-video-uploaded-every\\_20.html](http://youtube-global.blogspot.com/2009/05/zoinks-20-hours-of-video-uploaded-every_20.html)
- <sup>23</sup> L'Amérique insiste sur la neutralité du net: The right of bits. *The Economist* 24 September 2009.
- <sup>24</sup> Ce cas a connu plusieurs bouleversements. Pour plus d'information sur l'historique de ce cas, voir: Broache A (2008) FCC veut savoir: le fait de dégrader le trafic Pair à Pair est-il raisonnable? Cent News Blog. Disponible sur [http://news.cnet.com/8301-10784\\_3-9850611-7.html?tag=mncol;txt](http://news.cnet.com/8301-10784_3-9850611-7.html?tag=mncol;txt)
- La mise à jour la plus récente fut la décision de la cour contre la réglementation antérieure de FCC, voir Kang C (2010), Court rules for Comcast over FCC in 'net neutrality' case. Le Washington Post, 7 avril. Disponible sur <http://www.washingtonpost.com/wp-dyn/content/article/2010/04/06/AR2010040600742.html>
- <sup>25</sup> ' Save the Internet ' est particulièrement actif en recommandant la neutralité du réseau comme moyen de préserver l'ouverture et la liberté sur l'Internet.
- <sup>26</sup> L' 'Internet Governance Caucus (IGC)' était à l'origine créé par les acteurs individuels et des organisations de la société civile qui se mirent ensemble dans le contexte du SMSI pour promouvoir les objectifs de l'intérêt public général dans la mise en place de la Gouvernance de l'Internet. Disponible sur: [www.igcaucus.org](http://www.igcaucus.org)
- <sup>27</sup> John Herman illustre les offres de packages souvent utilisés par les protagonistes de la neutralité du réseau. Disponible sur: <http://gizmodo.com/5391712/net-neutrality-worst-case>
- <sup>28</sup> La *quadrature du Net*, un groupe de défense qui fait la promotion des droits et libertés des citoyens sur l'internet, affirme dans sa lettre ouverte au parlement européen concernant la neutralité du réseau: *Everyone around the globe has access to the same Internet, and even the smallest entrepreneurs are on equal footing with the leading global enterprises (toute personne sur la terre a accès au même et unique Internet, et donc même le plus petit entrepreneur est sur le même pied d'égalité que les grands groupes mondiaux)*. Disponible sur: <http://www.laquadrature.net/en/we-must-protect-net-neutrality-in-europe-openletter-to-the-european-parliament#>
- <sup>29</sup> Ogg E (2010) *Report: Google, Verizon reach Net neutrality deal*. CNet 4 August. Disponible sur: [http://news.cnet.com/8301-31021\\_3-20012703-260.html?tag=mncol;mlt\\_related](http://news.cnet.com/8301-31021_3-20012703-260.html?tag=mncol;mlt_related)
- <sup>30</sup> Ces éléments qui sont encore controversés et négociés dans l'avenir sont entre parenthèses.
- <sup>31</sup> Les rapports de ces réunions aussi bien que d'autres éléments pertinents sur la neutralité du réseau, sont disponibles sur: [www.diplomacy.edu/ig/nn](http://www.diplomacy.edu/ig/nn)
- <sup>32</sup> Le journal de la politique de (FCC 2005) sur la gestion et la neutralité du réseau. Disponible sur: [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/FCC-05-151A1.pdf](http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf)
- <sup>33</sup> Ministère de l'intérieur et des communications, Japon (2007), Rapport sur la neutralité du réseau. Disponible sur: [www.soumu.go.jp/main\\_sosiki/joho\\_tsusin/eng/pdf/070900\\_1.pdf](http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pdf/070900_1.pdf)

- <sup>34</sup> PTS (2009) *Open Networks and Services*. Disponible sur: <http://www.pts.se/en-gb/Documents/Reports/Internet/2009/Open-Networks-and-Services---PTS-ER-200932/>
- <sup>35</sup> Kroes N (2010) *Net neutrality in Europe*. Discours prononcé par le Vice Président de la Commission Européenne pour l'Agenda Numérique. Disponible sur: <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/153&format=HTML&aged=0&language=EN&guiLanguage=en>
- <sup>36</sup> NPT (2009) *Net neutrality: Guidelines for Internet neutrality*. Disponible sur: <http://www.npt.no/ikbViewer/Content/109604/Guidelines%20for%20network%20neutrality.pdf>
- <sup>37</sup> Anderson N (2009) *Norway gets net neutrality – voluntary, but broadly supported. Ars Technica*. Disponible sur: <http://arstechnica.com/tech-policy/news/2009/02/norway-getsvoluntary-net-neutrality.ars>
- <sup>38</sup> ISOC considère le concept de la neutralité du réseau plutôt (comme) mal défini et discute plutôt de l'ouverture et de l'interopérabilité continue des réseaux. Disponible sur: <http://www.isoc.org/pubpolpillar/usercentricity/openinternetworking.shtml>. Sa consultation du 16 mai sur la neutralité du net affirme qu': ' *Au lieu de se focaliser simplement sur une gamme de définitions possibles de la neutralité du réseau, l'Internet Society croit qu'il est plus approprié de se focaliser plus ouvertement sur l'impératif de la préservation d'un modèle d'Internet ouvert, centré sur l'utilisateur, lequel a eu du succès jusqu'à ce jour* ' ( *Rather than focusing simply on the range of possible Network Neutrality definitions, the Internet Society believes it is more appropriate to concentrate more broadly on the imperative of preserving the open, user-centric Internet model that has been so successful to date*). Disponible sur: [http://www.isoc.org/regions/europe/docs/netneutrality\\_20100516\\_en.pdf](http://www.isoc.org/regions/europe/docs/netneutrality_20100516_en.pdf)
- <sup>39</sup> *TACD calls for Net Neutrality*. Disponible sur: [http://tacd.org/index.php?option=com\\_content&task=view&id=162&Itemid=43](http://tacd.org/index.php?option=com_content&task=view&id=162&Itemid=43)
- <sup>40</sup> Williams F (2006) *ISPs should be liable for spam*, souligne le rapport des Nations Unies. *Financial Times*, 8 Novembre. Disponible sur: <http://www.qlinks.net/quicklinks/spam.htm>
- <sup>41</sup> Shannon V (2006) *The end user: Junk payout in spam case. International Herald Tribune*, 13 Avril. Disponible sur: <http://www.iht.com/articles/2006/04/12/business/PTEND13.php>
- <sup>42</sup> Le ' Peering ' est un accord bi- latéral fait par les opérateurs de réseau pour garantir l'accès aux clients des uns et des autres sans coût pour toutes les parties; comme défini par le groupe HSC. ([www.hscgroup.co.uk](http://www.hscgroup.co.uk)). L'arrangement ' Peering ' est un bénéfice mutuel et il est aussi courant chez les FAI que chez les opérateurs de télécom.
- <sup>43</sup> Au niveau 2, se trouve des FBP (Fournisseurs de Bande Passante) généralement appelés Points de Connexion Internet (PCI) ou Passerelles d'Internet.
- <sup>44</sup> Andrew Odlyzko voit la question de fixation de prix et d'architecture sur l'internet dans une perspective historique. Identifiant l'évolution de la politique de fixation de prix pratiquée dans les systèmes de transport dans l'ancien monde, il en fait une liaison avec la politique actuelle de fixation des prix de l'internet. Odlyzko A (2004) *Pricing and architecture of the Internet: Historical perspectives from telecommunications and transportation*. University of Minnesota: Minneapolis, MN, USA. Disponible sur: [http://www.dtc.umn.edu/\\_odlyzko/doc/pricing.architecture.pdf](http://www.dtc.umn.edu/_odlyzko/doc/pricing.architecture.pdf)

- <sup>45</sup> Shawn O'donnell, dans l'article *An economic map of the Internet*, fournit une analyse de comment le dollar de l'internet est distribué, expliquant où va le dollar que le consommateur paye au FAI, disponible sur: [http://ebusiness.mit.edu/research/papers/162\\_ODonnell\\_Map.pdf](http://ebusiness.mit.edu/research/papers/162_ODonnell_Map.pdf)
- <sup>46</sup> Nguyen TT, Armitage GJ (2005) Evaluating Internet pricing schemes: A three-dimensional visual model. *ETRI Journal* 27: 64–74.
- <sup>47</sup> Le site web du marché de la bande passante est un marché en ligne des ressources de l'internet, offrant la bande passante, l'accès à l'Internet et d'autres ressources d'Internet. Disponible sur: <http://www.bandwidthmarket.net/>
- <sup>48</sup> Huston G (2005) 'Where's the money? – Internet interconnection and \_ financial settlements'. The ISP Column, Internet Society. Disponible sur: <http://ispcolumn.isoc.org/2005-01/interconns.pdf>
- <sup>49</sup> AfrISPA (2002) the half way proposition: Un article sur la subvention en sens inverse des pays du G8 par les FAI africains, présenté à la conférence des ministres africains des finances, de la planification et du développement économique, Johannesburg, Afrique du sud, 19 octobre 2002. Disponible sur: [http://www.wougnet.org/WSIS/ug/WSIS2005/docs/HalfwayProposition\\_Draft4.pdf](http://www.wougnet.org/WSIS/ug/WSIS2005/docs/HalfwayProposition_Draft4.pdf)
- <sup>50</sup> Pour une étude complète des coûts d'interconnexion, voir Esmat B., Fernandez J. (2006) 'International Internet Connections Costs', in Drake WJ (2006) *Reforming Internet Governance: Perspectives from the Working Group on Internet Governance* (WGIG). WGIG: New York, NY, USA, pp. 73–86. Disponible sur: <http://www.wgig.org/book-Launch.html>
- <sup>51</sup> Vous pouvez trouver une analyse complète du sujet dans Jensen M (2005) *Interconnection Costs*. APC: Melville, Afrique du Sud. Disponible sur: <http://www.apc.org/en/pubs/issue/accessibility/all/interconnection-costs>
- <sup>52</sup> Huston (2005) *op. cit.* pp. 7-9.
- <sup>53</sup> L'un des obstacles dans la négociation de cette question entre les gouvernements est que la plupart des accords d'interconnexion sont conclus entre les opérateurs de télécommunication privés. Ils sont souvent confidentiels.
- <sup>54</sup> ACLU White paper (ND) *No competition: How monopoly control of the broadband Internet threatens free speech*. ACLU: New York, NY, USA.
- <sup>55</sup> Pour plus d'informations à propos de l'Agenda mondial sur la cyber sécurité de l'UIT, voir: <http://www.itu.int/osg/csd/cybersecurity/gca/>
- <sup>56</sup> Le texte de la convention est disponible sur: <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>
- <sup>57</sup> Le nom officiel de ces instruments est le 'Mutual Legal Assistance in Criminal Matters Treaties' (MLATs): Traités de l'Assistance mutuelle juridique dans le domaine des affaires criminelles.
- <sup>58</sup> L'approche 'Clipper' fut déjà proposée par le gouvernement des Etats-Unis en 1993. Elle reposait sur l'usage de la puce de Clipper qui était supposée être utilisée dans tous les téléphones et autres outils de communication. La puce de Clipper avait une porte arrière qui serait utilisée par les gouvernements pour la surveillance légale. Après une forte opposition des activistes des droits de l'homme et du public en général, le gouvernement des Etats-Unis abandonna cette proposition en 1995. Voir: Denning D (1995) 'The case for

clipper'. *MIT Technology Review*. MIT: Cambridge, MA, USA. Disponible sur: [http://encryption\\_policies.tripod.com/us/denning\\_0795\\_clipper.htm](http://encryption_policies.tripod.com/us/denning_0795_clipper.htm)

- <sup>59</sup> Plus de référence au 'Can-Spam' sont disponibles sur: <http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus61.shtm>
- <sup>60</sup> Le 'Contact Network of Spam Enforcement Authorities (CNSA)' a été mis en place en février 2005 par 13 pays de l'UE (France, Autriche, Belgique, Chypre, République Tchèque, Danemark, Grèce, Irlande, Italie, Lituanie, Malte, Royaume-Uni et Espagne). Il vise à promouvoir la coopération entre ces Etats, et la coordination avec les entités qui sont hors de l'UE, telles que l'OCDE et l'UIT.
- <sup>61</sup> Commission Européenne, Société de l'Information (2010). *Unsolicited communication: fighting spam*. Disponible sur: [http://ec.europa.eu/information\\_society/policy/ecommtodays\\_framework/privacy\\_protection/spam/index\\_en.htm](http://ec.europa.eu/information_society/policy/ecommtodays_framework/privacy_protection/spam/index_en.htm)



## Section 3

---

# La corbeille juridique





# La corbeille juridique

**P**resque tous les aspects de la gouvernance de l'Internet ont une dimension juridique, pourtant la conception d'un cadre juridique pour encadrer le développement rapide de l'Internet en est encore à ses balbutiements. Les deux approches dominantes sont:

- 1 Une approche 'loi-réelle', où l'Internet est en fait traité comme les technologies de télécommunications antérieures depuis la transmission des signaux par la fumée au téléphone. Bien que plus rapide et plus élaboré, l'Internet implique toujours la communication entre individus sur une certaine distance. En conséquence, toutes les règles juridiques existantes peuvent également être appliquées à Internet.<sup>1,2</sup>
- 2 Une approche 'cyber-loi' basée sur la présomption qu'Internet introduit de nouveaux types de rapports sociaux dans le Cyberspace. En conséquence, il y a besoin de formuler de nouvelles cyber-lois afin de réguler le cyberspace. L'un des arguments de cette approche est que la rapidité et le volume de communications transfrontalières, facilité par l'Internet, ne faciliterait pas l'application des règles juridiques existantes.

Bien que les deux approches aient les éléments valables, l'approche loi-réelle finit par avoir gain de cause. La conception générale est qu'une partie considérable de la législation existante peut être appliquée à l'Internet. Pour certaines questions, les lois-réelles devraient être adaptées afin d'être applicables au cyber monde. Pour d'autres, un nombre limité de questions, de nouvelles règles doivent être conçues.

## Instruments juridiques

Il y a une large variété d'instruments juridiques existants qui ont été déjà appliqués ou pourraient être appliqués à la Gouvernance de l'Internet.

## Instruments juridiques nationaux et communautaires

### Législation

Chaque instrument juridique se compose de règles et de sanctions. Les règles stipulent certains comportements socialement admis (par exemple, ne pas commettre de crime, payer les impôts) et les sanctions spécifient les punitions au cas où les règles ne sont pas observées (par exemple les amendes, l'emprisonnement, la peine de mort dans certaines sociétés).

Les activités législatives se sont progressivement intensifiées dans le domaine de l'Internet. Ceci est particulièrement le cas au sein des pays de l'Organisation pour la Coopération et le Développement Economique(OCDE), où l'Internet est répandu et a un impact important sur les relations économiques et sociales. Jusqu'ici, les secteurs prioritaires pour les régulations législatives ont été la protection de la vie privée, la protection des données, la propriété intellectuelle, la fiscalité, et la cybercriminalité.

Pourtant, les relations sociales sont trop complexes pour être régulées seulement par les législateurs. La société est dynamique et la législation est toujours à la traîne par rapport au changement. Ceci est particulièrement remarquable en ce moment, où le développement technologique transforme la réalité sociale beaucoup plus rapidement que les législateurs. Parfois, les règles deviennent désuètes avant même qu'elles ne soient adoptées. Le risque d'obsolescence juridique est un facteur important dans la régulation de l'Internet.

### Les normes sociales (coutumes)

Comme la loi, les normes sociales proscrivent certains comportements. À la différence de la loi, aucun pouvoir national n'est chargé de faire appliquer ces normes. Elles sont appliquées par la communauté par le jeu de pressions

#### Loi-réelle contre cyber-loi

En dépit de l'approche la plus appropriée - loi-réelle ou cyber-loi - le principe général reste que les lois ne rendent pas impossible les comportements interdits, elles les rendent seulement punissables. Le fait que la fraude soit interdite dans le monde virtuel et le monde réel ne signifie pas que la fraude sera éradiquée en conséquence. Cette distinction est importante parce que l'un des fréquents arguments en faveur d'une séparation de la cyber-régulation est que les comportements interdits (fraude, crime, etc.) sont déjà répandus dans le Cyberspace et que la loi-réelle ne peut pas être efficacement utilisée.

exercées par l'entourage. A ses débuts, l'Internet a été régi par un ensemble de normes sociales appelées 'netiquette', selon lesquelles la pression exercée par l'entourage et les risques d'exclusion étaient les sanctions principales. A cette période, l'Internet était principalement utilisé par une communauté relativement petite, principalement les universités; les règles sociales étaient largement observées. La croissance de l'Internet a rendu ces règles inefficaces. Ce type de régulation peut toujours être employé, mais seulement au sein de groupes restreints avec des liens communautaires très forts.

### Autorégulation

Le livre blanc du Gouvernement des Etats-Unis sur la Gouvernance de l'Internet (1998) donne la préférence à l'autorégulation comme mécanisme de normalisation de l'Internet. L'autorégulation présente des similitudes avec les normes sociales décrites précédemment. A la différence des normes sociales, qui typiquement impliquent un système réglementaire diffus, l'autorégulation est basée sur une approche délibérée et bien structurée. Les règles d'autorégulation sont habituellement établies en codes de bonne pratique ou de bonne conduite.

La tendance vers l'autorégulation est particulièrement remarquable parmi les fournisseurs des services Internet (FAI). Dans beaucoup de pays, les FAI sont sous la pression croissante des autorités gouvernementales qui imposent des règles relatives à la politique du contenu; ils emploient de plus en plus l'autorégulation comme méthode d'imposition de certaines normes de comportement, afin d'empêcher l'interférence des Etats dans leurs activités.

Alors que l'autorégulation peut être une technique de normalisation utile, il subsiste certains risques dans leur utilisation pour réguler les secteurs d'intérêt public de premier plan, telle que la politique de contenu. Il reste à voir dans quelle mesure les FAI pourront réguler le contenu hébergé sur leurs sites Web. Peuvent-ils prendre des décisions en lieu et place des autorités judiciaires? Les FAI peuvent-ils juger un contenu comme acceptable? D'autres problèmes doivent également être traités tels que la protection de la vie privée et la liberté d'expression.

### Jurisprudence

La jurisprudence (décisions des tribunaux) constitue un élément important du système juridique aux Etats Unis, le premier à aborder les enjeux juridiques de l'Internet. Dans ce système, les précédents créent la loi, particulièrement dans les affaires impliquant la régulation de nouveaux problèmes, tel que l'Internet. Les juges doivent trancher même s'ils n'ont pas les outils nécessaires pour le faire – les règles juridiques à appliquer.

Le premier outil juridique que les juges utilisent est l'analogie juridique, qui leur permet de comparer un concept nouveau avec quelque chose qui leur est familier. La plupart des affaires juridiques au sujet de l'Internet sont résolues par le biais d'analogies.

## Instrumentes juridiques internationaux

### La différence entre le droit privé international et le droit public international

Le besoin d'utiliser le droit international est fréquemment évoqué dans les discussions sur la gouvernance de l'Internet. Le terme 'droit international' est principalement employé comme synonyme du droit public international, établi par les Etats-nations et les organismes internationaux, habituellement par l'adoption de traités et de conventions. Cependant, la plupart des affaires juridiques internationales relatives à l'Internet comportent une forte dose de droit privé, portant sur des questions telles que les contrats et les torts. En traitant de ces questions, il est nécessaire d'utiliser le droit privé international dont les règles sont prescrites dans la législation nationale, et non dans les traités internationaux<sup>3</sup>. Les règles de droit international privé précisent les critères pour établir une juridiction valable et le droit dans les affaires juridiques impliquant des éléments étrangers (par exemple les relations juridiques impliquant deux ou plusieurs entités provenant de différents pays). Les critères pour identifier la juridiction compétente et la loi appropriée comprennent le lien entre un individu et une juridiction nationale (par exemple la nationalité, le domicile), ou le lien entre une transaction particulière et une juridiction nationale (par exemple le lieu où le contrat a été conclu, le lieu où l'échange s'est déroulé).

### Droit privé international

Etant donné la nature globale de l'Internet, les différends juridiques auxquels des individus et des institutions régis par des juridictions nationales différentes sont très fréquents. Cependant, le droit privé international n'a été que très rarement appliqué pour régler des affaires légales basées sur l'Internet, du fait que ces procédures sont souvent complexes, lentes et coûteuses. Les principaux mécanismes du droit privé international ont été développés au moment où l'interaction transfrontière était moins fréquente et intense et proportionnellement très peu de cas impliquaient des individus et des entités régis par différentes juridictions.

### Droit public international

Le droit public international régit les relations entre les Etats-nations. Certains instruments du droit public international traitent déjà de certains

aspects pertinents de gouvernance de l'Internet (exemple: la régulation des télécommunications, les conventions de droits de l'Homme, et les traités internationaux de commerce). Dans cette section, l'analyse portera sur les éléments du droit public international qui devraient être utilisés dans le domaine de la gouvernance de l'Internet, parmi lesquels figurent les traités et les conventions, les coutumes, la 'loi molle', et le *ius cogens* (norme impérative de droit international).

### Conventions internationales

L'une des principales séries de conventions sur des problèmes liés à l'Internet a été adoptée par l'Union Internationale des Télécommunications (UIT): la Régulation Internationale des Télécommunications (1988), d'une grande importance dans la préparation du cadre politique des télécommunications pour les développements qui découlent de l'Internet. En dehors des conventions de l'UIT, la seule convention qui traite directement des problèmes liés à l'Internet est la Convention du Conseil d'Europe sur la cyber criminalité. Cependant, beaucoup d'autres instruments juridiques internationaux régissent des aspects généraux de la gouvernance de l'Internet, tels que les droits de l'Homme, le commerce et les droits de propriété intellectuelle.

### Droit coutumier international

Le développement des règles coutumières inclue deux éléments: la pratique générale (*consuetudo*) et la reconnaissance que cette pratique est légalement contraignante (*opinio juris*). Une longue période est habituellement requise pour la cristallisation de la pratique générale.

Certains éléments émergents du droit coutumier apparaissent dans la manière dont le gouvernement des Etats-Unis surveille la racine de l'Internet. Il dispose d'une stratégie bien rodée de non-intervention dans le secteur des domaines nationaux dans le fichier de la zone de la racine de l'Internet.

Une pratique généralisée est le premier élément pour identifier le droit coutumier. Reste à savoir si une telle pratique est basée sur la prise de conscience par le gouvernement des Etats-Unis que cela était conforme aux règles juridiques internationales (*existence de l'opinio iuris*). Si tel est le cas, il est possible d'identifier le droit coutumier international en gérant les parties du système du serveur racine de l'Internet qui traite les domaines-pays des autres pays. Il serait difficile d'étendre un tel raisonnement au statut juridique des gTLDs - les domaines génériques de premier niveau (.com, .org, .edu, .net) qui n'impliquent pas d'autres pays.

## Droit mou

'La droit mou' est un terme fréquemment utilisé dans le débat sur la gouvernance de l'Internet. La plupart des définitions du droit mou mettent l'accent sur ce qu'il n'est pas: ce n'est pas un instrument juridiquement contraignant. Les actes du droit mou contiennent des principes et des normes plutôt que des règles spécifiques. On le retrouve dans les documents internationaux tels que les déclarations, les lignes directrices, et les modèles de lois.

Les documents principaux du sommet Mondial sur la Société de l'Information (SMSI) y compris la déclaration finale, le plan d'action, et les déclarations régionales ont la capacité de développer certaines normes du droit mou. Ils ne sont pas juridiquement contraignants, mais sont souvent le résultat de longues négociations et d'un consensus entre tous les pays. L'engagement des Etats-nations et des autres parties prenantes dans la négociation d'instruments juridiques du droit mou afin d'arriver à un consensus, est le premier élément de preuve que de tels documents sont plus que de simples déclarations politiques.<sup>4</sup>

Le droit mou donne certains avantages dans le règlement de certains différends de la Gouvernance de l'Internet. D'abord, c'est une approche moins formelle, qui ne nécessite pas l'engagement officiel des Etats et de ce fait, n'exige pas de longues négociations. Ensuite, il est assez flexible et facilite la mise à l'épreuve de nouvelles approches et s'adapte aux développements rapides dans le domaine de la Gouvernance de l'Internet. Et en troisième lieu, le droit mou donne une plus grande place à une approche multi parties prenantes que ne peut le faire une approche internationale légale qui ne se limite qu'aux Etats et aux organisations internationales.

## Ius cogens

Le Ius cogens est décrit par la Convention de Vienne sur le Droit des Traités comme:

*'... Une norme, acceptée et reconnue par la communauté internationale des Etats comme un tout, à laquelle aucune dérogation n'est permise et qui ne peut être modifiée que par une nouvelle norme du droit international général ayant le même caractère.'*<sup>5</sup>

Le professeur Brownlie énumère les exemples suivants des règles de *ius cogens*:<sup>6</sup>

- L'interdiction de l'utilisation de la force.
- La loi sur le génocide.

- Le principe de non-discrimination raciale.
- Les crimes contre l'humanité.
- Les règles interdisant le commerce d'esclaves et la piraterie.

Dans le domaine de la Gouvernance de l'Internet, le *ius cogens* pourrait être utilisé pour l'introduction d'un certain type de lois, telle que la prohibition de la pornographie infantile en ligne.

## Jurisdiction

Le nombre de différends relatifs à l'Internet a sensiblement augmenté, ce qui a entraîné le problème de juridiction, qui est l'un des problèmes les plus cruciaux de la Gouvernance de l'Internet. La confusion sur la juridiction peut avoir deux conséquences immédiates et simultanées:

- 1 l'incapacité d'un Etat à exercer son pouvoir judiciaire en tant qu'entité responsable de la régulation des relations sociales sur son territoire.
- 2 l'incapacité des individus et entités à jouir de leurs droits à la justice (dénier de justice)

Les autres conséquences d'une ambiguïté juridictionnelle peuvent être:

- Création d'un climat d'insécurité juridique sur l'Internet.
- Freinage du développement du commerce électronique.
- Cloisonnement de l'Internet en zones Internet sûres.

A cause de ces conséquences, la clarification de la juridiction ainsi que de ses procédures est une affaire vitale pour la Gouvernance de l'Internet.

## Relation entre la juridiction et l'Internet

La relation entre la juridiction et l'Internet comporte une ambiguïté intrinsèque dans la mesure où la juridiction repose essentiellement sur la division géographique du globe en territoires nationaux. Chaque pays a le droit souverain d'exercer sa propre juridiction sur son territoire. Cependant, l'Internet facilite beaucoup d'échanges transfrontaliers, ce qui rend difficile (pas toujours impossible) la gestion par les mécanismes traditionnels de l'Etat. La question de la juridiction sur Internet met en lumière l'un des principaux dilemmes relatifs à la Gouvernance de l'Internet: comment est-il possible de 'd'ancrer l'Internet au sein d'une géographie légale et politique existante?<sup>7</sup>

## Jurisdiction - les techniques de base

La jurisdiction présente trois aspects principaux:

- 1 Quel tribunal ou quel pouvoir de l'Etat dispose de l'autorité publique adéquate (droit procédural)?
- 2 Quelles règles devraient être appliquées (jurisdiction de fond)?
- 3 Comment les décisions du tribunal devraient – elles être appliquées (droit applicatif)?

Les critères fondamentaux suivants établissent la jurisdiction dans des cas particuliers:

- **Le principe territorial** - le droit d'un Etat à statuer sur les personnes et les biens sur son territoire.
- **Le principe personnel** - le droit d'un Etat à gouverner sur ses citoyens partout où ils se trouveraient (principe de nationalité).
- **Principe d'effets** - le droit d'un Etat à régner sur les effets économiques et juridiques d'un territoire particulier, découlant des activités réalisées à l'étranger.

Un autre principe important introduit par le droit international moderne est le principe de la jurisdiction universelle.<sup>8</sup>

*'La notion de la jurisdiction universelle dans sa définition la plus large, est le pouvoir d'un Etat de sanctionner certains crimes quelque soit l'endroit où ils ont été commis et quelque soit la personne qui les a commis, sans lien avec le territoire, la nationalité et l'intérêt particulier d'un Etat.'*<sup>9</sup>

La jurisdiction universelle couvre des crimes tels que la piraterie, les crimes de guerre et le génocide.

## Conflit de jurisdiction

Les principes d'établissement d'une jurisdiction (territorial, nationalité, et effets) conduisent inévitablement à des situations où la jurisdiction est invoquée par les tribunaux de plusieurs Etats. Les problèmes avec la jurisdiction surgissent lorsque les litiges impliquent des cas extraterritoriaux (impliquant par exemple les individus de plusieurs nationalités ou des transactions internationales). Etant donné que tout le contenu Internet est accessible partout, tout internaute pourrait s'exposer à n'importe quelle jurisdiction nationale. Lorsqu'on place du contenu sur Internet, il est difficile de savoir quelle loi nationale, si elle existe, serait violée. Dans ce contexte,

presque toute activité sur Internet a un caractère international qui peut conduire à de multiples juridictions ou le soit disant 'effet d'entraînement' (*spill-over-effect*).<sup>10</sup>

L'un des cas les plus illustratifs et le plus souvent cité qui traduit mieux le problème de juridiction est l'affaire Yahoo! en France, en 2001. L'affaire Yahoo! jugée par les tribunaux de France a réitéré la pertinence du problème des juridictions multiples.<sup>11</sup> Cela a commencé par la violation d'une loi française concernant le contenu nazi, qui interdit l'exposition et la vente de tels objets, même si le site web qui fournissait ces articles - le site de vente aux enchères de Yahoo.com - était hébergé aux Etats Unis, où l'exposition de tels objets est tout à fait légale. L'affaire a été résolue par l'utilisation d'une solution technique (logiciel de géo-localisation et les filtres d'accès). Yahoo ! a été forcé d'identifier les internautes qui veulent y accéder à partir de la France et de bloquer leur accès aux pages contenant les éléments nazis.<sup>12</sup>

A côté des solutions techniques (logiciel de géo-localisation et les filtres), d'autres approches pour régler le conflit de juridiction inclut l'harmonisation des lois nationales et l'usage de l'arbitrage et d'autres solutions de règlement de litiges.

L'harmonisation des lois nationales peut résulter en l'établissement d'un ensemble de règles au niveau mondial. Avec des lois identiques en place, la question de la juridiction serait moins urgente. L'harmonisation pourrait être conduite dans les domaines où se dégage un grand consensus; par exemple, en ce qui concerne la pédophilie, la piraterie, le terrorisme et la cyber criminalité. Les points de vue convergent également sur d'autres points tels que le spam et la cyber sécurité. Toutefois, dans certains domaines tels que la politique du contenu, il n'est pas évident que l'on parvienne à un consensus sur les règles de base globales dans la mesure où les différences culturelles se manifestent dans le monde virtuel de façon plus prononcée que dans le monde réel<sup>13</sup>. Une autre conséquence potentielle d'un manque d'harmonisation est la migration de matériels en ligne dans des pays ayant de faibles politiques de régulation de l'Internet. En faisant une analogie avec le Droit de la Mer, certains pays deviendraient des 'pavillons de complaisance' ou des centres *offshore* du monde de l'Internet.

## Un bref aperçu présentant les grandes différences entre les systèmes de tribunaux traditionnels et l'arbitrage.

Éléments	Juridiction du tribunal	Arbitrage
Organisation	Etablie par des lois/traités Permanents	Etabli par les parties (temporaire, ad hoc) Etabli par des conventions (permanente)
Loi applicable	La loi de la cour (le juge décide de la loi applicable)	Les parties peuvent choisir la loi. S'ils ne le peuvent pas, alors la loi est celle indiquée dans le contrat; s'il n'y a aucune indication, alors la loi de l'arbitrage prend le relais
Procédure	Les procédures du tribunal sont établies par les lois/traités	Etablies par les parties (temporaires, ad hoc) Etablies par l'arbitrage et la régulation (permanent)
Compétence/ Objet du litige	Etablie par les lois/traités en relation avec l'objet du litige	Etablie par les parties
Décision	Contraignantes	Contraignantes

## Arbitrage

L'arbitrage est un mécanisme de règlement de litige, impliquant un ou plusieurs arbitres indépendants choisis par les parties en conflit. L'arbitrage international en matière de commerce a une tradition de longue date. Un mécanisme d'arbitrage est toujours établi dans un contrat privé avec des parties qui conviennent de soumettre tout éventuel différend au régime d'arbitrage. Il existe une variété de contrats d'arbitrage disponibles, spécifiant les aspects tels que le lieu d'arbitrage, les procédures, et le choix de la loi.

En comparaison avec les tribunaux traditionnels, l'arbitrage présente plusieurs avantages, entre autre une grande flexibilité, des coûts abordables, la rapidité, le choix de la juridiction, et une plus grande facilité d'application des sentences arbitrales étrangères. L'un des principaux avantages de l'arbitrage est qu'il surmonte le problème du choix de la procédure et des juridictions. Les deux sont choisies par les parties en conflit. L'arbitrage a un avantage particulier par rapport à l'une des tâches les plus difficiles dans les affaires judiciaires liées à l'Internet: application des décisions (sentences arbitrales). Le *New York Convention on Recognition and Enforcement of Foreign Arbitral Awards* régle l'application des sentences d'arbitrage.<sup>14</sup> Selon cette convention, les tribunaux nationaux sont obligés d'appliquer les sentences d'arbitrage. Il est plus facile d'appliquer de telles sentences dans les pays

étrangers en usant de la Convention de New York (*New York Convention*) qu'en usant des jugements classiques des tribunaux traditionnels.

La principale limite de l'arbitrage c'est qu'il ne peut régler les affaires de grand intérêt public; ceux-ci requièrent l'intervention de tribunaux installés dans des Etats.

L'arbitrage a été très utilisé dans les affaires commerciales. Un système bien développé de règles et d'institutions qui traitent des contentieux commerciaux a été mis en place. La ressource principale au niveau international est la 'Loi type sur l'arbitrage commercial international' de 1985 de la Commission des Nations Unies pour le droit commercial international (CNUDCI) qui a été complétée par d'autres instruments.<sup>15</sup> Les principales institutions internationales d'arbitrage sont habituellement rattachées aux Chambres de Commerce, et sont organisées au niveau international (Exemple de la Cour internationale d'arbitrage), régional (exemple de la Cour européenne d'arbitrage), et national.

### Arbitrage et l'Internet

L'arbitrage et les autres systèmes de règlement des litiges sont largement utilisés pour pallier à la lacune engendrée par l'incapacité de l'actuel droit international privé de traiter des cas liés à Internet. Un exemple particulier d'une méthode alternative de résolution des différends des cas liés à Internet est l'*Uniform Domain-Name Dispute-Resolution Policy* (UDRP) qui a été développé par l'Organisation Mondiale pour la Propriété Intellectuelle (OMPI) et mis en place par l'Internet Corporation for Assigned Names and Numbers (ICANN) comme première procédure de résolution de contentieux.<sup>16</sup>

L'UDRP est d'office prescrit en tant que mécanisme dans tous les contrats impliquant l'enregistrement des gTLDs (.com, .edu, .org, .net) et pour quelques ccTLDs (country code top-level domains). Sa spécificité réside dans le fait que les sentences arbitrales sont directement appliquées par des changements dans le Système des Noms de Domaines (DNS) sans recourir à une mise en application par les tribunaux nationaux.

L'Arbitrage fournit des moyens plus rapides, plus simples, et moins chers de règlements des différends. Toutefois, l'usage de l'arbitrage en tant que mécanisme principal de résolution des différends sur Internet, comporte quelques points faibles. Premièrement, l'arbitrage est toujours établi par un accord préalable, il ne couvre pas une large diversité de domaines lorsqu'ils

ne sont pas couverts par un accord préalable entre les parties (diffamation, différents types de responsabilité, cyber criminalité).

Deuxièmement, beaucoup trouvent désavantageux, pour la partie la plus faible du contrat, la pratique actuelle qui consiste à attacher une clause d'arbitrage aux contrats réguliers (souvent un internaute ou un client de commerce électronique).

Troisièmement, certains craignent que l'arbitrage n'étende le droit basé sur les précédents à l'échelle mondiale (le système juridique des Etats-Unis/Royaume Uni) en supplantant graduellement les autres systèmes juridiques nationaux. Dans le cas du droit commercial, ceci pourrait s'avérer plus acceptable, compte tenu du haut niveau d'harmonisation déjà observé dans les règles de fond. Toutefois, cela deviendrait une tâche très délicate en ce qui concerne le contenu et les aspects socioculturels, où le système juridique national reflète des valeurs culturelles spécifiques.

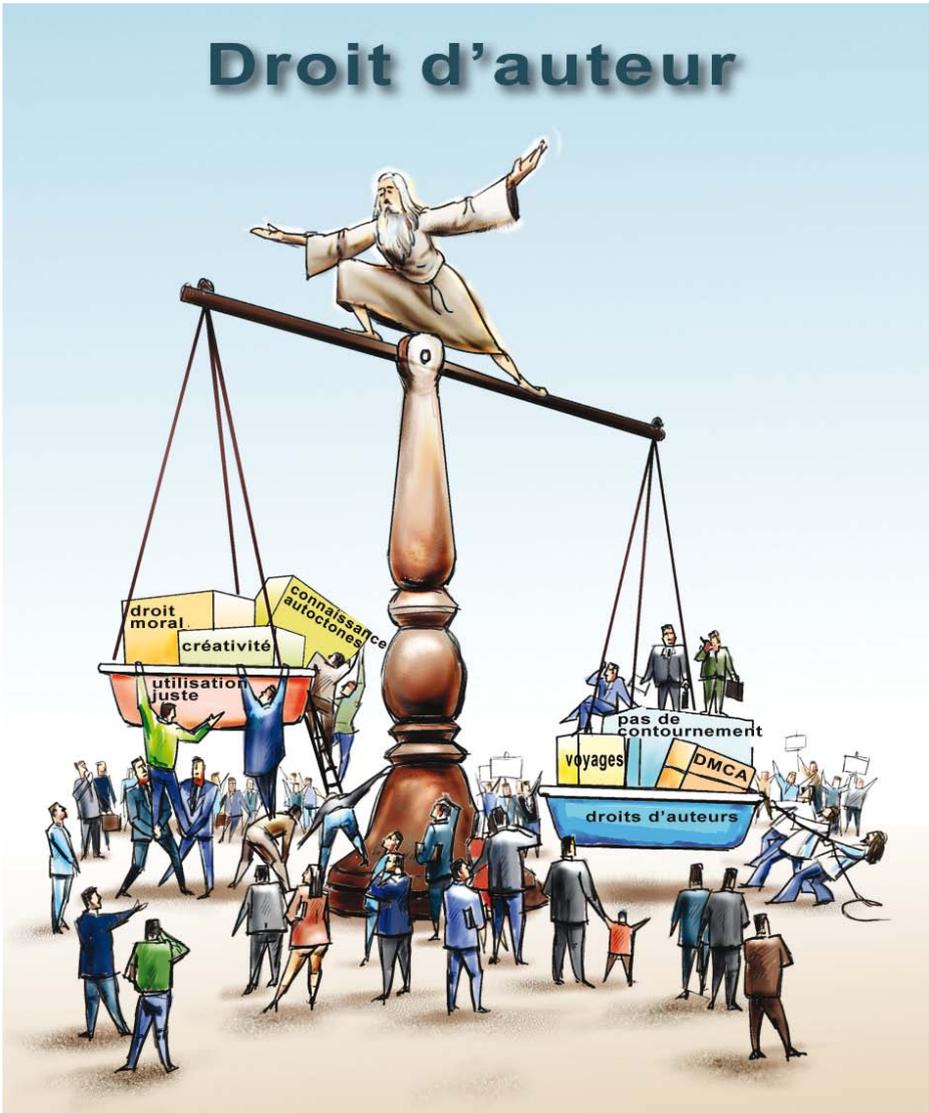
## Droits d'auteur

Le droit d'auteur protège seulement l'expression d'une idée lorsqu'elle est matérialisée sous diverses formes, telles qu'un livre, un CD, un fichier d'ordinateur etc. l'idée n'est pas protégée en elle-même. En réalité, il est parfois difficile de faire une distinction claire entre l'idée et son expression.

Le régime du droit d'auteur a soigneusement suivi l'évolution de la technologie. Chaque nouvelle invention, telle que l'impression, la radio, la télévision et le *VCR (Video Cassette Recording)* a affecté la forme et l'application du droit d'auteurs. L'Internet ne déroge pas à la règle. Le concept traditionnel du droit d'auteur a été défié de plusieurs manières, de simples textes copiés et collés à partir d'un site web, aux activités très complexes, telles que la distribution de fichiers de musique et de vidéo via le net presque gratuitement.

Paradoxalement, l'Internet renforce également les détenteurs des droits d'auteur, en leur fournissant des outils techniques très puissants pour protéger et gérer l'utilisation des éléments protégés. Dans le cas le plus extrême, les détenteurs des droits d'auteurs peuvent prohiber l'accès à tout un ensemble d'éléments protégés par le droit d'auteur, ce qui rendrait obsolète tout le concept des droits d'auteurs.

# Droit d'auteur



Ces développements mettent en danger le délicat équilibre entre les droits d'auteurs et l'intérêt public, qui est à la base de la loi du droit d'auteur.

Jusqu'ici, les détenteurs des droits d'auteur, représentés par de grandes compagnies d'enregistrement et du multimédia, ont été très en avance dans la protection de leurs intérêts. L'intérêt public a seulement été vaguement perçu et pas suffisamment protégé. Cependant, ceci change de manière graduelle, principalement à travers plusieurs initiatives globales se focalisant sur l'accès ouvert à la connaissance et à l'information.

## Droits de Propriété Intellectuelle (DPI)

La connaissance et les idées sont les ressources clés de l'économie mondiale. La protection des connaissances et des idées par le processus des DPI est devenue l'une des questions prédominantes dans le débat sur la gouvernance de l'Internet, et a une forte composante orientée vers le développement. Le DPI a été affecté par le développement de l'Internet, principalement par le biais de la numérisation de l'information et du savoir, ainsi que par de nouvelles possibilités pour leur manipulation. Les droits de propriété intellectuelle liés à l'Internet comprennent le droit d'auteur, les marques déposées et les brevets. Parmi les autres droits de propriété intellectuelle, l'on peut citer les conceptions graphiques, les marques de fabrique, les secrets commerciaux, les indications géographiques et les variétés végétales.

### La situation actuelle

#### Une protection plus stricte des droits d'auteurs au niveau national et international.

Les industries du disque et du divertissement ont subi de grandes pressions au niveau national et international pour renforcer la protection des droits d'auteurs. Aux Etats Unis, une protection plus stricte des droits d'auteurs a été introduite à travers le 'Digital Millenium Copyright Act' (DMCA), en 1998. Au niveau international, la protection des œuvres numériques, a été introduite dans le Traité des droits d'auteurs de l'OMPI (1996). Ce traité contient également des dispositions qui renforcent le régime de protection des droits d'auteurs, telles que des dispositions plus strictes pour les limitations des droits exclusifs d'auteurs, l'interdiction de contourner la technologie de protection des droits d'auteurs, et autres mesures connexes.

#### L'augmentation du nombre d'affaires judiciaires

Durant la seule année 2003, approximativement 1000 cas liés au DMCA contre les FAI ont été relevés, demandant à ces derniers d'arrêter les activités de partage de leurs fichiers par leurs abonnés, et plus de 500 plaintes contre des individus furent lancées. Un cas particulièrement pertinent pour le futur des droits d'auteurs sur l'Internet est le cas contre Grokster et Stream Cast, deux compagnies qui produisent des logiciels de partage de fichiers P2P (pair à pair). Suivant les dispositions du DMCA, le 'US Record Association' avait demandé à ces compagnies de ne pas soutenir le développement de la technologie du partage de fichiers qui contribue à la violation des droits d'auteurs. Initialement, les tribunaux des Etats Unis n'avaient pas reconnu Grokster et Stream Cast comme étant coupables d'une possible violation

des droits d'auteurs, sous réserve de circonstances raisonnables. Cependant, en Juin 2005, le verdict rendu par la Cour suprême des Etats Unis rend les développeurs du logiciel responsables de son mauvais usage.

### Logiciel contre la violation du droit d'auteur

Les outils utilisés par les malfaiteurs peuvent également être utilisés par les gens bien intentionnés. Traditionnellement, les Etats et les entreprises expriment leurs responsabilités à travers des mécanismes juridiques. Cependant, l'usage des outils logiciels 'alternatifs' par le secteur privé contre les contrevenants aux droits d'auteurs ne fait qu'augmenter.

Un article dans le New York Times a établi une liste de tactiques logicielles utilisées par les compagnies du disque et du divertissement pour protéger leurs droits d'auteurs:<sup>17</sup>

- *Un cheval de Troie* renvoie automatiquement les internautes sur les sites web où ils peuvent acheter légitimement la chanson qu'ils essaient de télécharger.
- Le logiciel '*Freeze*' bloque l'ordinateur pendant un laps de temps et lance un signal d'avertissement contre le téléchargement illégal de la musique.
- Le logiciel *de 'silence'* scanne les disques durs et tente de supprimer tout les fichiers illégaux trouvés.
- Le logiciel '*interdiction*' prive l'accès au net à ceux qui essaient de faire un téléchargement pirate de morceaux de musique.

Le professeur Lawrence Lessing de la Stanford Law School a alerté sur l'illégalité de telles mesures. Il a noté que parmi les anciennes mesures sujettes à un accord par rapport à la violation des droits d'auteurs, celles-ci n'étaient pas incluses. Les compagnies qui prennent de telles mesures enfreignent-elles la loi?

### Technologies de gestion des droits numériques

Comme approche à long terme et très structurelle, le secteur privé a présenté diverses technologies pour gérer l'accès aux éléments protégés par des droits d'auteurs. Microsoft a introduit le '*Digital Rights Management*' (*DRM*), qui est un logiciel qui sert à gérer le téléchargement de fichiers sonores, de films et d'autres éléments protégés par le droit d'auteur. Des systèmes similaires ont également été développés par Xerox (Content Guard), Philips, et Sony (Inter Trust).

L'usage des outils technologiques de protection des droits d'auteurs a reçu un grand soutien au niveau international (Traité du Droit d'auteur de l'OMPI)

et dans le DMCA. En outre, le DMCA a criminalisé les actions qui visent à contourner la protection technologique des éléments protégés.

## Les problèmes

### Amender les mécanismes existants ou développer de nouveaux mécanismes des droits d'auteurs?

Comment les mécanismes des droits d'auteurs devraient-ils être adaptés pour refléter des changements significatifs causés par les Technologies de l'information et de la communication (TIC) et les développements de l'Internet? Une réponse suggérée par le '*White Paper on Intellectual Property and the National Information Infrastructure*'<sup>18</sup> du gouvernement des Etats Unis, dit que seuls les changements mineurs sont nécessaires, principalement la 'dématérialisation' des concepts des droits d'auteurs de fixation, de distribution, de transmission, et de publication. Cette approche fut suivie dans les principaux traités internationaux des droits d'auteurs, incluant les aspects du droit de propriété intellectuelle relatifs au commerce (ADPIC) et les conventions des droits d'auteurs de l'OMPI.

Cependant, un point de vue contraire soutient que les changements dans le système juridique doivent être profonds, car les droits d'auteurs dans le domaine numérique ne se limitent pas seulement au 'droit de prévenir la copie' mais aussi au droit de prévenir l'accès. En fin de compte, avec de plus grandes possibilités techniques de limiter l'accès aux éléments numériques, l'on peut se demander si la protection des droits d'auteur est vraiment nécessaire. Il reste à voir comment l'intérêt public, la seconde partie de l'équation du droit d'auteur sera protégé.

### Protection de l'intérêt public – un usage 'équitable' des éléments protégés par droit d'auteur

Le droit d'auteur était initialement conçu pour encourager la créativité et l'invention. C'est la raison pour laquelle il combine deux éléments: la protection des droits d'auteurs et la protection de l'intérêt public. Le principal défi consistait à déterminer la manière dont le grand public devait consulter les éléments protégés afin d'améliorer la créativité, le savoir et le bien-être global. Opérationnellement parlant, cet intérêt public était protégé à travers le concept de 'l'usage équitable' des éléments protégés. L'usage équitable est défini comme l'usage d'éléments protégés sans demander la permission du détenteur des droits, à des fins de commentaire, critique, reportage d'actualité, recherche, enseignement, ou stage.<sup>19</sup>

### Droits d'auteur et développement

Toute restriction de l'usage équitable pourrait affaiblir la position des pays en développement. L'Internet fournit aux chercheurs, étudiants, et autres ressortissants des pays en développement un outil puissant de participation aux échanges académiques et scientifiques mondiaux. Le régime restrictif des droits d'auteurs pourrait avoir un impact négatif sur le renforcement des capacités des pays en développement.

Un autre aspect est la numérisation croissante des produits culturels et artistiques des pays en développement. Paradoxalement, les pays développés pourraient finir par payer pour bénéficier de leurs héritages culturels et artistiques dès qu'ils deviennent numérisés, 'réemballés', et détenus par des compagnies étrangères de divertissement et de média.

### L'OMPI et l'Accord sur les ADPIC

Comme déjà mentionné, il existe deux principaux régimes internationaux des droits de propriété intellectuelle. L'OMPI gère le régime classique des DPI, basé sur les conventions de Berne et de Paris. Un autre régime émergent est utilisé par l'Organisation Mondiale du Commerce (OMC) et est fondé sur les ADPIC. La transition de la coordination internationale du DPI de l'OMPI à l'OMC a été effectuée pour renforcer la protection des DPI, spécialement dans le domaine de sa mise en vigueur. Ceci était l'un des grands profits des pays développés pendant la phase de négociations de l'OMC durant le Cycle d'Uruguay.

Beaucoup de pays en développement sont perturbés par ce développement. Les mécanismes rigoureux de mise en application adoptés par l'OMC pourraient réduire la marge de manœuvre des pays en développement et la possibilité de trouver un juste équilibre entre les besoins de développement et la protection des DPI internationaux, principalement américains. Jusqu'ici, l'accent de l'OMC et des ADPIC a été mis sur différentes interprétations des DPI pour les produits pharmaceutiques. Il est très probable que les discussions futures s'élargissent et portent sur les DPI et l'Internet.

### Responsabilité des FAI en matière de violation des droits d'auteurs

Les mécanismes internationaux d'application de la loi dans le domaine de la propriété intellectuelle ont été renforcés en rendant les FAI responsables des éléments hébergés qui enfreignent les droits d'auteurs si l'élément n'est pas enlevé après notification de l'infraction. Ceci a directement rendu applicable le régime DPI dans le domaine de l'Internet.

## Marques déposées

Les marques déposées sont pertinentes pour l'Internet à cause de l'enregistrement des noms de domaine. Dans la première phase du développement de l'Internet, l'enregistrement de nom du domaine était basé sur le principe du premier arrivé, premier servi. Ceci a conduit au 'cyber squatting', la tendance à enregistrer les noms des compagnies et à les revendre plus tard à un prix élevé.

Cette situation a obligé le secteur privé à placer la question de la protection des marques déposées au centre de la réforme de la gouvernance de l'Internet conduisant à l'établissement de l'ICANN en 1998. Dans le papier blanc de la création de l'ICANN, le gouvernement des Etats Unis a demandé à ce que l'ICANN développe et mette en œuvre un mécanisme pour la protection des marques commerciales dans le domaine des noms de domaine. Sitôt après sa formation, l'ICANN a introduit l'*UDRP*<sup>20</sup> développé par l'OMPI.

## Brevets

En principe, un brevet protège un nouveau processus ou un nouveau produit de nature essentiellement technique ou manufacturière. Cependant, ce n'est que récemment que des brevets ont été attribués pour les logiciels. Plusieurs enregistrements de brevets finissent dans les tribunaux entre les éditeurs de logiciel américains, portant sur d'énormes sommes d'argent.

Quelques brevets accordés pour des procédures d'affaires ont été controversées, telle que la requête de 'British Telecom' pour réclamer des frais de licence pour le brevet sur les liens hypertextes, enregistrés en 1980. En Août 2002, le cas fut rejeté<sup>21</sup>. Si British télécom avait gagné ce procès, les utilisateurs d'Internet auraient dû payer un montant pour chaque lien hypertexte créé ou utilisé. La pratique d'octroi de licences aux procédures liées aux logiciels et à l'Internet n'a pas été acceptée en Europe et dans d'autres régions<sup>22</sup>.

## Cyber criminalité

Il existe une dichotomie entre le droit réel et le cyber droit dans le débat sur la cybercriminalité. L'approche du droit réel (positif) insiste sur le fait

que la criminalité est identique à un crime en dehors de l'Internet, mais est souvent commis par l'utilisation d'un ordinateur qui est probablement connecté à l'Internet. Le crime est le même, seulement les outils sont différents. L'approche du cyber-droit insiste sur le fait qu'il y a des éléments qui justifient un traitement spécial, surtout lorsqu'il s'agit de la mise en application et de la prévention.

Les rédacteurs de la Convention du Conseil de l'Europe sur la cyber criminalité étaient plus proches de l'approche du droit positif, en insistant sur le fait que le seul aspect spécifique de la cyber criminalité est l'usage des TIC comme moyen de commettre le crime. La convention est entrée en vigueur le 1er Juillet 2004; c'est le principal instrument international dans ce domaine.<sup>23</sup>

## Les problèmes

### Définition de la cyber criminalité

La définition de la cybercriminalité est l'un des problèmes les plus épineux du cyber droit étant donné qu'il a un impact juridique pratique et au vu des aspects couverts. Si l'accent est mis sur les délits commis contre des systèmes informatiques, le cyber crime inclurait l'accès non autorisé, le dommage aux données ou des programmes, le sabotage du fonctionnement d'un système, d'un ordinateur ou d'un réseau, l'interception non autorisée des données à partir, ou au sein d'un système ou d'un réseau aussi bien que l'espionnage de l'ordinateur. Une définition du cyber crime comme 'tout crime commis à travers l'Internet et les systèmes informatiques' inclurait une grande partie de crimes, y compris ceux spécifiés dans la Convention sur la cybercriminalité: fraude réalisée par l'intermédiaire de l'ordinateur, violations des droits d'auteurs, pédopornographie et sécurité du réseau.

### Cyber crime et la protection des droits de l'Homme

La convention sur le cyber crime a renforcé la discussion à propos de l'équilibre entre la sécurité et les droits de l'Homme. Plusieurs préoccupations ont été soulevées, articulées en premier lieu par la société civile, sur le fait que la convention donne trop d'autorité aux Etats, y compris le droit de contrôler les ordinateurs des hackers, la surveillance des communications et plus encore. Ces vastes pouvoirs mettraient potentiellement les droits de l'Homme en danger, particulièrement la protection de la vie privée et la liberté d'expression.<sup>24</sup> La Convention sur le cyber crime a été adoptée par le Conseil de l'Europe, l'un des promoteurs les plus actifs des droits de l'Homme. Ceci peut aider à établir l'équilibre nécessaire entre la lutte contre le cyber crime et la protection des droits de l'Homme.

### Collecte et sauvegarde des preuves

Un des principaux défis pour la lutte contre la cybercriminalité est la collecte de preuves destinées aux procès. La vitesse des communications d'aujourd'hui exige une réponse rapide de la part des agences en charge de l'application de la loi. Une possibilité pour conserver les preuves serait l'instauration de la capture des *logs dans les journaux*, au sein du réseau, qui fournissent des informations sur les personnes ayant accédées à des ressources Internet particulières, et le moment où cela s'est produit. La Convention sur le cyber crime spécifie l'obligation de préserver le trafic des données Internet. Cette règle pourrait affecter le rôle des FAI dans des activités liées à l'application des lois liées à Internet.

### Droit du travail

Il est fréquemment mentionné que l'Internet va changer la manière dont nous travaillons. Bien que ce phénomène exige une élaboration plus large, les aspects suivants sont en rapport direct avec la gouvernance d'Internet:

- L'Internet a permis d'avoir un grand taux de travailleurs temporaires et à court terme. Le néologisme 'travailleurs permanents temporaires' a été inventé pour les employés qui, pour le travail, ont été gardés durant de longues périodes sous des contrats à court terme régulièrement renouvelés. Ceci a introduit un très bas niveau de protection sociale des salariés.
- Le télétravail est de plus en plus pertinent avec le développement prononcé des télécommunications, en particulier avec l'accès à l'Internet à large bande.
- La sous-traitance à d'autres pays dans le secteur des services TIC, tels que les centres d'appel et les unités de traitement de données, est à la hausse. Un nombre considérable de ces activités ont déjà été transférées vers des pays à faible coût de main d'œuvre, principalement en Asie et en Amérique latine.

Les TIC ont chambardé la routine classique du travail, du temps libre, et du sommeil (8 +8 +8 heures). Il est de plus en plus difficile de distinguer où le travail commence et où il se termine. Les changements dans la façon de travailler peuvent exiger une nouvelle législation du travail, abordant des questions telles les heures de travail, la protection des intérêts des travailleurs, et la rémunération.

Dans le domaine du droit du travail, la question du respect de la vie privée sur le lieu de travail constitue un enjeu majeur. Un employeur a-t-il le droit de surveiller l'utilisation de l'Internet de ses employés (le contenu des messages e-mails ou la consultation des sites Web)? La jurisprudence est entrain de se développer progressivement, avec une variété de nouvelles solutions à offrir.



En France, au Portugal et au Royaume Uni, les consignes juridiques et quelques cas ont eu comme conséquence de limiter la surveillance des e-mails de l'employé. L'employeur doit au préalable donner une mise en garde préalable à toute surveillance éventuelle. Au Danemark, les tribunaux ont considéré un cas de licenciement d'un employé ayant envoyé des e-mails privés, et ayant accédé à un site web de *chat* à orientation sexuelle. Le tribunal a statué que le licenciement n'était pas légitime puisque l'employeur n'avait pas des règles d'utilisation de l'Internet mise en place interdisant l'usage non officiel de l'Internet. Une autre logique appliquée par le tribunal danois a été le fait que l'utilisation de l'Internet par le salarié n'avait pas affecté la performance de son travail.

De par la tradition, le droit du travail a toujours été un enjeu national. Cependant, la mondialisation générale, et l'Internet en particulier, ont conduit à l'internationalisation des questions liées au travail. Avec un nombre croissant de personnes travaillant pour des entités étrangères et interagissant avec les équipes de travail sur une base mondiale, un important besoin s'est manifesté pour des mécanismes internationaux de réglementation adéquats. Cet aspect a été reconnu dans la déclaration du SMSI, qui, au paragraphe 47, a appelé au respect de toutes les normes internationales pertinentes dans le domaine du marché de travail des TIC.

## Notes de fin

- <sup>1</sup> L'un des plus fervents partisans de l'approche du 'droit-réel' est le juge Frank Easterbrook qui est cité en disant: 'Rentrez chez vous; le cyber droit n'existe pas. Dans l'article *'cyberespace and the law of horse'* (le cyber espace et la loi du cheval), il soutient que bien que les chevaux aient été très importants, il n'y a jamais eu de loi 'pour le cheval'. Le juge Easterbrook fait valoir qu'il ya un besoin de se concentrer sur les instruments juridiques clés, tels que les contrats, la responsabilité, etc. Disponible sur <http://www.lessig.org/content/articles/works/.nalhls.pdf>
- <sup>2</sup> Le juge Frank Easterbrook a suscité plusieurs réactions, dont celle de Lawrence Lessig, dans *'The law of the horse: What cyberlaw might teach - Le droit du cheval: La leçon que nous pourrions tirer) pourrait être enseigné.* Disponible sur: <http://www.lessig.org/content/articles/works/finalhls.pdf>
- <sup>3</sup> Quelques tentatives internationales ont été faites pour harmoniser le droit international privé. La principale tribune mondiale est la Conférence du droit privé international de la Haye – 'the Hague Conference on International Private Law', qui a adopté de nombreuses conventions dans ce domaine.
- <sup>4</sup> Ici Il y a une fréquence élevée d'utilisation de l'auxiliaire modal 'devrait' dans les documents du Sommet Mondial sur la Société de l'Information (SMSI), l'une des caractéristiques des instruments juridiques mous. Pour plus d'informations, voir: *The emerging language of ICT diplomacy – Qualitative analysis of terms and concepts.* Disponible sur: <http://www.diplomacy.edu/IS/Language/html/words.htm>
- <sup>5</sup> L'article 53 de la Convention de Vienne de 1969 sur le Droit des Traités.
- <sup>6</sup> Brownlie I (1999) *Principles of Public International Law, 5th Edn.* Oxford University Press: Oxford, UK, p. 513.
- <sup>7</sup> Pour plus d'informations, voir: Salis RP (2001) *A summary of the American Bar Association's (ABA) Jurisdiction in Cyberspace Project: Achieving legal and business order in cyberspace. A report on global jurisdiction issues created by the Internet.* Disponible sur: <http://www.lex-electronica.org/articles/v7-1/Salis.htm>. Zittrain J (2006) *Jurisdiction in cyberspace*, Internet Law Program, Harvard Law School. Disponible sur: [http://cyber.law.harvard.edu/ilaw/mexico\\_2006\\_module\\_9\\_jurisdiction](http://cyber.law.harvard.edu/ilaw/mexico_2006_module_9_jurisdiction). ABA (2002) *Jurisdiction over Internet disputes: Different perspectives under American and European law in 2002, ABA Section on International Law and Practice.* Rencontre annuelle du printemps, New York, NY, USA, 8 mai 2002. Disponible sur: [http://www.howardrice.com/uploads/content/jurisdiction\\_internet.pdf](http://www.howardrice.com/uploads/content/jurisdiction_internet.pdf) Brownlie I (1999) *Principles of Public International Law, 5th Edition.* Oxford University Press: Oxford, UK, p. 513.
- <sup>8</sup> Parmi les ressources les plus importantes dans ce domaine, il y a *'the Princeton Principles on Universal Jurisdiction'* (2001). Disponible sur: <http://www1.umn.edu/humanrts/instreet/princeton.html>
- <sup>9</sup> Malanczuk P (1997) *Akehurst's 'Modern Introduction to International Law' (Introduction au droit international moderne).* Routledge: Londres, Royaume-Uni, p. 113.

- <sup>10</sup> Pour un aperçu des cas impliquant une compétence extraterritoriale à propos concernant le contenu Internet, voir: Timofeeva YA (2005) dans *'Worldwide prescriptive jurisdiction in Internet content controversies: A comparative analysis'* *Connecticut Journal of International Law* **20**: 199. Disponible sur: <http://ssrn.com/abstract=637961>
- <sup>11</sup> Pour suivre le développement du cas voir: [http://w2.e\\_.org/legal/Jurisdiction\\_and\\_sovereignty/](http://w2.e_.org/legal/Jurisdiction_and_sovereignty/)
- <sup>12</sup> Parmi d'autres affaires juridiques, est incluse l'affaire de la Cour fédérale allemande, contre Frederick Toben, ancien citoyen allemand ayant la nationalité australienne, qui avait posté des documents s'interrogeant sur l'existence réelle de l'holocauste sur un site web hébergé en Australie. Disponible sur: [http://www.ihr.org/jhr/v18/v18n4p-2\\_Toben.html](http://www.ihr.org/jhr/v18/v18n4p-2_Toben.html)
- <sup>13</sup> Contenus racistes et pornographiques (dans les cas présentés dans les notes 11 et 12) ne sont pas les seules questions à controverse – d'autres exemples comprennent les jeux illégaux d'argent en ligne, la publicité pour le tabac, et à la vente de la drogue.
- <sup>14</sup> Le texte complet de la Convention est disponible sur: [http://www.uncitral.org/uncitral/en/uncitral\\_texts/arbitration/NYConvention.html](http://www.uncitral.org/uncitral/en/uncitral_texts/arbitration/NYConvention.html)
- <sup>15</sup> Autres instruments de la CNUDCI comprennent le Règlement d'arbitrage de la CNUDCI (1976), le Règlement de conciliation de la CNUDCI (1980), les mémoires de la CNUDCI sur l'organisation des actes d'arbitrage (1996), et la Loi cadre de la CNUDCI sur la conciliation commerciale internationale (2002).
- <sup>16</sup> Uniform Domain – Name Dispute – Resolution Policy, ICANN, 26 Aout 1999 (politiques uniformes de résolution des différends sur les noms de domaine). Disponible sur: <http://www.icann.org/udrp/udrp-policy-24oct99.htm>
- <sup>17</sup> Sorkin AR (2003) Software bullet is sought to kill musical piracy. *New York Times*, 4 mai. Disponible sur: <http://www.nytimes.com/2003/05/04/business/04MUSI.html>
- <sup>18</sup> Disponible sur: <http://www.uspto.gov/web/offices/com/doc/ipnii/>
- <sup>19</sup> Disponible sur: [http://en.wikipedia.org/wiki/Fair\\_use](http://en.wikipedia.org/wiki/Fair_use)
- <sup>20</sup> Pour une enquête exhaustive sur les principaux problèmes ayant recours à l'UDRP, voir: *WIPO's Overview of WIPO panel views on selected UDRP questions*. Disponible sur: <http://arbitr.wipo.int/domains/search/overview/index.html>
- <sup>21</sup> Loney M (2002) *Hyperlink patent case fails to click*. CNET News.com. Disponible sur: <http://news.com.com/2100-1033-955001.html>
- <sup>22</sup> Pour plus d'information sur les discussions concernant la question des brevets sur les logiciels en Europe, voir: <http://swpat.ff.i.org>
- <sup>23</sup> Le texte complet de la Convention est disponible sur: <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>
- <sup>24</sup> Pour les vues et positions critiques sur la *Convention sur la cybercriminalité*, exprimant la préoccupation de la société civile et de militants des droits de l'Homme, voir: Bailey C (2002) *Report on the Cybercrime Convention*. The Association for Progressive Communication. Disponible sur: [http://rights.apc.org/privacy/treaties\\_icc\\_bailey.Shtml](http://rights.apc.org/privacy/treaties_icc_bailey.Shtml) Site web de treatyWatch.org (2010). Disponible sur: <http://www.treatywatch.org/>



## Section 4

---

# La corbeille économique





# La corbeille économique

Le commerce électronique a été l'un des principaux moteurs de la croissance de l'Internet au cours des 15 dernières années. Son importance a été illustrée par le titre du document qui a initié la réforme de la gouvernance de l'Internet et qui a établi l'ICANN (Internet Corporation for Assigned Names and Numbers: Corporation pour l'Assignation des Noms et des numéros de l'internet): Cadre du commerce électronique global (1997) qui stipule que le secteur privé devrait gérer le processus de la gouvernance de l'Internet et que la principale fonction de cette gouvernance serait de mettre en place un environnement juridique prévisible, minimaliste, consistant et simple pour le commerce électronique. Ces principes sont le fondement du régime de la gouvernance de l'Internet basé sur l'ICANN.

## La définition du commerce électronique

Le choix d'une définition du commerce électronique a beaucoup d'implications juridiques pratiques.<sup>1</sup> Les règles spécifiques sont appliquées selon qu'une transaction particulière est classée comme commerce électronique, telles que celles qui régulent la taxation et les opérations des douanes.

Pour le gouvernement des Etats-Unis, l'élément clé qui distingue le commerce traditionnel du commerce électronique c'est 'l'engagement en ligne pour la vente des marchandises ou des services'. Cela signifie que toute opération commerciale en ligne devrait être vue comme une transaction de commerce électronique, même si la réalisation de la transaction implique une livraison physique. Par exemple, acheter un livre via Amazon.com est considéré comme une transaction de commerce électronique bien que le livre est souvent livré via le courrier traditionnel. L'Organisation Mondiale du

Commerce (OMC) définit le commerce électronique comme la production, la distribution, le marketing, la vente et la livraison des marchandises et services par les moyens électroniques.<sup>2</sup>

Le commerce électronique prend plusieurs formes:

- De l'entreprise vers le consommateur (B2C) – le type de commerce électronique le plus répandu (ex. Amazon.com).
- D'entreprise à entreprise (B2B) – C'est la plus intensive économiquement, comptant pour 90% de toutes les transactions de commerce électronique.
- D'entreprise à Etat (B2G) – très important dans le domaine de la passation des marchés.
- Du consommateur au consommateur (C2C) – par exemple, vente aux enchères par e-Bay.

Beaucoup de pays se sont engagés dans le développement d'un environnement réglementaire pour le commerce électronique. Des lois ont été adoptées dans les domaines des signatures électroniques, de la résolution des litiges, de la cybercriminalité, de la protection du consommateur, et de la taxation. Au niveau international, un nombre croissant de régimes et d'initiatives sont en rapport avec le commerce électronique.

### L'OMC et le commerce électronique

Le principal acteur de la politique dans le domaine du commerce mondial moderne est l'OMC qui règle plusieurs problèmes relatifs au commerce électronique, y compris la libéralisation du secteur des télécommunications, des droits de propriété intellectuelle (IPR), et quelques aspects du développement des Technologies de l'Information et de la Communication (TIC).

Le commerce électronique est présent dans les initiatives et activités suivantes de l'OMC:

- Le moratoire temporaire des tarifs douaniers sur les transactions électroniques, introduit en 1998. Il a rendu toutes les transactions électroniques globalement libres des toutes taxes douanières.
- La mise en place d'un programme de travail de l'OMC pour le commerce électronique, programme qui promeut la discussion à propos du commerce électronique.<sup>3</sup>
- Un mécanisme de résolution des litiges. Le commerce électronique était particulièrement pertinent dans l'affaire entre les Etats-Unis et Antigua à propos des jeux d'argent en ligne.<sup>4</sup>

Bien que le commerce électronique ait été mis au second plan de l'agenda de l'OMC, plusieurs initiatives ont été prises et quelques enjeux fondamentaux ont été identifiés. Certains de ces enjeux sont mentionnés ci-dessous.

Les transactions de commerce électronique devraient-elles être classées comme services (régulées par l'AGCS- l'Accord général sur le commerce des services) ou comme biens (régulés par le GATT- l'Accord général sur les tarifs et le commerce, en français)?

La catégorisation de la musique comme une marchandise ou comme un service change-t-elle selon qu'elle soit livrée sur un CD (bien matériel) ou via l'internet (immatériel)?

En fin de compte, la même chanson pourrait avoir un statut commercial différent (et être soumises aux réglementations douanières et fiscales) en fonction du moyen de livraison. Le problème de la catégorisation a des implications importantes, à cause des mécanismes réglementaires différents entre les marchandises et les services.

Quel devrait être le rapport entre l'Accord sur les Aspects de droits de propriété intellectuelle qui touchent au commerce (ADPIC) – et la protection des Droits de propriété Intellectuelle (DPI) sur l'internet?

Puisque l'accord de l'OMC sur les ADPIC fournit beaucoup de mécanismes plus efficaces et coercitifs pour les DPI, les pays développés essayent d'étendre la couverture de l'Accord sur les ADPIC jusqu'au commerce électronique et à l'Internet en utilisant deux (2) approches. D'abord, en citant en exemple le principe de 'la neutralité technologique', ils stipulent que l'Accord sur les ADPIC, comme d'autres règles de l'OMC devraient être étendus sur tout moyen de télécommunications, y compris l'Internet. Ensuite, certains pays développés ont demandé une intégration plus étroite 'des traités numériques' de l'OMPI dans le régime de l'Accord sur les ADPIC. Cet Accord fournit des mécanismes plus efficaces et coercitifs que les conventions de l'OMPI. Les deux problèmes restent en suspens et vont devenir de plus en plus importants durant les futures négociations de l'OMC. Pendant la phase actuelle des négociations, il n'est pas très probable que le commerce électronique soit à l'ordre du jour de l'OMC. Le manque des dispositifs mondiaux du commerce électronique sera compensé par quelques initiatives spécifiques (comme par exemple, les contrats et les signatures) et plusieurs accords régionaux, notamment dans l'UE et la région Asie-Pacifique.

## D'autres initiatives Internationales en matière de commerce électronique

L'une des initiatives internationales les plus réussies et parmi les plus mieux reçues dans le domaine de commerce électronique est la loi type (Model de droit???) sur le Commerce Electronique de l'UNCITRAL (*UN Commission on International Trade Law* – la Commission des Nations Unies sur le Droit du Commerce International: CNUDCI). Cette loi –type met un accent sur les mécanismes pour l'intégration du commerce électronique dans le droit commercial traditionnel (exemple, reconnaissance de la validité des documents électroniques). Le modèle de droit était utilisé comme base de régulation du commerce électronique dans plusieurs pays. Une autre initiative conçue pour développer le commerce électronique est l'introduction du e-business XML (eb XML) par le UN/CEFAT (*United Nations Center for Trade Facilitation and Electronic Business* – Centre des Nation Unies pour la facilitation du commerce et des affaires électroniques), qui est une série des normes basée sur la technologie XML. En fait, l'ebXML pourrait bientôt devenir la principale norme pour l'échange des documents de commerce électronique, en remplaçant l'actuelle 'EDI' (*Electronic Data Interchange – Echange de données électroniques*).

L'Union Européenne a réalisé une série d'actions dans le domaine du commerce électronique, son principal centre d'intérêt étant les petites et moyennes entreprises.<sup>5</sup> Les activités de l'Organisation pour la Coopération et le Développement Economique (OCDE) abordent plusieurs aspects liés au commerce électronique, y compris la protection du consommateur et les signatures numériques. L'OCDE met l'accent sur la promotion et la recherche en matière de commerce électronique à travers ses recommandations et ses lignes directrices.

La Conférence des Nations Unies sur le Commerce et le Développement (CNUCED) est particulièrement active en matière de recherche et de formation, en mettant l'accent sur l'importance du commerce électronique dans le développement. Chaque année, elle publie le *Rapport sur le Commerce Electronique et le Développement* qui contient une vue générale de la situation actuelle et des propositions pour des développements futurs.

Dans le secteur des affaires, les organisations internationales les plus actives sont la Chambre de Commerce Internationale (CCI) qui publie en éventail de recommandations et d'analyses dans le domaine du commerce électronique, et le Dialogue Mondial des Entreprises, qui promeut le commerce électronique dans les contextes tant international que national.

### Initiatives régionales

L'Union Européenne a développé une stratégie sur le commerce électronique lors 'Sommet des *Dot com*' des leaders de l'UE à Lisbonne (en mars 2000). Bien qu'elle ait opté pour une approche du commerce électronique centrée sur le privé et le marché, l'Union Européenne a aussi introduit quelques mesures correctives qui visaient à protéger les intérêts sociaux et publiques (la promotion de l'accès universel, une politique de concurrence qui tienne compte des intérêts du public, et une restriction dans la distribution de contenus nuisibles). L'Union Européenne a adopté la Directive sur le commerce électronique ainsi bien qu'une série d'autres directives liées aux signatures électroniques, à la protection des données et aux transactions financières électroniques.

Dans la région de l'Asie-Pacifique, le point focal de la coopération en matière de commerce électronique est la coopération économique d'Asie-pacifique (*Asia-Pacific Economic Cooperation (APEC)*). L'APEC a mis en place le groupe de pilotage, qui se penche sur plusieurs questions relatives au commerce électronique, y compris la protection du consommateur, la protection des données, le spam, et la cyber sécurité. L'initiative la plus importante est le plan d'action individuel pour les échanges commerciaux sans papier de l'APEC, qui visait à créer un commerce de biens sans papier dans la région Asie-Pacifique d'ici à 2010.

### Protection du consommateur

La confiance du consommateur est l'une des conditions préalable au succès du commerce électronique. Ce dernier est encore relativement nouveau et les consommateurs n'en sont pas rassurés comme ils le sont lorsqu'ils font les achats dans le 'monde réel'. La protection du consommateur est un artifice juridique important pour développer la confiance dans le commerce électronique. La régulation du commerce électronique devrait protéger les consommateurs dans un certain nombre de secteurs à savoir:

- La manipulation en ligne des informations sur les cartes de paiement ;
- La publicité mensongère ; et
- La livraison de produits défectueux.

Une nouvelle particularité du commerce électronique réside dans l'internationalisation de la protection de l'utilisateur qui en fait n'est pas un problème vital dans le commerce traditionnel. Dans le passé, les utilisateurs

n'avaient pas souvent besoin de la protection internationale. Les utilisateurs faisaient leurs achats localement et par conséquent, avaient rarement besoin d'invoquer un mécanisme international de protection. Avec le commerce électronique, un nombre croissant des transactions a lieu à travers les frontières internationales.

La juridiction est une question importante qui garantit la protection de l'utilisateur. Elle implique deux (2) principales approches. La première favorise le vendeur (principalement une compagnie de commerce électronique), et il s'agit d'une 'approche pays d'origine'/prescribe-par-le-vendeur. Dans ce scénario, les compagnies de commerce électronique ont l'avantage de compter sur un environnement juridique prévisible et bien connu. L'autre approche, qui elle favorise le client, est une approche 'pays de destination'.

Son principal inconvénient pour les compagnies de commerce électronique tient au risque de se trouver exposé à une grande variété de tribunaux compétents. Une solution possible à ce dilemme serait une harmonisation plus systématique des règles de protection des consommateurs, ce qui rendrait la question de la juridiction moins pertinente.

Comme avec d'autres enjeux du commerce électronique, l'OCDE a pris le devant en adoptant les lignes directrices pour la protection du consommateur dans le contexte du commerce électronique (2000) et les lignes directrices pour protéger les utilisateurs contre des pratiques commerciales frauduleuses et trompeuses à travers les frontières (2003).

Les principes fondamentaux établis par l'OCDE ont été adoptés par d'autres associations d'affaire, y compris le CCI et le Conseil des bureaux d'éthique commerciale.

L'UE offre un grand niveau de protection du consommateur dans le commerce électronique. Le problème de la juridiction a été résolu à travers la Convention de Bruxelles, qui stipule que les utilisateurs feront toujours recours à la protection juridique locale.

A l'échelle mondiale, aucun instrument juridique international pertinent n'a été élaboré. L'un des plus appropriés, la Convention des Nations Unies sur les contrats pour la vente internationale des marchandises (1980), n'aborde pas les contrats passés avec les consommateurs et la protection de l'utilisateur.

Un certain nombre d'associations privées et d'organisations non gouvernementales (ONG) mettent aussi l'accent sur la protection du consommateur dans le commerce électronique, y compris 'Consumers International', le 'Consumer Project on Technology', le 'International Consumer Project on Technology', le 'International Consumer Protection Enforcement Network', et le 'Consumer Web Watch' .

Le futur développement du commerce électronique nécessitera soit l'harmonisation des lois nationales, soit un nouveau régime international pour la protection de l'utilisateur de commerce électronique

## Fiscalité

*Monsieur, je ne sais pas à quoi cela va servir. Mais une chose dont je suis tout à fait certain, c'est qu'un jour vous aller y prélever des taxes*

**Michael Faraday répondait aux politiciens sceptiques à propos de la finalité de son invention sur l'induction électromagnétique en 1831<sup>6</sup>**

Du fait de l'importance capitale de l'Internet dans la société moderne, la question de la fiscalité est devenue centrale. Elle est même devenue plus importante depuis la crise financière en 2008. Plusieurs gouvernements essaient d'augmenter le revenu fiscal dans le but de réduire la dette publique. La taxation des activités économiques sur Internet est devenue l'une des premières possibilités pour augmenter le revenu fiscal. L'une des demandes les plus fréquentes est de limiter le jeu d'argent en ligne dans le but de les empêcher de drainer les revenus fiscaux provenant des centres de jeu d'argent traditionnels. D'autres propositions incluent l'introduction des taxes spéciales d'accès à Internet.

Le dilemme de la Gouvernance de l'Internet à savoir si les problèmes du cyberspace devraient être traités différemment de ceux de la vie réelle se reflète clairement sur la question de la taxation.<sup>7</sup> Dès les premiers jours, les Etats-Unis ont réclamé que l'Internet soit une zone franche. En 1988, le congrès des Etats-Unis d'Amérique a adopté la loi sur la liberté fiscale, loi qui fut encore prorogée pour trois (3) autres années en décembre 2004. En octobre 2007, la loi a été prorogée jusqu'en 2014, malgré la crainte qu'elle puisse conduire à une perte substantielle de revenus.<sup>8</sup>

L'OCDE et l'UE ont développé un point de vue contraire, à savoir que Internet ne devrait pas avoir un traitement spécial en matière de fiscalité. Les principes d'Ottawa de l'OCDE spécifient qu'aucune différence n'existe entre la fiscalité traditionnelle et la e-fiscalité qui demanderait des réglementations spéciales. En appliquant ce principe, en 2003, l'UE a introduit une demande de régulation demandant aux compagnies non-européennes de commerce électronique à payer la taxe sur la valeur ajoutée (TVA) pour vendre des marchandises au sein de l'Union Européenne. La principale motivation de la décision du UE était que les compagnies qui n'appartiennent pas à UE (notamment les Etats-Unis) qui n'avaient pas d'affiliation avec des compagnies européennes devraient payer la TVA sur toutes les transactions, y compris celles dites électroniques.

Un autre problème de la fiscalité électronique qui demeure non résolu entre l'UE et les USA est la question de la localisation du prélèvement de l'impôt. Les principes d'Ottawa ont introduit un principe de la taxation à 'destination' au lieu du principe de la taxation à 'l'origine'. Le gouvernement des Etats-Unis a un intérêt capital en gardant les impôts à l'origine des transactions, puisque la plupart des compagnies de commerce électronique sont basées aux Etats Unis. Par contraste, l'intérêt de l'UE pour la taxation à destination est largement inspiré par le fait que l'UE a plus de consommateurs que de vendeurs dans le commerce électronique.

## **Signature numérique**

D'une manière générale, les signatures numériques sont liées à l'authentification des individus sur l'Internet ce qui affecte plusieurs aspects de l'Internet, y compris la juridiction, le cyber crime et le commerce électronique. L'usage des signatures numériques devrait contribuer à établir la confiance sur Internet. L'authentification numérique est généralement une partie du cadre du commerce électronique. Elle devrait faciliter les transactions du commerce électronique à travers la conclusion des contrats électronique. Par exemple, un accord est-il valide et obligatoire s'il a été conclu par e-mail ou à travers un site web?

Dans plusieurs pays, la loi exige que les contrats soient 'écrits' ou 'signés'. Qu'est-ce que cela signifie en termes d'internet? Confrontés à ces dilemmes et mis sous pression pour établir un environnement du commerce électronique, plusieurs gouvernements ont commencé à adopter des lois sur les signatures numériques.<sup>9</sup>

Pour ce qui est des signatures numériques, le grand défi est que les gouvernements ne régulent pas un problème existant, comme le cyber crime ou l'infraction du droit d'auteur, mais ils créent un nouvel environnement réglementaire dans lequel ils n'ont aucune expérience pratique. Ceci a débouché sur une variété de solutions et un tâtonnement général dans les réglementations sur les signatures numériques. Trois approches majeures à la régulation des signatures numériques ont émergé.

La première est une 'approche minimaliste' qui précise que les signatures électroniques ne peuvent pas être reniées du fait qu'elles sont sous forme électronique. Cette approche indique un très grand usage des signatures numériques, et elle a été adoptée dans les pays du Common Law: les États-Unis, le Canada, l'Australie et la Nouvelle Zélande.

La seconde est une 'approche maximaliste' qui spécifie le cadre et les procédures des signatures numériques, comprenant la cryptographie et l'usage de clés d'identifiants publics. Cette approche spécifie souvent l'établissement d'une autorité de certification, pouvant certifier les futurs utilisateurs des signatures numériques. Cette approche a prévalu dans les législations des pays Européens, tels que l'Allemagne et l'Italie.

La troisième approche adoptée dans le cadre de la directive de l'UE sur les signatures numériques combine ces deux approches.<sup>10</sup> Elle a une provision minimaliste pour la reconnaissance des signatures fournies par un moyen électronique. L'approche maximale est aussi reconnue à travers l'admission du fait que 'les signatures électroniques avancées' auront un effet juridique plus fort dans le système juridique (c'est-à-dire facilité de produire la preuve de ces signatures dans les affaires portées devant les tribunaux).

Au niveau mondial, l'UNCITRAL a adopté en 2001 une loi type sur les signatures électroniques; loi qui accorde le même statut aux signatures numériques qu'aux signatures manuelles, tant que quelques exigences techniques sont réunies. La Chambre Internationale de Commerce a produit un guide général d'utilisation dans le domaine d'un commerce électronique plus sûr (*General Usage in international Digitally Ensured Commerce: GUIDEC*) qui fournit une vue d'ensemble des meilleurs pratiques sur les problèmes de régulation et de certification.<sup>11</sup> Ce sont les initiatives sur l'infrastructure à clé publique (PKI) qui sont directement liées aux signatures numériques. Deux organisations, l'UIT (l'Union Internationale des Télécommunications) et l'IETF sont impliquées dans la normalisation de la PKI.

## Les enjeux

### Vie privée et les signatures numériques

Les signatures numériques font partie d'une grande considération entre la vie privée et l'authentification sur Internet. Elles sont d'une importance technique (mais pas seulement) pour l'identification des individus sur Internet.<sup>12</sup> Par exemple, l'authentification des SMS par des téléphones mobiles est utilisée par les banques pour approuver les transactions en ligne des clients dans certains pays où la législation sur la signature numérique ou les normes et procédures n'ont pas encore été établies.

### Le besoin de mise en application détaillée de normes

Bien que beaucoup de pays développés aient adopté la loi générale sur les signatures numériques, elle manque souvent d'instruments d'exécution, de procédures et de normes détaillées. Etant donné la nouveauté des problèmes soulevés, beaucoup de pays attendent de voir dans quelle direction les normes concrètes vont se développer.

Les initiatives de la standardisation se produisent à plusieurs niveaux comprenant, les organisations internationales (UIT) et les associations professionnelles (IETF).

### Le risque d'incompatibilité

La variété des normes et d'approches dans le domaine des signatures numériques pourrait conduire à l'incompatibilité entre les différents systèmes nationaux. Des solutions disparates pourraient restreindre le développement du commerce électronique au niveau international. Une harmonisation devra être nécessairement faite à travers les organisations internationales et régionales.

## Paiement électronique: Transaction bancaires et monnaie électroniques

L'élément commun dans la variété des définitions de 'e-' (électronique) est que les transactions financières se produisent en ligne à travers l'usage des systèmes de paiement en ligne. L'existence d'un système de paiement électronique est une pré-condition pour le succès du développement du commerce électronique. Le domaine des paiements électronique nécessite de faire la différence entre l (la banque sur Internet) et la e-monnaie (la monnaie électronique).

La banque virtuelle implique l'usage de l'Internet pour faire les opérations bancaires conventionnelles, tels que les paiements par carte ou les transferts des fonds. La nouveauté est seulement sur le moyen utilisé ; le service bancaire demeure essentiellement le même.

La banque sur Internet offre des avantages aux clients en introduisant des nouveaux services et en réduisant les coûts des transactions. Par exemple, les transactions du client, qui coûtent 1\$ américain dans le cadre du système bancaire classique, coûtent seulement 0,02\$ américain dans le cadre des banques en ligne.<sup>13</sup> En termes de gouvernance, les banques sur Internet posent de nouveaux défis pour ce qui est de la licence/autorisation à accorder aux banques par les autorités financières. Comment des banques virtuelles pourraient-elles se voir accorder des licences/autorisations? Un autre problème de gouvernance est la protection du consommateur/client au niveau international.

D'autre part, la monnaie électronique (e-monnaie) apporte une innovation importante. Le conseil d'administration de la réserve fédérale américaine définit la monnaie électronique comme 'l'argent qui circule électroniquement'. La monnaie électronique est souvent associée aux cartes dites 'intelligentes' émises par les compagnies telles que ; Mondex, Visa Cash, et Cyber cash.

Toute monnaie électronique a les caractéristiques suivantes:

- Elle est généralement emmagasinée électroniquement sur une carte magnétique ou une puce à microprocesseur.
- Elle est transférée électroniquement. Dans la plupart des cas, ceci a lieu entre les utilisateurs et les vendeurs. Quelquefois il est possible d'effectuer les transferts entre les individus.
- Les transactions impliquent un système complexe, y compris l'émetteur de la valeur de la monnaie électronique, les opérateurs du réseau, et le bénéficiaire final des transactions.

Jusqu'à présent, la monnaie électronique est encore dans les premières phases de développement. Elle n'a pas été largement utilisée, à cause de la sécurité limitée et de l'absence du respect de la vie privée. Elle pourrait se développer dans deux directions.

La première est un développement évolutionniste qui inclurait plus de méthodes sophistiquées des transactions basées sur l'électronique, y compris le développement de systèmes de micro paiements efficaces. Finalement, toutes ces transactions seraient ancrées dans le système monétaire et bancaire existant.

La seconde est un développement révolutionnaire qui sortirait la monnaie électronique hors du contrôle des banques centrales. La banque de règlements internationaux (Bank of International Settlement) a déjà identifié une diminution du contrôle de la circulation du capital et de l'émission de la monnaie comme des risques associés à la monnaie électronique. Conceptuellement, émettre de la monnaie électronique sera analogue à l'impression de monnaie sans le contrôle d'une institution de la banque centrale. Une telle approche permettrait à des institutions privées d'émettre de l'argent exclusivement pour le commerce électronique. L'introduction récente de *Facebook* a soulevé des problèmes à cause du volume de ses activités en ligne, il se peut qu'il prenne *de facto* dans le futur une fonction monétaire.<sup>14</sup> Dans le contexte de la crise financière récente et les tentatives des gouvernements de gagner à nouveau le contrôle du système financier, il n'est pas très probable que les expériences de la monnaie électronique soient encouragées.

## Les enjeux

### Changements à apporter au système bancaire mondial

L'utilisation de la banque sur Internet (e-banque) et de la monnaie électronique (e-monnaie) pourrait occasionner des changements au système bancaire mondial, en fournissant aux clients des possibilités supplémentaires et en réduisant en même temps les charges bancaires. Des méthodes bancaires rigides seront plus concurrencées par le très bénéfique système de banques en ligne (en termes de coûts).<sup>15</sup> Il faut noter que plusieurs banques traditionnelles ont déjà adopté les services bancaires en ligne. En 2002, il y avait seulement 30 banques virtuelles aux Etats-Unis. Aujourd'hui, il est difficile de trouver une banque sans services bancaire en ligne.

### Cyber sécurité

La cyber sécurité est l'un des principaux défis pour un large déploiement des paiements électroniques. Comment la sécurité des transactions financières peut-elle être assurée via Internet? Sur ce point, il est important d'insister sur la responsabilité des banques et des autres institutions financières pour ce qui est de la sécurité des transactions en ligne. Le principal développement à cet égard était la loi Sarbanes-Oxley, adoptée par le Congrès américain comme une réaction aux scandales financiers d'Enron, d'Arthur Andersen, et de Worldcom. Cette loi renforce le contrôle financier et augmente la responsabilité des institutions financières pour la sécurité des transactions en ligne. Elle partage également la charge de la responsabilité de la sécurité entre les clients, qui doivent faire preuve d'une certaine prudence, et les institutions financières.<sup>16</sup>

### Manque de méthodes de paiement

Les enquêtes sur le commerce électronique indiquent le manque des méthodes de paiement (cartes par exemple) comme troisième raison, après la sécurité et le respect de la vie privée, pour expliquer le non recours au commerce électronique. Actuellement, le commerce électronique est fondamentalement lié à l'utilisation de cartes de crédit. C'est un obstacle significatif pour les pays en développement qui n'ont pas un marché développé des cartes de crédit.

Les gouvernements dans ces pays devraient mettre en place un environnement légal nécessaire afin de permettre l'introduction plus rapide des cartes de paiement.

### Paiement électronique au comptant

Dans le but de favoriser le développement du commerce électronique, les gouvernements du monde entier auraient besoin d'encourager toutes les formes de paiements libres au comptant (cash), y compris les cartes de crédit et la monnaie électronique. L'introduction plus rapide de la monnaie électronique nécessitera les activités de régulation gouvernementales supplémentaires. Après Hong Kong, le premier pays à introduire une législation concernant la monnaie électronique, l'Union Européenne a adopté la directive sur la monnaie électronique en 2000.<sup>17</sup> Les gouvernements sont hésitants à introduire la monnaie électronique à cause des risques potentiels de friction avec l'autorité des banques centrales. Les inquiétudes importantes sont exprimées par des points de vues tels que ceux exprimés par l'économiste David Saxton: 'Le cash numérique est une menace pour chaque gouvernement sur cette planète voulant gérer sa propre monnaie'.<sup>18</sup> Les gouvernements sont aussi consternés par l'utilisation potentielle de la monnaie électronique pour le blanchiment d'argent.

### Petites transactions

Certains analystes pensent que la vraie expansion du commerce électronique est liée à l'introduction des services fiables et effectifs pour des petites transactions. Par exemple, les utilisateurs de l'Internet sont encore hésitant quant à l'utilisation des cartes de crédit pour des petits paiements (peu d'euro /dollars) qui sont souvent facturés pour avoir accès aux articles ou à d'autres services sur Internet. Un plan de micro-paiement basé sur la monnaie électronique peut apporter la solution nécessaire. C'est important de noter que W3C (*World Wide Web Consortium*) l'organe principal de la standardisation du Web, a cessé ses activités de micro-paiement/commerce électronique, ce qui est considéré comme un pas en arrière face aux efforts globaux vers la normalisation dans ce domaine.<sup>19</sup>

### Règlement du problème au niveau international

A cause de la nature de l'Internet, il est probable que la monnaie électronique devienne un phénomène international – ce qui pousse à vouloir chercher à régler ce problème au niveau international. Un acteur potentiel dans le domaine du système bancaire en ligne est le groupe '*Basel Committee E-banking Group*'. Ce groupe a déjà commencé à aborder les questions d'autorisation, de normes prudentielles, de transparence, de vie privée, du blanchiment d'argent, de surveillance des frontières, et de tous les problèmes clés liés à l'introduction de la monnaie électronique.<sup>20</sup>

### Lien avec l'application de la loi

La récente demande du procureur général de l'État de New York à PayPal et à Citibank de ne pas exécuter les paiements aux casinos effectués directement sur Internet lie le paiement électronique à l'application de la loi.<sup>21</sup> Ce que les autorités chargées de l'application de la loi applicable ne pourraient pas accomplir à travers les mécanismes juridiques, elles pourraient le faire à travers le contrôle des paiements électroniques.

## Notes de fin

- 1 La pertinence juridique pour établir une définition claire est ouvertement expliquée dans la page interactive sur le e-commerce de UE: '*Normally, we avoid defining electronic commerce, aside from the vague non-definition of e-commerce being about doing business electronically. However there is a need for a legal definition for legal papers*' - Normalement, nous évitons de définir le commerce électronique, à côté d'une définition vague qui dit qu'il s'agit juste de faire des affaires de manière électronique. Cependant, il y a nécessité d'une définition légale pour des documents officiels'  
 Disponible sur: <http://ec.europa.eu/archives/ISPO/e-commerce/drecommerce/answers/000025.html>
- 2 WTO (1998) programme de travail sur le commerce électronique. Disponible sur: [http://www.wto.org/english/tratop\\_e/ecom\\_e/wkprog\\_e.htm](http://www.wto.org/english/tratop_e/ecom_e/wkprog_e.htm)
- 3 Cette section du site web de l'OMC se centre sur le commerce électronique: [http://www.wto.org/english/tratop\\_e/ecom\\_e/ecom\\_e.htm](http://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm)
- 4 Pour plus d'informations sur le cas Etats-Unis d'Amérique /Antigua (cas de blanchiment en ligne voir: [http://www.wto.org/english/tratop\\_e/dispu\\_e/cases\\_e/ds285\\_e.htm](http://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm)
- 5 Pour plus d'informations sur les initiatives du commerce électronique de l'UE, voir: [http://ec.europa.eu/information\\_society/europe/2002/action\\_plan/e-commerce/index\\_en.htm](http://ec.europa.eu/information_society/europe/2002/action_plan/e-commerce/index_en.htm)
- 6 Maastricht Economic Research Institute on Innovation and Technology (MERIT). Disponible sur: <http://www.merit.unimaas.nl/cybertax/>
- 7 Pour une discussion sur divers aspects des politiques de taxation et Internet, voir: Cockfield AJ (2001) Transforming the Internet into a taxable forum: A case study in e-commerce taxation, *Minnesota Law Review* 85:1171–1236. Disponible sur: <http://post.queensu.ca/~ac24/MinnLRevArticle.pdf>  
 Morse EA (1997) *State taxation of Internet commerce: Something new under the sun?* *Creighton Law Review*. 30: 1124–1127.  
 Williams WR (2001) *Thee role of Caesar in the next millennium? Taxation of e-commerce: An overview and analysis*, *Wm. Mitchell Law Review* 27: 1703–1707.
- 8 Mazerov M (2007) *Making the 'Internet Tax Freedom Act' permanent could lead to a substantial revenue loss for states and localities*. Disponible sur: <http://www.cbpp.org/7-11-07sfp.htm>
- 9 Pour plus d'explications détaillées de la thèse sur les trois approches, voir the *Survey of Electronic and Digital Signature Initiatives* fourni par ' the Internet Law & Policy Forum'. Disponible sur: <http://www.ilpf.org/groups/survey.htm#IB>
- 10 Directive 1999/93/EC par le parlement européen et le Conseil le 13 Décembre 1999 sur a *Community Framework for Electronic Signatures*. Disponible sur: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:en:HTML>

- 11 GUIDEDEC (General Usage for International Digitally Ensured Commerce) par la Chambre Internationale de Commerce et de l'Industrie. Accessible sur: <http://cryptome.org/jya/guidec2.htm>
- 12 Longmuir G (2000) *Privacy and digital authentication*. Disponible sur: <http://caligula.anu.edu.au/~gavin/ResearchPaper.htm>. Le document se focalise sur les aspects personnels, communautaires et gouvernementaux des besoins d'authentification dans le monde virtuel.
- 13 Nsouli SM, Schaechter A (2002) Challenges of the e-banking revolution. *Finance and Development* 39(3). Disponible sur: <http://www.imf.org/external/pubs/ft/fandd/2002/09/nsouli.htm>
- 14 A propos des aspects légaux de l'Introduction de la money virtuelles Facebook voir: Claburn T (2010) Virtual money presents some legal problems, *InformationWeek*. Disponible sur: <http://www.informationweek.com/news/security/app-security/showArticle.jhtml?articleID=223101009>
- 15 Bankrate.com (2002) *What is online banking?* Disponible sur: <http://www.bankrate.com/brm/olbstep2.asp>. C'est un article qui fournit u une introduction sur la banque en ligne et une enquête sur les avantages et désavantages de la banque traditionnelle.
- 16 Pour plus d'informations, voir: Jacobs E (ND) *Security as a legal obligation: About EU legislation related to security and Sarbanes-Oxley in the European Union*. Disponible sur: <http://www.arraydev.com/commerce/JIBC/2005-08/security.htm>
- 17 Directive 2000/46/EC du Parlement Européen et du Conseil du 18 Septembre 2000, sur la prise en main, la poursuite et la supervision prudente des affaires des institutions impliquées dans la monnaie électronique money institutions. Disponible sur: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0046:EN:HTML>
- 18 Holland K, Cortese A (1995) *\_ e future of money: e-cash could transform the world's financial life*. Disponible sur: <http://www.businessweek.com/1995/24/b3428001.htm>
- 19 Pour des arguments contre le micro-paiements, voir: Shirky C (2000) *\_ e case against micropayments*. Disponible sur: <http://www.openp2p.com/pub/a/p2p/2000/12/19/micropayments.html>
- 20 Le Basel Group est basé à la 'Bank for International Settlements' Il produit régulièrement: *Survey of Developments in Electronic Money and Internet and Mobile Payments*. Disponible sur: <http://www.bis.org/publ/cpss62.pdf>
- 21 Pour plus d'information, voir: [http://www.ag.ny.gov/media\\_center/2002/aug/aug21a\\_02.html](http://www.ag.ny.gov/media_center/2002/aug/aug21a_02.html)

## Section 5

---

# La corbeille de développement





# La corbeille de développement

La technologie n'est jamais neutre. L'histoire humaine nous donne beaucoup d'exemples où la technologie a rendu puissants quelques hommes, groupes et États, tandis qu'elle en excluait. L'Internet ne déroge pas à la règle en la matière. Du niveau individuel au niveau global, il s'est opéré de grands changements dans la distribution de la richesse et du pouvoir. L'impact des TIC/Internet sur la distribution du pouvoir et du développement a suscité plusieurs questions :

- Comment les rapides changements des TIC/Internet affectent-ils la fracture déjà existante entre le Nord et Sud? Les TIC/Internet réduiront-ils ou aggraveront la fracture existante?
- Comment et quand les pays en voie de développement atteindraient-ils le niveau des pays les plus industrialisés?

La réponse à ces questions et à d'autres requiert une analyse de la pertinence du développement dans le contexte de la gouvernance de l'Internet.

Presque chaque aspect de la gouvernance de l'Internet comporte un aspect développemental.

- L'existence d'une infrastructure de télécommunication facilite l'accès ; la première condition pour surmonter la fracture numérique.
- Le modèle économique actuel de l'Internet met une charge disproportionnée sur ces pays en développement qui doivent payer l'accès aux backbones situés dans les pays développés.
- Le spam a une incidence plus négative dans les pays en développement comparativement aux pays développés à cause de la bande passante limitée et le manque de capacité pour y faire face.

Une régulation globale des Droits de Propriété Intellectuelle (DPI) affecte directement le développement à cause de l'opportunité réduite des pays en développement d'accéder au savoir et à l'information en ligne.

L'aspect développement du Sommet Mondial sur la Société de l'Information (SMSI) a souvent été maintes fois réaffirmé, à commencer par la Résolution de l'Assemblée Générale des Nations Unies sur le SMSI qui a mis un accent particulier sur le fait que le SMSI devrait 'promouvoir le développement, en particulier en tenant compte de l'accès et du transfert de technologie'. Le Plan d'action du SMSI de Genève et Plan d'Action a mis l'accent sur le développement comme étant une priorité et l'a lié à la Résolution du Millénaire ainsi qu'à la promotion de 'l'accès de tous les pays à l'information, au savoir et aux technologies de l'information et de la communication pour le développement'. En liaison avec les Objectifs du Millénaire, le SMSI s'est fortement positionné dans un contexte de développement.

### Comment les TIC affectent-ils le développement des sociétés?

Les principaux dilemmes entre les TIC et le développement sont résumés dans un article de *l'Economist*.<sup>1</sup> L'article propose un argumentaire pour et contre la thèse selon laquelle les TIC donnent une impulsion spécifique au développement.

#### Les TIC ne facilitent pas le développement

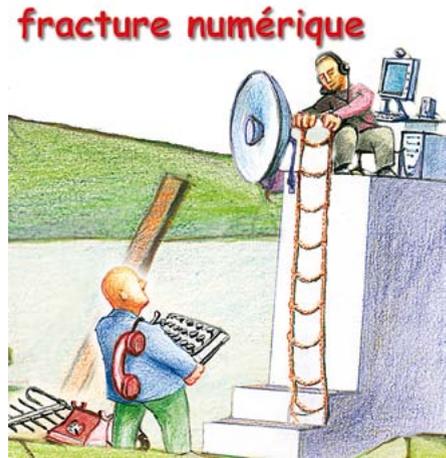
- Les 'externalités du réseau' favorisent les premiers arrivés à s'établir dans une position dominante. Cela favorise les grandes sociétés américaines de façon à ce que les entreprises des économies émergentes seraient effectivement écartées du commerce électronique.
- Le transfert de pouvoir du vendeur à l'acheteur (l'Internet permet inévitablement l'émergence d'un fournisseur alternatif qui n'est ni plus ni moins qu'un scénario au moyen d'un clic de souris) fragilisera les pays les plus pauvres. Cela nuira aux producteurs surtout ceux des pays en développement.
- De grands profits fournis par les actions placées dans la haute technologie de ces économies riches réduiraient l'intérêt des investisseurs dans les pays en développement.

#### Les TIC favorisent

- Les TIC baissent les coûts de travail ; il est beaucoup moins cher d'investir dans les pays en développement.
- A l'opposé des anciennes technologies, les TIC se diffusent plus rapidement à travers les frontières. Les anciennes technologies (Rail, électricité) ont pris du temps pour s'étendre jusqu'aux pays en développement, alors que les TIC avancent à pas de géant.
- L'opportunité de surclasser les anciennes technologies en sautant les étapes intermédiaires, tels que les lignes en cuivre et les téléphones analogiques, encourage le développement.
- La propension des TIC à réduire de façon optimale la taille d'une entreprise dans la plupart des industries est beaucoup plus proche des besoins des pays en voie de développement.

## La fracture numérique

La fracture numérique peut être définie comme une fissure entre ceux qui, pour des raisons techniques, politiques, sociales ou économiques, ont accès aux TIC/internet et ont la possibilité de les utiliser, et ceux qui ne peuvent pas. Plusieurs points de vue ont été avancés concernant l'ampleur et l'importance de la fracture numérique.



La fracture numérique existe à tous les niveaux : dans les pays et entre les pays, entre les populations urbaines et les populations rurales, entre les jeunes et les vieux, et bien entendu entre les hommes et les femmes. Les fractures numériques ne sont pas des phénomènes indépendants. Elles reflètent les grandes inégalités socioéconomiques qui existent en matière d'éducation, de santé, de logement, d'emploi, d'accès à l'eau potable et à la nourriture. Ceci a été clairement rapporté par le G8 DOT Force (Digital Opportunity Task Force)

*'Il y a pas de dichotomie entre la fracture numérique et la large fracture sociale et économique que le processus de développement devra résoudre ; la fracture numérique devra être comprise et combattue dans le contexte de ces grandes fractures.'*<sup>2</sup>

### La fracture numérique s'accroît-elle?

Les développements des TIC/Internet délaissent le monde en développement à une vitesse plus prononcée par rapport à d'autres domaines (Ex : l'agriculture et les techniques médicales), et comme les pays riches possèdent les outils nécessaires à l'utilisation de ces avancées technologiques, la fracture numérique semble s'agrandir rapidement et continuellement. Ceci est le point de vue exprimé dans plusieurs documents, tel que le *Rapport sur le développement humain* du Programme des Nations Unies pour le Développement (PNUD) et le *Rapport mondial de l'Emploi* de l'Organisation Internationale du Travail (OIT).

Certaines voix discordantes soutiennent que les statistiques sur la fracture numérique sont souvent biaisées et que la fracture numérique ne s'aggrave

pas du tout. Selon ce point de vue, la traditionnelle attention portée sur le nombre d'ordinateurs, le nombre des sites Internet, ou la bande passante disponible devrait être remplacée par une attention sur l'impact des TIC/Internet sur les sociétés des pays en développement. Les succès dans le domaine des technologies numériques au Brésil, en Chine et en Inde sont souvent cités en exemple.

## **L'accès universel**

A côté de la fracture numérique, l'autre concept souvent cité dans le débat sur développement est l'accès universel, c'est à dire l'accès pour tous. Bien que cela doive être la pierre angulaire de toute politique de développement des TIC, il y a des compréhensions et conceptions différentes sur la nature et l'esprit de cet accès universel. De fréquentes références à l'accès universel dans les préambules des déclarations et résolutions internationales sans les soutiens politique et financier nécessaires font de l'accès universel un principe vague ayant une pertinence limitée au niveau pratique. La question de l'accès universel reste une question hautement politique au niveau international, par conséquent, il est dépendant de la bonne volonté des pays développés à s'impliquer dans la réalisation de cet objectif.

A l'opposé du contexte mondial, l'accès universel dans certains pays est un concept économique et juridique bien développé. Fournir un accès aux télécommunications à tous ses citoyens a été le fondement de la politique des télécommunications des Etats-Unis. Le résultat de cela a été un système bien développé de plusieurs mécanismes politiques et financiers dont le but est de subventionner les coûts d'accès des zones éloignées et des régions aux coûts de connexion très élevés. Les subventions sont financées par les régions aux faibles coûts, à commencer par les grandes villes. L'UE a aussi pris des mesures concrètes pour réussir l'accès universel.

## **Stratégies pour surmonter la fracture numérique**

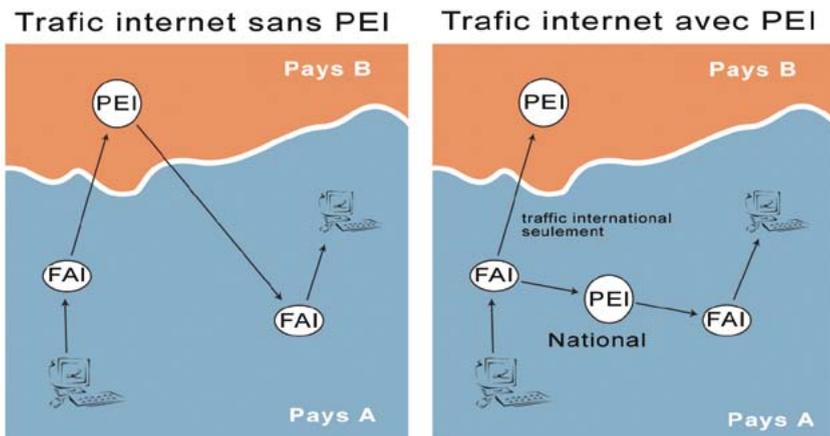
La théorie du développement centré sur la technologie, qui a dominé pendant ces 50 dernières années dans les milieux politiques et intellectuels, soutient que le développement dépend de la disponibilité de la technologie. Plus il y a de technologie, plus il y a de développement. Toutefois, cette approche a échoué dans plusieurs pays (principalement dans les anciens pays socialistes)

dans lesquels il s'est finalement avéré que le développement est un processus beaucoup plus complexe. La technologie est nécessaire mais ne suffit pas à elle seule en tant que condition suffisante pour le développement. Les autres éléments intègrent un cadre de régulation, un soutien financier, une disponibilité des ressources humaines, et d'autres conditions socioculturelles. Même si tous ces ingrédients sont réunis, le défi majeur demeure : comment et quand doivent-ils interagir, être utilisés et combinés

### L'accès: le développement des infrastructures de télécommunications et de l'Internet

L'accès à l'Internet est l'un des plus grands défis pour surmonter la fracture numérique. Le taux de pénétration de l'Internet en Afrique est de l'ordre de 5,6 %, comparé à 73,8% au Japon ou 60,7% en Europe.<sup>3</sup> Il y a deux grands problèmes dans l'accès Internet dans les pays en développement. Premièrement, c'est l'accès aux backbones Internet internationaux. Deuxièmement, c'est le problème de connectivité entre les pays en développement.

L'accès aux backbones Internet internationaux dépend principalement de la disponibilité du câble sous marin à fibre optique. Pendant longtemps, seule l'Afrique occidentale, jusqu'en Afrique du Sud, était desservie par le câble sous-marin SAT-3. Après l'Afrique de l'Est s'est également reliée à un câble sous-marin : *Eastern African Submarine System (EASSY)* qui a commencé à fonctionner en juillet 2010.<sup>4</sup> Quelques autres câbles sous marin additionnels seront fonctionnels dans un futur proche. Cela va créer un puissant pourtour numérique autour de l'Afrique ce qui va substantiellement accroître la bande passante disponible pour tout le continent africain.<sup>5</sup>



Deuxièmement, c'est l'introduction de points d'échanges Internet (IXPs) qui maintiennent le trafic local dans le pays et qui réduit à la fois l'usage et les coûts de la bande passante internationale.<sup>6</sup> Beaucoup de pays africains n'ont pas encore de point d'échange Internet, ce qui signifie qu'une grande partie du trafic entre clients d'un même pays transitent par un autre pays. Ceci augmente le volume des données longue-distance et le coût de fourniture du service Internet. Plusieurs initiatives tentent d'établir des IXP dans les pays en développement. L'initiative qui a atteint un certain niveau de succès est celle de l'Association Africaine des fournisseurs d'accès Internet. Cette association a été à la base de l'installation de plusieurs points d'échange internet en Afrique.<sup>7</sup>

La connectivité à l'intérieur des pays en développement est un autre grand défi. La majorité des utilisateurs d'Internet se concentrent dans les grandes villes. Les zones rurales sont restées sans possibilité d'accès à Internet. La situation a commencé à changer avec le développement rapide de la téléphonie mobile et des communications sans fil. Patrick Gelsinger d'Intel a conseillé aux Africains de dire 'non' aux infrastructures de télécommunications en cuivre et de continuer à utiliser le sans fil comme solution pour la boucle locale et la fibre optique pour les backbones nationaux. La communication sans fil doit être la solution au problème du développement d'infrastructures de communication terrestres traditionnelles (Déploiement des câbles sur de très longues distances partout à l'intérieur des pays asiatiques et africains). Dans ce cas, le problème du dernier kilomètre ou de la boucle locale, un des grands obstacles pour un développement rapide de l'Internet, pourrait être surmonté.

### **Le soutien financier**

Les pays en développement reçoivent des soutiens financiers par différents canaux y compris par les agences bilatérales ou multilatérales de développement comme le PNUD ou la Banque Mondiale, ainsi que les initiatives de développement régionales et les banques. Avec la libéralisation accrue du marché des télécommunications, une tendance au développement des infrastructures de télécommunications au moyen d'investissements étrangers directs s'est accrue. Étant donné que les marchés de télécommunications des pays développés sont sursaturés, plusieurs compagnies internationales de télécommunications considèrent les marchés des pays en développement comme des zones de croissance dans l'avenir.

Pendant le processus du SMSI, l'importance d'un soutien financier pour réduire la fracture numérique a été clairement reconnue. Une des idées

proposées au SMSI a été l'établissement d'un Fonds de solidarité numérique administré par les Nations Unies pour aider technologiquement les pays les moins avancés à construire les infrastructures de télécommunications. Cependant, la proposition n'a pas reçu un vrai soutien de la part des pays développés, qui ont favorisé des investissements directs à la place d'un fonds de développement centralisé. Après le SMSI, le Fonds de solidarité numérique s'est installé à Genève en tant que fondation indépendante principalement financée par les villes et les autorités locales du monde entier.

### Les aspects socioculturels

Les aspects socioculturels de la fracture numérique englobent plusieurs aspects, y compris l'alphabétisation, les capacités TIC, la formation, l'éducation et la protection des langues.

Pour les pays en développement, un des problèmes a été la 'fuite des cerveaux' décrit comme le mouvement de la main d'œuvre hautement qualifiée des pays en développement vers les pays développés. A travers la fuite des cerveaux, les pays en développement ont perdu à bien des égards. La principale perte réside dans la perte de la main d'œuvre qualifiée. Les pays en développement ont également perdu dans leurs investissements dans la formation et l'éducation des travailleurs qualifiés émigrants. La tendance est que la fuite des cerveaux va continuer au regard de différents schémas d'émigration mis en place par les Etats-Unis, l'Allemagne et les autres pays développés en vue d'attirer une main d'œuvre qualifiée, principalement dans le domaine des TIC.

Un des développements qui peut stopper, ou dans une certaine mesure, inverser la fuite des cerveaux, est l'accroissement de l'externalisation des tâches liées aux TIC vers les pays en développement. Les exemples les plus réussis sont les centres industriels de développements de logiciels, tel que Bangalore et Hyderabad.

Au niveau mondial, les Nations Unies ont initié le *Digital Diaspora Network* pour promouvoir le développement en Afrique, à travers une mobilisation d'expertise technologique, entrepreneuriale et professionnelle ainsi que les ressources de la diaspora africaine spécialiste en TICs.

### La politique et la régulation des télécommunications

Les problèmes de politique de télécommunications sont très liés la réduction de la fracture numérique.

- Les investisseurs privés et de plus en plus de donateurs publics sont de plus en plus réticents à investir dans les pays sans un environnement légal et institutionnel approprié pour le développement de l'Internet.
- Le développement du secteur national des TIC dépend de la création d'un cadre nécessaire de régulation.
- La politique des télécommunications devrait faciliter la mise en place d'un marché de télécommunications efficace avec plus de compétition, des coûts bas et une grande variété des services fournis.

La création d'un environnement incitatif est une tâche exigeante, entraînant une démonopolisation du marché des télécommunications, l'introduction d'une réglementation liée à Internet (couvrant le cybercrime, le copyright, la protection de la vie privée, le e-commerce, etc.), et garantir l'accès de tous les citoyens sans restriction.

Institutionnellement parlant, une des premières étapes est la mise en place d'autorités de régulation des télécommunications indépendantes et professionnelles. L'expérience des pays développés montre que des régulateurs solides sont la condition primordiale d'un développement rapide d'infrastructures de télécommunications. Dans les pays en développement, le développement d'autorités de régulation est encore à ses débuts. Ces autorités sont généralement faibles, manquent d'indépendance et font souvent partie du système dans lequel les opérateurs télécoms appartenant à l'Etat influencent le processus politique et la régulation.

Un autre défi a été la libéralisation du marché des télécommunications. L'Inde et le Brésil sont souvent cités comme les pays en développement où la libéralisation a facilité la croissance de l'Internet et du secteur des TIC. Cela a également été bénéfique à toute l'économie de ces pays. D'autres pays, les moins avancés en particulier, trouvent que la libéralisation du marché des télécommunications est un grand défi. Avec la perte des monopoles de télécommunications, les gouvernements de ces Etats ont perdu de grandes sources de revenus budgétaires. Dans d'autres cas, alors qu'ils perdaient les revenus, ces pays n'ont pas récolté les bénéfices de cette libéralisation sous forme de baisse de coûts et d'amélioration de services de télécommunications. Dans beaucoup de cas, cela était dû au fait que la privatisation de ces compagnies de télécommunications n'étaient pas doublée par l'instauration un marché efficace et compétitif. De telles pratiques ont conduit la Banque Mondiale à insister sur le fait que ces pays ouvrent les plus grandes parts de marché de télécommunications à la concurrence avant de, ou concomitamment, privatiser les opérateurs étatiques ; dans ce cas, ils réduiront plus rapidement les coûts que ne le feront les pays qui privatisent d'abord et introduisent ensuite la concurrence.<sup>8</sup>

## Notes de fin

- <sup>1</sup> Falling through the Net? *The Economist*, 21 Septembre 2000.
- <sup>2</sup> DOT Force (2001) Digital opportunities for all: Meeting the challenge. Rapport du Digital Opportunity Task Force (DOT Force) incluant une proposition pour ‘un plan d’action Genoa’. Accessible sur : <http://www.g7.utoronto.ca/summit/2001genoa/dotforce1.html>
- <sup>3</sup> Internet World Stats. Accessible sur: <http://www.internetworldstats.com/stats.htm>
- <sup>4</sup> <http://www.eassy.org/>
- <sup>5</sup> Une carte des câbles sous marins autour de l’Afrique est accessible sur: <http://manypossibilities.net/african-undersea-cables/>
- <sup>6</sup> Les points d’échange Internet (Internet exchange points IXPs) sont des infrastructures techniques par lesquelles les Fournisseurs de Service Internet échangent du trafic par ‘peering’. Les IXPs sont généralement mis en place dans le but de maintenir le trafic internet à l’intérieur de petites communautés (par exemple une ville, une région, un pays), permettant d’éviter un routage inutile des paquets par des lieux géographiquement éloignés.
- <sup>7</sup> MTN (2008) ‘We are MTN’. Accessible sur: <http://www.mtn.co.za/?pid=8049>
- <sup>8</sup> Ismail S (2006) Analyzing the World Bank’s blueprint for promoting ‘information and communications. *Federal Communications Law Journal* 59(1). Disponible sur: <http://www.law.indiana.edu/fclj/pubs/v59/no1/13-Book%20ReviewFINAL.pdf>



## Section 6

---

# La corbeille socioculturelle





# La corbeille socioculturelle

L'internet a eu un impact considérable sur la configuration sociale et culturelle de la société moderne. Il est difficile d'identifier un secteur de notre vie sociale qui n'ait pas été affecté par l'internet. L'internet introduit de nouveaux canaux de communication, brise les barrières linguistiques, et crée de nouvelles formes d'expression. Aujourd'hui, l'Internet est entrain de devenir progressivement plus un phénomène social, qu'un phénomène technologique.

## Les droits de l'homme

Un ensemble de base des droits de l'homme relatifs à Internet inclut la vie privée, la liberté d'expression, le droit à l'information, divers droits protégeant la diversité culturelle, linguistique et minoritaire, et le droit à l'éducation. Il n'est pas surprenant que les problèmes relatifs aux droits de l'homme aient été très souvent à la fois débattus au Sommet Mondial sur la Société de l'Information (SMSI) et dans les processus du Forum sur la Gouvernance de l'Internet (FGI).

Alors que les droits de l'homme sont clairement abordés, ils sont aussi impliqués dans des aspects transversaux qui surgissent lorsqu'on traite de la neutralité du réseau (droit à l'accès, à la liberté d'expression, et à l'anonymat), la cyber sécurité (prise en compte des droits de l'homme au moment de l'exécution des activités de protection et de la cyber sécurité), le contrôle du contenu etc. Le SMSI a reconnu l'importance des droits de l'homme, en particulier le droit au développement et le droit à la liberté d'expression.

## Les droits du monde réel contre les droits du cyberespace

Parallèlement au débat juridique conceptuel sur la question de savoir si la loi actuelle est suffisante pour réguler l'Internet ou s'il y a besoin d'une nouvelle loi du cyberespace, il y a eu un débat dans les milieux des droits de l'homme au sujet de savoir si les concepts traditionnels des droits de l'homme ont besoin d'être révisés en vue de leur usage sur Internet. L'Association pour le Progrès des Communications (APC) dans la charte des droits sur internet stipule que les droits de l'homme relatifs à l'Internet sont fortement incarnés dans le système des droits de l'Homme des Nations Unies basés sur la Déclaration Universelle des Droits de l'Homme et d'autres instruments connexes.<sup>1</sup>

Il y a aussi une proposition pour l'établissement du droit de communiquer comme un nouveau type de droit de l'homme principalement inspiré par de nouvelles formes de communication basées sur l'Internet.

## L'enquête sur des initiatives sur les droits de l'homme et l'Internet

La principale initiative sur les cyber-droits est présentement '*Internet Bill of Rights*' (IBR) sponsorisé par le gouvernement de l'Italie et la société civile. Ce projet a déclenché le processus actuellement supporté par la Coalition<sup>2</sup> des Droits et Principes Dynamiques sur Internet et inclus d'autres développements, tels que les droits de surveillance de l'internet. L'IBR a été débattu à tous les précédents FGI. Dans une tentative de délimiter les cybers droits, l'APC a ébauché une charte<sup>3</sup> des droits sur Internet. Une autre initiative à prédominance académique est la charte de la liberté sur des réseaux de communication proposée par la Faculté de Droit à l'Université de Toronto.

Google, Microsoft et quelques autres compagnies Internet ont initié l'Initiative de Réseau Global (Global Network Initiative) en novembre 2008 avec l'objectif principal de promouvoir les droits de l'homme, en particulier la liberté d'expression et la vie privée.

### Le droit d'accès à l'Internet

La Finlande est l'un des premier pays à légalement garantir le droit d'accès à l'internet. Comme en juillet 2010 tous les citoyens en Finlande vont avoir le droit à un-megabit de connexion large bande.

Cette initiative est particulièrement importante parce que les activités commerciales des grandes compagnies de l'Internet peuvent directement affecter la manière dont les droits de l'homme sont protégés.<sup>4</sup>

## Les Activités du Conseil de l'Europe sur les droits de l'homme et l'Internet

L'un des principaux acteurs dans le domaine des droits de l'homme et de l'Internet est le Conseil de l'Europe. Ce Conseil est l'institution centrale de cette activité qui est en charge des droits de l'homme paneuropéens, avec la Convention Européenne pour la Protection des Droits de l'homme et des Libertés Fondamentales (195)<sup>5</sup> comme principal instrument. Depuis 2003, le Conseil de l'Europe a adopté plusieurs déclarations mettant en exergue l'importance des droits de l'homme sur Internet.<sup>6</sup>

Le Conseil est aussi le dépositaire de la Convention sur la cybercriminalité comme principal instrument dans ce domaine au niveau mondial. Ceci peut positionner le Conseil de l'Europe comme l'une des institutions clé dans la recherche de l'équilibre entre les droits de l'homme et les impératifs de la cybercriminalité dans le développement futur de l'Internet.

## La liberté d'expression et le droit de rechercher, de recevoir à partager l'information

L'un des domaines les plus controversés concernant les droits de l'homme sur l'Internet c'est la liberté d'expression. C'est l'un des droits de l'homme le plus fondamental, qui revient souvent au centre des débats sur le contrôle et la censure des contenus. Dans la Déclaration Universelle des Droits de l'Homme, la liberté d'expression (Article 19) est contre balancée par le droit de l'Etat de limiter la liberté d'expression pour des besoins de la moralité de l'ordre public et du bien-être général (Article 29). Ainsi, à la fois la discussion sur l'article 19 et sa mise en application doivent être placées dans le contexte d'établissement d'un équilibre adéquat entre les deux besoins. Cette situation ambiguë donne lieux à beaucoup de possibilités d'interprétations des normes et finalement à plusieurs possibilités de mise en pratique. Cette controverse autour du juste équilibre entre les articles 10 et 29 dans le monde 'réel' se reflète dans les débats sur la recherche de cet équilibre sur Internet.

La liberté d'expression est la préoccupation particulière des organisations non gouvernementales (ONG) des droits de l'homme telles qu'"Amnesty international" et le 'Freedom House'. Une étude récente conduite par 'Freedom House' évalue le niveau de liberté, sur l'Internet et sur le téléphone mobile, dont jouissent les utilisateurs moyens dans un échantillon de 15 pays à travers 6 régions. Couvrant le calendrier des années 2007–2008, l'étude fait l'inventaire des facteurs qui pourraient affecter une telle liberté y compris l'infrastructure des télécommunications de l'Etat, les restrictions du gouvernement sur l'accès à la technologie, le cadre de régulation pour les

fournisseurs de services, la censure et le contrôle du contenu, l'environnement juridique, la surveillance, et les attaques extra judiciaires sur les utilisateurs ou les producteurs de contenu. Les indicateurs sélectionnés couvrent non seulement les actions des gouvernements mais aussi la rigueur, la diversité, et l'activisme dans le domaine des nouveaux médias dans chaque pays, quel que soit les efforts ou en dépit des efforts du gouvernement à en restreindre l'usage.<sup>7</sup>

## La politique du contenu

L'un des principaux aspects du volet socioculturel est la politique du contenu, souvent abordée sous l'angle des droits de l'homme (liberté d'expression et droit à communiquer), du point de vue du gouvernement (contrôle du contenu), et de la technologie (les outils de contrôle du contenu). Les débats sont généralement centrés sur trois groupes de contenu.

- 1 Les contenus qui ont recueilli un large consensus pour son contrôle. Sont inclus ici la pornographie infantile, la justification du génocide, et l'incitation ou l'organisation d'actes terroristes; tout ce qui est interdit par le droit international (*ius cogens*).<sup>8</sup>
- 2 Les contenus sensibles pour des pays, régions, ou groupes ethniques particuliers à cause de leurs valeurs culturelles et religieuses particulières. Une communication globalisée en ligne fait ressurgir des défis pour des valeurs culturelles et religieuses dans plusieurs sociétés. La plupart du temps, le contrôle de contenu au Moyen-Orient et dans les pays d'Asie est officiellement justifié par la protection des valeurs culturelles spécifiques. Cela explique pourquoi l'accès aux sites pornographiques et aux jeux de paris en ligne est souvent bloqué.<sup>9</sup>
- 3 La censure politique sur Internet. En 2007, Reporters sans Frontières a rapporté que 12 pays font de la censure politique sur l'Internet.<sup>10</sup>

### Comment la politique du contenu est-elle conduite?

Un menu à la carte pour la politique du contenu contient les options juridiques et techniques suivantes qui sont utilisées dans différentes combinaisons.

### Le filtrage gouvernemental du contenu

L'élément commun pour le filtrage gouvernemental est un Index Internet des sites web bloqués à l'accès dès qu'ils sont sollicités par les citoyens.<sup>11</sup> Si un site web fait parti de l'index Internet, l'accès à ce site ne sera pas accordé.

Du point de vue technique, le filtrage utilise généralement le blocage d'adresses du protocole Internet (IP) au niveau du routeur, au niveau des serveurs proxy, et au niveau de la redirection du système de nom de domaine (DNS).<sup>12</sup> En plus des pays qui habituellement s'adonnent à ces pratiques telles que la Chine, l'Arabie Saoudite, et Singapour, d'autres pays adoptent de plus en plus cette pratique. Par exemple, l'Australie à un système de filtrage pour certaines pages nationales spécifiques, bien quelles ne soient pas internationales.<sup>13</sup>

### Les systèmes de classement et de filtrage privés

Face au risque potentiel de la désintégration de l'Internet à cause du développement de diverses barrières nationales (systèmes de filtrage), le W3C (World Wide Web Consortium) et d'autres institutions similaires ont pris des mesures proactives en proposant la mise en œuvre de systèmes de classement et de filtrage contrôlés par l'utilisateur.<sup>14</sup> Dans ces systèmes, les mécanismes de filtrage sont intégrés dans les navigateurs Internet. Un label indique l'accessibilité d'un contenu particulier sur un site Web particulier. L'usage de ce type de filtrage est particulièrement favorisé en ayant accès à des sites adaptés aux enfants.

### Filtrage des contenus basés sur la géo-localisation

Une autre solution technique relative au contenu est l'utilisation de logiciels de géo-localisation, qui filtrent l'accès à un contenu Internet particulier selon l'origine nationale ou géographie des utilisateurs.

Le cas de Yahoo! fut un exemple important à cet égard, puisque le groupe d'experts impliqués, y compris Vint Cerf, ont indiqué que dans 70 à 90 % des cas, Yahoo! pourrait déterminer si les sections d'un de ses sites web hébergeant des souvenirs nazis étaient accessibles à partir de la France.<sup>15</sup>

Les compagnies de géo-localisation déclarent qu'elles peuvent identifier le pays d'origine avec certitude et identifier la ville, dans environ 85% des cas, particulièrement s'il s'agit d'une grande ville.<sup>16</sup>

### Le contrôle de contenu à travers les moteurs de recherche

Le pont entre le dernier utilisateur et le contenu web est généralement le moteur de recherche. Il a été rapporté que les autorités chinoises avaient initié l'un des premiers exemples du contrôle de contenu à partir des moteurs de recherche. Si les utilisateurs entraient des mots interdits dans la recherche Google, ils perdaient leur connectivité IP pour quelques minutes.<sup>17</sup> La réponse du département de l'information Chinois est la suivante:

*'... avec certains sites Internet, il est vraiment normal que parfois vous puissiez y accéder et d'autres fois non. Le ministère n'a reçu aucune information au sujet du blocage de Google.'*<sup>18</sup>

Le filtrage des recherches était l'une des raisons de la récente tension entre Google et les autorités Chinoises.<sup>19</sup>

Pour s'ajuster à certaines lois locales, Google a décidé de limiter quelques contenus sur des sites nationaux. Par exemple, sur la version Française et Allemande de Google, il n'est pas possible de chercher et de trouver de sites web avec un contenu nazi. Ceci implique un certain niveau d'autocensure pour éviter des possibles cas litigieux.<sup>20</sup>

### Le déficit du Web 2.0: les utilisateurs comme contributeurs

Avec le développement des Plateformes Web 2.0 - des blogs, des forums, des sites web de partage des documents, des mondes virtuels - la différence entre l'utilisateur et le créateur s'est amenuisée. Les utilisateurs de l'Internet peuvent créer des larges portions de contenu web, telles que le postage de blogs, des vidéos You Tube et des galeries de photos.

Identifier, filtrer et étiqueter les sites web "impropres" devient progressivement difficile. Pendant que les techniques de filtrage automatique existent déjà, la reconnaissance automatique, le filtrage et l'étiquetage du contenu visuel n'est pas encore réalisable.

Une approche utilisée quelques fois par le Maroc, le Pakistan, la Turquie et la Tunisie consiste à bloquer l'accès à You Tube dans tout le pays. Cette approche maximaliste conduit par ailleurs à un blocage non objectif de contenu car même un contenu éducatif se retrouve inaccessible.

### Nécessité d'un cadre juridique approprié

Le vide juridique dans le domaine de la politique du contenu permet aux gouvernements de décider en toute discrétion quel contenu devrait être bloqué. Puisque la politique du contenu est une question sensible pour chaque société, l'adoption d'actes juridiques est vitale. La régulation nationale dans le domaine de la politique du contenu peut fournir une meilleure protection de droit de l'homme et régler les occasionnels problèmes du rôle ambigu des fournisseurs d'accès Internet (FAI), des agences de mise en application et d'autres acteurs. Ces dernières années, plusieurs pays ont introduit une loi sur la politique du contenu.

## Les initiatives internationales

Au niveau international, les initiatives principales viennent des pays européens avec une loi stricte dans le domaine des discours haineux incluant le racisme et l'antisémitisme. Les institutions régionales européennes ont tenté d'appliquer ces règles sur le cyberspace. Le premier acte juridique abordant le problème du contenu est le protocole additionnel du conseil de l'Europe sur la convention contre la cybercriminalité.

L'UE a initié le contrôle du contenu, adoptant la recommandation de la Commission Européenne contre le Racisme via l'Internet. A un niveau plus pratique, l'UE a introduit un plan d'action sur la sécurité de l'Internet qui comprend les principaux points suivants:

- Mise en place du réseau européen des 'centres d'écoutes et de traitement' pour le rapportage des contenus illégaux.
- Encourager l'autorégulation.
- Mise en place de système de classement de contenu, de filtrage, et d'évaluation pour le filtrage.
- Développement de logiciels et de services.
- Mener une campagne de sensibilisation pour l'utilisation sécurisée de l'Internet.<sup>21</sup>

L'Organisation de la sécurité et la coopération en Europe est aussi active dans ce domaine. Depuis 2003, un certain nombre de conférences et de réunions ont été organisées avec un accent particulier mis sur la liberté d'expression et les potentiels abus sur Internet (ex. la propagande raciste, xénophobe et antisémite).

## Les enjeux

### Le contrôle du contenu face à la liberté d'expression

S'agissant du contrôle du contenu, le revers de la médaille est très souvent la restriction de la liberté d'expression. Ceci est surtout important aux Etats Unis où le Premier amendement garantit une totale liberté d'expression, et même le droit de publier des contenus nazis et connexes.

La liberté d'expression contribue largement au positionnement des Etats Unis dans le débat international sur les problèmes relatifs à l'Internet. Par exemple, au moment où les Etats Unis ont signé la Convention sur la cybercriminalité, ils ne pouvaient pas signer un protocole additionnel qui traite du discours

haineux et du contrôle du contenu. La question de la liberté d'expression était aussi soulevée dans le contexte du cas judiciaire de Yahoo! Dans ses initiatives internationales, les États Unis ne franchiront pas la ligne jusqu'au bout afin d'éviter de compromettre la liberté d'expression telle que stipulée dans le Premier amendement.

### Illicite hors ligne – illicite en ligne

Ceci porte le débat au sujet du dilemme entre le monde réel et l'univers 'cybernétique'. Les règles existantes au sujet du contenu peuvent être appliquées sur l'Internet. Cela est fréquemment mis en exergue dans le contexte européen. La Décision - cadre du Conseil de l'UE sur la lutte contre le racisme et la xénophobie indique clairement que 'ce qui est illicite hors de l'Internet, est aussi illicite sur Internet'. L'un des arguments de l'approche cyber à la régulation de l'Internet est que la quantité (intensité de communication, le nombre de messages) crée une différence qualitative. De ce point de vue, le problème du discours haineux ne réside pas dans le fait qu'aucune régulation n'est exercée contre ce fléau, mais que le partage et la propagation à travers l'Internet donne lieu à un autre type de problème juridique. Il y a plus d'individus exposés et il est difficile de faire appliquer les règles existantes. Par conséquent, la différence apportée par l'Internet est essentiellement liée aux problèmes d'application des règles, et non aux règles elles-mêmes.

### L'efficacité du contrôle de contenu

Dans les débats concernant la politique de l'Internet, l'un des arguments clés est que la nature décentralisée de l'internet permet de contourner la censure. L'Internet dispose de plusieurs techniques et mécanismes pouvant assurer un contrôle efficace. Cependant, techniquement parlant, ces mécanismes de contrôle peuvent être contournés.

Dans les pays où le contrôle direct du contenu par le gouvernement est en vigueur, des usagers techniquement doués ont trouvé des moyens pour échapper à un tel contrôle. Néanmoins, le contrôle des contenus n'est pas tourné vers ce petit groupe d'usagers techniquement doués ; il vise la masse populaire. D'après Lessig, 'une régulation n'a pas besoin d'être totalement effective pour être suffisamment efficace'.<sup>22</sup>

### Qui devrait être responsable de la politique du contenu?

Les acteurs principaux dans le domaine du contrôle des contenus sont les gouvernements. Les gouvernements prescrivent quel contenu doit être contrôlé et comment. Les FAI, comme les passerelles Internet, sont habituellement tenus pour responsables de la mise en œuvre du filtrage des contenus, soit selon les prescriptions du gouvernement ou selon

l'auto régulation (au moins sur les questions à large consensus, telles que la pornographie infantile).<sup>23</sup> Certains groupes d'utilisateurs, tels que les parents, sont désireux d'introduire une politique de contenu plus efficace pour protéger les enfants. Plusieurs initiatives de classement aident les parents à trouver des contenus adaptés aux enfants. De nouvelles versions de navigateurs Internet intègrent habituellement plusieurs options de filtrage. Les compagnies privées et les universités appliquent aussi les contrôles des contenus. Dans certains cas, les contenus sont contrôlés à travers des *packages* de logiciels; par exemple, le mouvement de la scientologie a distribué un package de logiciels aux membres, lesquels logiciels interdisent l'accès aux sites web critiques envers la scientologie.<sup>24</sup>

## La vie privée et la protection des données<sup>25</sup>

La vie privée et la protection des données sont deux problèmes étroitement liées à la gouvernance de l'Internet. La protection des données est un mécanisme juridique qui garantit la vie privée. A ce propos, qu'est-ce que la vie privée? Elle est souvent définie comme le droit de tout citoyen de contrôler son information personnelle et d'en décider (de la garder en secret ou de la divulguer). La vie privée est un droit fondamental de l'homme. Elle est reconnue dans la déclaration universelle des droits de l'Homme, dans la Convention internationale sur les droits civils et politiques, et dans d'autres conventions régionales et internationales des droits de la personne humaine.

Les cultures nationales et les modes de vie influencent la pratique de la vie privée. Bien que cette question soit préoccupante dans les sociétés occidentales, elle peut avoir moins d'importance dans d'autres cultures. Les pratiques modernes de la vie privée se focalisent sur la confidentialité dans la communication (pas de surveillance de la communication) et sur la confidentialité de l'information (ne pas manipuler les informations individuelles). Les questions de vie privée qui se focalisaient naguère sur les activités gouvernementales incluent désormais le secteur privé, comme décrit dans le triangle sur la vie privée illustrée sur la page ci-contre.<sup>26</sup>

### La protection de la vie privée: les questions en discussion

#### Les individus et les Etats

L'information a toujours été un outil essentiel des Etats pour exercer le pouvoir sur leurs territoires et sur les populations. Les gouvernements



collectant une grande partie des informations personnelles (Registres des naissances et des mariages, les parts de sécurité sociale, les listes électorales, les casiers judiciaires, les registres de commerce, les attestations de résidence, les cartes grises) il n'est pas possible pour un individu d'échapper aux opérations de collecte d'informations surtout que même en cas d'émigration dans un autre pays, il ou elle sera confronté(e) au même problème.

La technologie de l'information telle que celle utilisée dans l'extraction de connaissances à partir des données contribue à l'agrégation et la corrélation des données à partir de beaucoup de systèmes spécialisés (exemple la taxation, les attestations de résidences, cartes grises) pour mener des analyses approfondies, permettant la recherche de faits inhabituels et des incohérences. L'un des défis majeurs des initiatives de la gouvernance électronique est de garantir un équilibre adéquat entre la modernisation des fonctions gouvernementales et la garantie des droits à la vie privée pour les citoyens.

Après les événements du 11 Septembre 2001 aux Etats Unis, le '*US Patriot Act*' et une législation similaire dans d'autres pays avaient permis au pouvoir exécutif d'élargir son autorité dans la collecte d'informations et même de constituer une base de données d'informations à des fins judiciaires.<sup>27</sup>

Le concept de l'interception légale pour la fourniture de preuves est aussi incluse dans la Convention du conseil de l'Europe sur la cyber criminalité (Article 20 et 21).

### Les individus et le monde des affaires

Dans le triangle de la vie privé ci-dessous évoquée, la deuxième relation qui est en plein essor est celle entre les individus et le secteur privé. Les gens divulguent des données personnelles à l'ouverture d'un compte bancaire, lors de la réservation de places sur des vols ou d'une chambre d'hôtel, lors de transactions en ligne par carte de crédit ou lors de recherches sur internet. Plusieurs traces des données sont souvent laissées lors de chacune de ces activités.

Dans une économie de l'information, les informations au sujet des clients, y compris leurs préférences et profils d'achats, devient un bien commercial important. Pour certaines compagnies telles Google et Amazon, l'information sur les préférences des clients constitue le noyau de leur modèle d'affaire. Le succès et la durabilité du commerce électronique, (affaires-clients et affaires-affaires) dépendent de l'établissement de la confiance à la fois dans les politiques de respect de leur vie privée et dans les mesures de sécurité qu'ils établissent pour protéger les informations confidentielles des clients contre le vol et l'usurpation.<sup>28</sup> Avec l'expansion des plateformes de réseaux sociaux, des inquiétudes naissent à propos d'une éventuelle usurpation des données personnelles non seulement par le propriétaire ou l'administrateur de la plateforme du réseau social mais aussi par d'autres individus qui y participent.

### Les Etats et le monde des affaires

Le 3<sup>e</sup> côté du triangle de la vie privée est le moins médiatisé, mais il constitue certainement la question la plus importante de la vie privée. Les Etats et les entreprises collectent une quantité importante de données individuelles. Certaines de ces données sont échangées avec d'autres Etats et d'autres entreprises pour étoffer des activités terroristes. Cependant, dans certaines situations telles que celles auxquelles s'appliquent la Directive européenne sur la protection des données, l'Etat surveille et protège les données individuelles tenues par des compagnies.

### Les individus entre eux

Le dernier aspect dans le triangle de la protection de la vie privée, non représenté dans le triangle de la vie privée, constitue un potentiel à risque pour la protection de la vie privée. De nos jours, des individus ayant suffisamment de moyens financiers peuvent avoir accès à de puissants outils de surveillance. Ainsi, un simple téléphone portable équipé d'une caméra peut devenir un outil de surveillance. La technologie a rendu plus populaire la surveillance; pour citer le magazine *'The Economist'*. Plusieurs occasions d'intrusion dans la vie privée se sont manifestées, partant du simple voyeurisme à l'usage de cameras sophistiquées pour enregistrer des

cartes bancaires et pour l'espionnage électronique. Le problème majeur pour la protection de ce type de violation de la vie privée est que la plupart des législations se focalisent sur les risques de violation de la vie privée émanant de l'Etat. Face à cette nouvelle réalité, quelques gouvernements ont fait des démarches en prenant certaines initiatives. Le congrès Américain a adopté l'Acte de prévention contre le vidéo voyeurisme interdisant de filmer des personnes nues sans leur accord. L'Allemagne et d'autres pays ont adopté des lois similaires pour réglementer la surveillance des personnes.

### **La régulation internationale de la protection de la vie privée et des données**

L'un des plus importants instruments sur la protection des données et de la vie privée est la Convention du Conseil de l'Europe pour la protection des individus face à l'informatisation des données personnelles de 1981. Bien qu'elle fût adoptée par le Conseil de l'Europe, elle est ouverte à d'autres pays, y compris les Etats non européens. Puisque la convention est technologiquement neutre, elle a survécu à l'épreuve du temps. Plus récemment, elle a été examinée pour être appliquée à la collecte et l'informatisation des données biométriques. La Directive de l'UE sur la protection des données (Directive 45/46/EC) a également constitué à un cadre législatif important dans l'informatisation des données personnelles dans l'UE et a eu un grand impact sur le développement de la législation nationale non seulement en Europe mais aussi d'une manière globale.

Un autre document international clé – non contraignant – sur la vie privée et la protection des données est celui de l'Organisation pour le Développement et la Coopération Economique (OECD) concernant les Lignes directrices sur la protection de la vie privée et les flux transfrontaliers des données personnelles de 1980. Ces lignes directrices et les travaux subséquents de l'OECD ont inspiré plusieurs régulations nationales, régionales et internationales sur la protection de la vie privée et des données personnelles. De nos jours, tous les pays de l'OECD ont virtuellement mis en place des lois sur la protection de la vie privée et des données personnelles et ont accordé les pleins pouvoirs aux autorités pour leur mise en œuvre.

Même si les principes de l'OCDE ont été largement acceptés, la grande différence réside dans leur mise en œuvre, particulièrement entre l'approche européenne et l'approche américaine. En Europe, il y a une législation générale sur la protection des données alors qu'aux Etats-Unis cette régulation sur la vie privée est développée dans chaque secteur de l'économie, y compris la vie privée en matière de finances (La loi Graham-Leach-Bliley)<sup>29,30</sup>, la vie privée des enfants (la loi sur la protection de la vie privée des enfants en ligne)<sup>31</sup>, et la vie privée au niveau médical (les régulations

proposées sur des services de santé et à l'être humain)<sup>32</sup>. Une autre différence majeure est qu'en Europe, la législation sur la vie privée devrait être assurée par les pouvoirs publics, alors qu'aux Etats-Unis, la mise en œuvre se repose principalement sur le secteur privé et l'autorégulation. Les compagnies ont mis en place des politiques sur la vie privée. Il est du ressort des compagnies et des individus de décider par eux-mêmes les politiques de la vie privée à appliquer. La critique majeure de l'approche américaine est que les individus sont dans une position comparativement faible ; ils sont souvent peu conscients de l'importance des options offertes par les politiques sur la vie privée et ils sont généralement d'accord sans qu'ils soient eux-mêmes informés à ce sujet.

### L'accord 'Safe Harbour' entre les Etats-Unis d'Amérique et l'UE

Ces deux approches, américaine et européenne, sur la protection de la vie privée ont commencé à diverger. Le problème fondamental est né de l'usage que les compagnies commerciales font des données personnelles. Par exemple comment l'UE peut elle imposer ses normes sur les compagnies de logiciel basées aux Etats Unis? Et comment l'UE peut elle s'assurer que les données de ses citoyens sont protégées selon les règles mentionnées dans sa Directive sur la Protection de la vie privée? Selon quelles règles (qu'elles soient de l'approche américaine ou européenne) les données sont elles transférées à travers le réseau d'une compagnie à partir de l'UE vers les Etats Unis? L'UE a menacé de bloquer le transfert des données à tout pays qui ne pourrait pas observer le même niveau de protection de la vie privée comme clairement mentionnée dans sa Directive. Cela a inévitablement conduit à un clash avec l'approche américaine d'auto régulation dans la protection de la vie privée.

Cette profonde divergence a constitué un grand obstacle à la mise en place d'un accord. Par ailleurs, aligner la loi américaine à la Directive de l'UE ne serait rendu possible étant donné que cela nécessiterait le changement de certains principes importants du système judiciaire américain. La sortie de l'impasse s'est produite lorsque l'ambassadeur américain Aaron a suggéré une formule 'Safe Harbour'. Cela a reformulé toute la question et a fourni une issue de sortie de l'impasse lors des négociations.

Une solution a été trouvée où les régulations de l'UE pourraient être appliquées aux compagnies américaines en se référant aux dispositions du 'Safe Harbour'. Les compagnies américaines manipulant les données des citoyens de l'UE pourraient volontairement s'engager à observer les exigences de la protection de la vie privée de l'UE.

Après avoir signé, les compagnies doivent observer les mécanismes formels de renforcement conclus entre l'UE et les Etats Unis.

Au moment de sa signature en 2000, l'Accord 'Safe Harbour' a été accepté avec grand espoir comme outil juridique pouvant régler des problèmes similaires avec d'autres pays. Cependant, le bilan n'est pas très encourageant. Il a été critiqué par le parlement européen pour ne pas suffisamment protéger la vie privée des citoyens de l'UE. Les compagnies américaines n'étaient pas particulièrement enthousiastes à utiliser cette approche. Selon une récente étude faite par Galaxia, sur 1597 compagnies ayant souscrit au système 'Safe Harbour', seulement 348 en remplissent les exigences (par exemple la politique sur la vie privée).<sup>33</sup> Etant donné la grande importance attachée à la question relative à la protection de la vie privée et des données dans l'UE, il n'est pas exclu qu'une pression soit exercée jusqu'à ce qu'une solution soit trouvée au dysfonctionnement de l'accord 'Safe Harbour'.

## Multilinguisme et diversité culturelle

Dès ses premiers jours, Internet a été un médium à dominance anglophone. Selon certaines statistiques, environ 80% des contenus web sont en Anglais alors que 80% de la population mondiale ne parlent pas Anglais. Cette situation a poussé les pays à entreprendre des actions concertées en vue de promouvoir le multilinguisme et la protection de la diversité culturelle. La promotion du multilinguisme n'est pas seulement un problème culturel, mais est directement liée au besoin du développement de l'Internet.<sup>34</sup> Si l'Internet doit être utilisé par la grande majorité de la population et non pas seulement par quelques élites nationales, alors les contenus doivent être accessibles dans plusieurs langues.

### Les enjeux

#### Les alphabets non romains

La promotion du multilinguisme nécessite la mise au point de normes techniques qui puissent faciliter l'usage des alphabets non romains. L'une des premières initiatives à l'usage des ordinateurs multilingues était entreprise par le Consortium Unicode, une institution à but non lucratif qui développe des normes afin de faciliter l'usage de séries de caractères de différentes langues. A leur tour, l'Internet Corporation for Assigned Names and Numbers (ICANN) et l'Internet Engineering Task Force (IETF) ont joué

un rôle important dans la promotion des noms de domaines internationalisés (Internationalized Domain Names, en anglais). L'IDN facilite l'usage du nom de domaine écrit en Chinois, en Arabe, et dans d'autres alphabets non latins.<sup>35</sup>

### La traduction mécanique

Beaucoup d'efforts ont été fournis afin d'améliorer la traduction mécanique. Étant donné sa politique de traduction de toutes les cérémonies officielles dans les langues de tous les États membres, l'UE a sponsorisé plusieurs activités de développement dans le domaine de la traduction mécanique. Bien que de grands progrès soient faits, quelques difficultés demeurent.

### Cadres gouvernementaux appropriés

La promotion du multilinguisme nécessite des régimes appropriés de gouvernance. Le premier élément des régimes de gouvernance a été fourni par des organisations comme l'Organisation des Nations Unies pour la Science, l'Éducation et la Culture (UNESCO). L'UNESCO a suscité plusieurs initiatives en mettant l'accent sur le multilinguisme, y compris l'adoption de documents importants, tels que la Déclaration universelle sur la diversité culturelle. Un autre promoteur clé du multilinguisme est l'UE, puisqu'elle incarne le multilinguisme comme l'un de ses principes fondamentaux de travail.

L'évolution et l'usage à grande échelle des outils web 2.0, permettant aux utilisateurs ordinaires de devenir facilement des contributeurs et des développeurs de contenus, offre une opportunité pour une grande disponibilité de contenus locaux dans une grande variété de langues. Néanmoins, sans un grand cadre de promotion du multilinguisme cette opportunité pourrait finir par créer un fossé encore plus profond, si *l'engouement actuel n'est pas maintenu*. Les nouveaux usagers de l'Internet vont trouver plus utile d'apprendre l'Anglais et de l'utiliser en ligne, ce qui renforce le prestige de la langue en forçant ainsi les nouveaux usagers subséquents à apprendre eux même l'Anglais.<sup>36</sup>

### Biens publics universels

Le concept de bien publics universel peut être lié à plusieurs aspects de la gouvernance de l'Internet. Les implications les plus directes se trouvent dans les domaines de l'accès à l'infrastructure de l'Internet, la protection du savoir développé à travers l'interaction sur l'Internet, la protection des normes et standards techniques publiques et l'accès à l'éducation en ligne.

Des compagnies privées gèrent quasiment l'infrastructure de l'Internet. L'un des défis est l'harmonisation de la propriété privée de l'infrastructure de l'Internet avec le statut de l'Internet comme un bien public universel. Les législations nationales prévoient que la propriété privée puisse être limitée par certaines exigences publiques, y compris l'octroi de droits similaires à tous les utilisateurs potentiels et la non ingérence dans le contenu transporté.

L'une des caractéristiques primordiales de l'Internet est que par le biais de l'interaction à grande échelle des internautes, un nouveau savoir et de nouvelles informations voient le jour. Une masse importante de savoir a été générée à travers les échanges des *mailing-lists*, des réseaux sociaux et des blogs. A l'exception des 'creative commons',<sup>37</sup> il n'y a pas de mécanisme juridique pour protéger de telles connaissances. Laissées dans un vide juridique, ces connaissances ont été rendues libres pour la modification et la commercialisation. Ce groupe de connaissances communes, base importante de créativité, court le risque de s'épuiser. Plus le contenu Internet sera commercialisé, moins il y aura d'échanges spontanés. Ceci pourrait conduire à la réduction des interactions créatives.

Le concept de biens publics universels, associé aux initiatives telles que celle du 'creative commons' pourraient donner des solutions qui protégeraient à la fois l'environnement du créatif actuel de l'Internet et préserver les connaissances générées par l'Internet pour les générations futures.

En ce qui concerne la normalisation, des efforts presque constants sont fournis pour remplacer des normes publiques par celles dites privées et propriétaires. Ce fut le cas avec Microsoft (avec les navigateurs et ASP) et Sun Microsystems (avec Java).

Les standards Internet (principalement TCP / IP: Transmission Control Protocol Internet Protocol) sont ouverts et publics. Le régime de gouvernance de l'Internet devrait assurer la protection des normes principales de l'Internet comme des biens publics universels.

## Les enjeux

### Équilibre entre intérêts publics et privés

L'un des problèmes sous-jacents de la future évolution de l'Internet est l'établissement d'un équilibre entre les intérêts privés et les intérêts publics. La question est celle de savoir comment fournir un environnement commercial approprié au secteur privé tout en assurant le développement de

l'Internet comme bien public universel. Dans beaucoup de cas, ce n'est pas 'la somme-zéro' mais une situation 'gagnant-gagnant'. Google et bien d'autres entreprises de la vague du Web 2.0 ont réussi à développer des modèles d'affaires qui génèrent à la fois des revenus et permettent le développement créatif de l'Internet.

### **Protéger l'Internet comme un bien public universel<sup>38</sup>**

Quelques solutions peuvent être développées en se basant sur les concepts juridiques et économiques existants. Par exemple, la théorie économique a un concept bien développé de 'biens publics', qui a été élargi au niveau international au concept de 'biens publics universels'. Un bien public a deux propriétés critiques: la consommation non- concurrente et le caractère non-exclusif. La première stipule que la consommation d'un individu n'empêche pas celle d'un autre; la seconde, qui est difficile voire impossible, est celle qui consisterait à exclure un individu de la jouissance d'un bien. L'accès aux outils de base du web et à bien d'autres services Internet remplit les deux critères: la consommation non-concurrente et la consommation non-exclusive.

### **Droits des personnes vivant avec des handicaps<sup>39</sup>**

Les Nations Unies estiment qu'aujourd'hui 500 millions de personnes dans le monde vivent avec handicap. Ce nombre augmente chaque année à cause des facteurs tels que la guerre et la destruction, les mauvaises conditions sanitaires, ou le manque d'information au sujet du handicap, de ses causes, des moyens de sa prévention et de son traitement.<sup>40</sup> L'Internet fournit des nouvelles possibilités de réinsertion sociale des personnes vivant avec des handicaps. Dans le but de maximiser les possibilités technologiques des personnes vivant avec un handicap, il y a un besoin de développer la gouvernance de l'Internet et de son cadre politique. L'élément international fondamental dans ce domaine est la Convention sur les droits des personnes vivant avec un handicap, approuvée par les Nations Unies en 2006 et déjà ratifiée par 139 pays; qui établissent les droits qui sont entrain d'être progressivement inclus dans les législations nationales, et qui les rendront applicables dans quelques années.<sup>41</sup>

La prise de conscience sur les besoins de solutions technologiques qui prennent en ligne de compte les personnes avec un handicap s'accroît avec le travail des organisations qui enseignent et assistent la communauté des handicapés telles que la Coalition dynamique sur l'accessibilité et l'handicap<sup>42</sup> du FGI, ainsi que le Chapitre de l'Internet Society pour l'Handicap et les Besoins Spéciaux.<sup>43</sup>

Le manque d'accessibilité découle du fossé entre les capacités requises pour utiliser les équipements, les logiciels et les contenus, et la capacité disponible de la personne avec un handicap. Pour réduire ce fossé, il y a deux actions à entreprendre:

- 1 Inclure des normes d'accessibilités comme l'une des conditions requises lors de la conception d'équipements, de logiciels et de contenus.
- 2 Orienter les efforts vers la disponibilité des accessoires pour équipements et logiciels qui augmentent ou remplacent les capacités fonctionnelles de la personne.

Dans le domaine de la gouvernance de l'internet, l'accent principal est mis sur les contenus numériques, étant donné qu'ils sont en développement rapide et constituent une sorte d'infrastructure. Plusieurs applications en ligne ne respectent pas les normes d'accessibilité à cause du manque de prise de conscience ou de la complexité telle que perçue et des coûts élevés (on est loin de la réalité d'aujourd'hui). Les normes internationales ou nationales d'accessibilité numérique sont développées par W3C qui les appelle 'principes directeurs d'accessibilité au contenu web' (*Web Content Accessibility Guidelines: WCAG*).<sup>44</sup>

Une action politique qui devrait améliorer l'accès des personnes ayant un handicap est le régime universel pour l'Internet mis en place par l'Internet Society's Universal Design for the Internet (ISOC) qui est définie comme:

*Un régime dénommé 'Universal Design for the Internet' est mis en place pour assurer que la présentation du contenu sur l'Internet et la technologie de leur structuration soit assez flexible pour satisfaire les besoins du plus grand nombre possible d'utilisateurs potentiels sans distinction d'âge, de langue ou d'handicap.*<sup>45</sup>

## Education

L'internet a ouvert de nouvelles possibilités d'éducation. Plusieurs initiatives d'apprentissage électronique, d'apprentissage en ligne et de formation à distance ont été introduites. Leur but principal est d'utiliser l'internet comme un moyen de transmission du savoir. Bien qu'il ne puisse pas remplacer l'éducation traditionnelle, l'apprentissage en ligne fournit des nouvelles possibilités d'apprentissage. Particulièrement lorsque des contraintes spatio-temporelles ne permettent pas que la personne soit présente aux cours.

Certaines estimations laissent à croire que le marché de l'enseignement en ligne atteindra environ 10 milliards de dollars de chiffre d'affaire en 2010.

Traditionnellement, l'éducation a toujours été gérée par des institutions nationales. L'accréditation des institutions éducatives, la reconnaissance des diplômes, et l'assurance de la qualité sont toutes également gérées au niveau local. Par ailleurs, l'éducation trans-frontalière exige de nouveaux régimes de gestion. Plusieurs initiatives internationales visent à combler le vide, notamment dans les domaines tels que l'assurance de la qualité et la reconnaissance des diplômes académiques.

## Les enjeux

### L'OMC et l'Éducation

Une question controversée dans les négociations de l'Organisation Mondiale du Commerce (OMC) est l'interprétation des articles I.3 (b) et (c) de l'Accord général sur le commerce des services (AGCS), qui spécifient les exceptions du régime de libre échange pour les services fournis par le gouvernement. Selon un certain point de vue soutenu particulièrement par les Etats Unis et le Royaume Uni, ces exceptions devraient être traitées de façon très étroite, permettant de facto le libre échange dans l'enseignement supérieur. Ce point de vue tend principalement à défendre des intérêts du secteur de l'éducation anglophone de façon à se tailler une large part dans la couverture du marché global de l'éducation. Il a cependant été considérablement contredit dans plusieurs pays.

Le futur débat qui tend à se développer dans le contexte de l'OMC et d'autres organisations internationales, sera centré sur le dilemme de traiter l'enseignement comme une marchandise ou comme un bien public. Si l'enseignement est considéré comme une marchandise, les règles de libre échange de l'OMC seront également appliquées dans ce domaine. D'autre part, l'approche bien publique préserverait le modèle actuel de l'enseignement dans lequel les universités publiques reçoivent un statut spécial en tant qu'institutions de grande importance dans la culture nationale.

### Assurance qualité

La disponibilité des systèmes de fourniture de l'enseignement en ligne et la facilité d'entrée dans ce marché a ouvert la question de la qualité de l'enseignement. En mettant trop l'accent sur la fourniture en ligne, l'on peut mettre de côté l'importance de la qualité des matériaux didactiques.

Une variété de difficultés éventuelles peut mettre en péril la qualité de l'enseignement. L'une concerne la montée en ligne relativement aisée de nouvelles institutions surtout à but essentiellement lucratif qui n'ont souvent que très peu de capacités didactiques et académiques. Un autre problème de l'assurance qualité est que le simple transfert des supports didactiques classiques (papiers) vers des supports en ligne ne tire pas pleinement parti du potentiel didactique qu'offre ce nouveau médium.

### La reconnaissance des diplômes académiques et transfert de crédits

La reconnaissance des diplômes est devenue particulièrement d'actualité dans l'environnement de l'enseignement en ligne; le défi majeur est la reconnaissance des diplômes au delà du contexte régional, surtout au niveau global. L'UE a commencé à développer un plan de régulation avec le système de transfert de crédit européen (ECTS: European Credit Transfer System). La région Asie-Pacifique est entrain de suivre le modèle européen en introduisant son propre modèle régional pour l'échange d'étudiants, ainsi qu'un système de crédit y relatif.

### La standardisation de l'enseignement en ligne

La première phase du développement de l'enseignement en ligne était caractérisée par un développement rapide et une grande diversité de matériaux, dans le sens des plates formes, des contenus, et du matériel didactique. Cependant, il y a un besoin de développer des normes communes en vue de faciliter l'échange des cours en ligne et introduire une certaine norme de qualité.

Le gros du travail de normalisation est développé aux Etats Unis par des institutions professionnelles et privées. D'autres incluant des initiatives internationales sont à une échelle plus réduite.

### La sécurité de l'enfant en ligne<sup>46</sup>

Les enfants ont toujours été vulnérables à la victimisation. La majorité des problèmes liés à la sureté de l'Internet concernent en premier lieu la jeunesse et surtout les mineurs.

Pourtant, les lignes couramment floues deviennent plus nettes en ce qui concerne la sécurité des enfants. Le contenu répréhensible est clairement indiqué comme étant impropre et inapproprié, et comprend une grande variété de matériaux y compris la pornographie, du contenu véhiculant de la

haine et de la violence, du contenu dangereux pour la santé, des conseils au suicide, des conseils à l'anorexie, etc.

## Les enjeux

### Cyber intimidation

Le harcèlement est un défi particulièrement important lorsque des mineurs sont visés. Les mineurs sont particulièrement vulnérables en utilisant de nombreux outils de communication tels que la messagerie, les *salons de discussion* et les réseaux sociaux. Les enfants peuvent aisément devenir des victimes de la cyber intimidation, le plus souvent par leurs pairs en utilisant les nouvelles technologies de la communication et de l'information, incluant le téléphone portable avec caméras, les systèmes de partage de fichiers et les réseaux sociaux.

### Abus et exploitation sexuels

Les mauvais comportements visant les mineurs peuvent être particulièrement dangereux lorsqu'ils sont commis par des adultes. Le camouflage de l'identité est l'une des approches les plus fréquentes utilisée par les pédophiles sur internet. En prétendant être des pairs, ces 'prédateurs en ligne' collectent des informations sur des jeunes en bas âge; ils réussissent ainsi à gagner la confiance des enfants allant jusqu'à établir un contact physique. Le contact virtuel se transforme ainsi en un contact réel et peut conduire à l'exploitation et aux abus sexuels, à la pédophilie et aux sollicitations des mineurs à des fins sexuelles et même au trafic d'enfants.

### Les jeux violents

Les jeux violents (généralement dans un environnement de réseau, comme par exemple Dungeons) sont en train de rapidement prendre le dessus sur les films dans lesquels la violence est dite 'passive'. L'impact de la violence de ces jeux sur le comportement des jeunes est largement débattu. Les jeux les plus dangereux recourent à des armes sophistiquées (en montrant les caractéristiques réelles de ces armes et ou à d'autres caractéristiques fantaisistes) et au carnage et sont généralement étiquetés comme des 'éliminateurs de stress'. En effet le top 10 des jeux, pour les différentes plateformes et matériels y compris Microsoft Xbox, NintendoDS, Nintendo Wii, PC, Playstation, PSP, sont dominés par des jeux d'action violents.

### Relever des défis

Le défi majeur auquel les éducateurs et les parents font face dans la protection des enfants, lorsqu'ils sont en ligne, est le fait que les 'digital natives' (ceux qui sont nés à l'ère numérique) accèdent plus facilement à

la connaissance en ce qui concerne l'usage des ICT. Ils savent beaucoup, mais ils comprennent moins. Ainsi, la coopération de la communauté des proches parents, éducateurs, et des pairs est d'une importance capitale. Les parents, les décideurs politiques et la communauté mondiale toute entière sont néanmoins en train de prendre conscience des situations ci-dessus mentionnées et de mettre en place des initiatives pour sauvegarder les enfants dans les environnements où l'outil informatique est omniprésent.

Pour faire prendre conscience les divers parties prenantes, la Commission Européenne a mis en action le projet '*insafe*,' un réseau Européen pour la sécurité électronique fournissant plusieurs matériaux de prise de conscience pour les parents et les éducateurs dans plusieurs langues, libres pour téléchargement et la dissémination. La campagne médiatique polonaise sur la cyber intimidation a engendré des clips vidéos et un cours d'apprentissage électronique sur la protection de l'Internet pour les enfants. L'initiative de *NetSafe* en Nouvelle Zélande, fondée en 1998, figure parmi les premières initiatives nationales en matière de sécurité sur l'Internet, elle regroupe les parties prenantes clés y compris les ministères, le secteur privé et les médias.

Parmi les modèles les plus réussis de campagne de sensibilisation et de formation au niveau national, il y a le Cyber Peace Initiative (CPI) de l'Égypte sous les auspices de Suzanne Moubarak (Women's International Peace Movement: Mouvement des femmes pour la Paix internationale). Un groupe de jeunes enthousiastes dénommé '*Net-Aman*', et un groupe de représentants de parents ont été bien formés et entraînés pour piloter des actions dans le futur. Ensemble avec des partenaires y compris le Ministère Égyptien de la Communication et des Nouvelles Technologies et même des partenaires internationaux, comme Child Net International, ils ont atteint des dizaines de milliers de jeunes et de parents à travers le pays au cours des années passées. Cela a conduit à la production de plusieurs kits d'éducation et de prise de conscience pour les enfants, parents et éducateurs qui ont été traduits en Arabe.

Une étape très attendue au delà de la capacité d'apprentissage et de la prise de conscience de la jeunesse, des parents et des éducateurs est la capacité de construire une zone d'internet de confiance par la mise en place d'un groupe multi parties prenantes de décideurs politiques: les autorités gouvernementales, les entités privées, les médias, les universités, Think-tanks, les ONG, etc. Diverses ONG internationales discutent sur d'éventuels modèles de coopération pour l'établissement de tels programmes, parmi lesquels figurent le Conseil de l'Europe, l'UIT, l'initiative CPI et DiploFoundation.

A long terme, des mise à jours du curriculum éducationnel seront également nécessaires, afin d'inclure dans les programmes scolaires les questions d'intérêt concernant la sécurité comme la protection et la sécurité de la vie privée, la protection de la réputation personnelle et de celle d'autrui sur le net, l'éthique, la publication des abus, le transfert des principes moraux et des compétences de la vie réelle au cyber monde etc. De nombreuses initiatives de ce genre existent à travers le monde, telles que *le Cyber Smart!, iKeepSafe, i-Safe, and NetSmartz.*

Des mécanismes légaux et politiques tant nationaux qu'internationaux synchronisés sont un composant indispensable. Un exemple très récent est la Déclaration de Prague pour un Internet de confiance pour les enfants, adopté à la Conférence ministérielle de Prague en Avril 2009. Cette Déclaration constitue une réussite pour l'initiative européenne. Le programme global sur la cyber sécurité (GCA: Global Cyber Security Agenda) de l'UIT présente le 'Child online protection - COP' comme une de ses initiatives intégrales. En outre il y a plusieurs autres forums internationaux où la protection des enfants est une question débattue et bien inscrite sur les agendas y compris le Forum sur la gouvernance de l'Internet avec sa coalition dynamique sur la protection de l'enfant en ligne.

La coopération internationale en matière de la protection de l'enfance a est déjà une expérience réussie en ce qui concerne le secours international d'urgence et les centres d'assistance par téléphone. Quelques unes des initiatives réussies sont:

- La coopération officielle COSPOL *Internet Related Child Abusive Material Project (CIRCAMP)* initiée par le chef de la Task force des commissaires de police européens.
- Le travail des ONG en coopération avec les gouvernements telles que la Fondation pour la surveillance Internet (Internet Watch Foundation), la Perverted Justice Foundation, ICMEC, ECPAT, *Save the Children, Internet Content Related Association, Child exploitation et Online Protection Centre.*
- Les partenariats publics – privés telle que la coopération entre Norway Telecom et la police norvégienne.

## Notes de fin

- <sup>1</sup> La charte de l'APC des droits sur Internet. Disponible sur: <http://www.apc.org/en/node/5677/>
- <sup>2</sup> Internet Rights and Principles Coalition (2010). Disponible sur: <http://internetrightsandprinciples.org/>
- <sup>3</sup> La charte ACP des droits sur l'Internet comprend: accès à internet pour tous; la liberté d'expression et d'association; l'accès à la connaissance; l'apprentissage et la création partagées – logiciel libre et ouvert, et le développement technologique; la vie privée, la surveillance et le cryptage; la gouvernance de l'Internet; la vulgarisation, la protection et la réalisation des droits. Disponible sur: <http://www.apc.org/en/node/5677>
- <sup>4</sup> Global Network Initiative (2010) Disponible sur: <http://www.globalnetworkinitiative.org>
- <sup>5</sup> Convention on Cybercrime. Disponible sur: <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>
- <sup>6</sup> Le Conseil de l'Europe a adopté les principales déclarations pertinentes suivantes sur les droits de l'Homme et l'Internet: La Déclaration sur la liberté de communication sur Internet (28 Mai 2003); et la Déclaration sur les droits humains et la règle de loi dans la société de l'information (13 Mai 2005).
- <sup>7</sup> Freedom House (2009) *Freedom on the Internet: A global assessment of Internet and digital media*. Disponible sur: [http://www.freedomhouse.org/uploads/specialreportsNetFreedom2009/FreedomOn€eNet\\_FullReport.pdf](http://www.freedomhouse.org/uploads/specialreportsNetFreedom2009/FreedomOn€eNet_FullReport.pdf)
- <sup>8</sup> Zick T (1999) Congress, the Internet, and the intractable pornography problem: the Child Online Protection Act of 1998. *Creighton Law Review* **32**:1147, 1153, 1201.
- <sup>9</sup> Pour une discussion sur les jeux d'argent sur Internet, voir: Karadbil JF (2000) Note: Casinos of the next millennium: a look into the proposed ban on internet gambling. *Arizona Journal of International and Comparative Law* **17**:413, 437–38.
- <sup>10</sup> *Internet under surveillance*. Disponible sur: <http://en.rsf.org/spip.php?page=recherche&lang=en&recherche=internet+enemies&image.x=47&image.y=13&image=%3E%3E>
- <sup>11</sup> Zittrain J, Edelman B (2008) *Documentation of Internet filtering worldwide*. Open Net Initiative. Disponible sur: <http://cyber.law.harvard.edu/filtering/>
- <sup>12</sup> Le filtrage officiel en Arabie Saoudite est fait via un system proxy. voir: <http://www.isu.net.sa/saudi-internet/contenet-filttring/.filtrng-mechanism.htm>
- <sup>13</sup> Electronic Frontiers Australia (2006) *Internet censorship laws in Australia*. Disponible sur: <http://www.efa.org.au/Issues/Censor/cens1.html>
- <sup>14</sup> Resnick P, Miller J (1996) PICS: Internet access controls without censorship. *Communications of the ACM* **39**(10): 87–93. Disponible sur: <http://www.w3.org/PICS/iacwcv2.htm>
- <sup>15</sup> Bien que Vint Cerf ait participé au panel, il a contesté le rapport final, rapport dont il dit

- qu'il n'était pas centré sur les défauts et la large implication dans l'installation des barrières en ligne. Guernsey L (2001) *Welcome to the world wide web Passport please*. Disponible sur: [http://www.criminology.fsu.edu/transcrime/articles/Welcom%20to%20the%20World%20Wide%20Web\\_%20Passport,%20Please.htm](http://www.criminology.fsu.edu/transcrime/articles/Welcom%20to%20the%20World%20Wide%20Web_%20Passport,%20Please.htm)
- 16 Akami déclare que cela peut identifier la localisation géographique des gens et peut même aller jusqu'à l'identification de leur codes ZIP. Voici la limite technologique: l'information au sujet des adresses de rue ne peut être obtenue par une adresse IP. *Silicon Valleys Quova Inc., l'un des fournisseur qui pilote cette technologie, dit que cela peut correctement identifier le pays d'origine de l'utilisateur d'ordinateur à 98 pour cent et la ville dans 85 pour cent des cas, mais seulement si c'est une grande ville*. Des études indépendantes ont fixé le taux d'exactitude de ces programmes, qui sont également vendus par des entreprises comme *InfoSplit, Digital Envoy, Netgeo, and Akami, entre 70 à 90 percent*. Cha AE (2002) Rise of internet borders prompts fears of web's future. *Washington Post*, 4 January. Disponible sur: <http://www.google-watch.org/geolocat.html>
- 17 Pour une enquête sur des articles au sujet du cas Google-Chine, voir: <http://searchenginewatch.com/sereport/article.php/2165031>
- 18 Knight W (2002) Google keywords knock Chinese surfers offline. *New Scientist Internet edition*, 13 September. Disponible sur: <http://www.newscientist.com/article/dn2797-google-keywords-knock-chinese-surfers-o.ine.html>
- 19 Knight W (2002) On-off\_ access for Google in China. *New Scientist Internet edition*, 13 septembre. Disponible sur: <http://www.newscientist.com/article/dn2795-ono.-access-forgoogle-in-china.html>
- 20 Zittrain J, Edelman B (2002) *Localised Google search result exclusions: statement of issues and call for data*. Harvard Law School. Disponible sur: <http://cyber.law.harvard.edu/fi ltering/google/>
- 21 EU Information Society (2005) *Safer Internet Programme*. Disponible sur: [http://europa.eu/legislation\\_summaries/information\\_society/124190d\\_en.htm](http://europa.eu/legislation_summaries/information_society/124190d_en.htm)
- 22 Lessig L (1996) The zones of cyberspace. *Stanford Law Review* **48**: 1403, 1405.
- 23 European Internet Service Providers Association (EuroISPA) a adopté le *Human rights guidelines for Internet service providers*. C'est un exemple intéressant pour l'auto-régulation sur des problèmes aussi importants de politique publique globale (les droits de l'Homme). Disponible sur: [http://www.euroispa.org/fi les/human\\_rights\\_guidelines.pdf](http://www.euroispa.org/fi les/human_rights_guidelines.pdf)
- 24 Operation Clambake (2010) *Church of Scientology censors net access for members*. Disponible sur: <http://www.xenu.net/archive/events/censorship>
- 25 Des commentaires pertinents donnés par Katitza Rodriguez.
- 26 Ce rapport explique le problème de la privatisation de la surveillance et de nouveaux défis liés à la protection de la vie privée: Stanley J (2004) *The surveillance-industrial complex: How the American government is conscripting businesses and individuals in the construction of a surveillance society*. ACLU: New York, NY, USA. Disponible sur: [http://www.aclu.org/FilesPDFs/surveillance\\_report.pdf](http://www.aclu.org/FilesPDFs/surveillance_report.pdf)
- 27 USA Patriot Act (2001) Disponible sur: <http://www.epic.org/privacy/terrorism/hr3162.html>

- <sup>28</sup> For a discussion of customer trust in business privacy protection see: Whiting R (2002) Wary customers don't trust business to protect privacy. *Information Week*, 19 août. Disponible sur: <http://www.informationweek.com/shared/printableArticle.jhtml?articleID=6503045>
- <sup>29</sup> Overview of the Gramm-Leach-Bliley Act. Disponible sur: <http://www.frbsf.org/publications/banking/gramm/grammpg1.html>
- <sup>30</sup> Gramm-Leach-Bliley Act: Privacy of Consumer Financial Information. Disponible sur: <http://www.ftc.gov/privacy/glbact/glboutline.htm>
- <sup>31</sup> Children's Online Privacy Protection Act of 1998. Disponible sur: <http://www.ftc.gov/ogc/coppa1.shtm>
- <sup>32</sup> Health Insurance Portability and Accountability Act of 1996, *Public Law* 104–191, §264; Department of Health and Human Services, Standards for Privacy of Individually Identifiable Health Information; Proposed Rule, 64 Fed. Reg. 59917. Disponible sur: [http://www.epic.org/privacy/medical/HHS\\_medical\\_privacy\\_regs.html](http://www.epic.org/privacy/medical/HHS_medical_privacy_regs.html)
- <sup>33</sup> Connolly C (2008) *The US Safe Harbor – Fact or Fiction?* Galexia: Pyrmont, Australia. Disponible sur: [http://www.galexia.com/public/research/articles/research\\_articles-pa08.Html](http://www.galexia.com/public/research/articles/research_articles-pa08.Html)
- <sup>34</sup> Pour plus d'information sur le multilinguisme sur l'Internet, voir: Al-Shatti Q, Aquirre R, Cretu V (2007) *Multilingualism – the communication bridge*. DiploFoundation Internet Governance Research Project. Disponible sur: <http://textus.diplomacy.edu/thina/TxFsetW.asp?tURL=http://textus.diplomacy.edu/thina/txgetdoc.asp?IDconv=3241>
- <sup>35</sup> Pour plus d'information sur les IDN, voire: Marson C (2010) Internationalization in Names and Other Identifiers. *IEFT Journal* 5(3). Disponible sur: <http://www.isoc.org/tools/blogs/ietjournal/?p=1521> (scroll down).
- <sup>36</sup> Wikipedia (2010) *English in computing*. Disponible sur: [http://en.wikipedia.org/wiki/English\\_on\\_the\\_Internet#Internet\\_content](http://en.wikipedia.org/wiki/English_on_the_Internet#Internet_content)
- <sup>37</sup> Creative Commons (CC) est une organisation non gouvernementale ayant son siège à San Francisco, Californie, aux Etats Unis, dont le but est l'expansion des travaux créatifs et leur disponibilité afin que d'autres puissent faire d'autres travaux de manière légale et les partager. L'organisation a produit beaucoup de matériaux protégés par un droit d'auteur dont le type de licence est du genre 'Creative Commons' accessibles gratuitement au public. Ces licences selon leur choix, restreignent seulement quelques droits (ou aucun) des travaux. Le droit d'auteur, donne droit aux créateurs de communiquer quels droits ils se réservent, et quels droits ils retirent aux utilisateurs ou à d'autres créateurs. (Source: Wikipedia).
- <sup>38</sup> Arata S, Psaila S (2006) *Protection of Public Interest on the Internet*. DiploFoundation Internet Governance Research Project. Disponible sur: <http://www.diplomacy.edu/ig/Research/display.asp?Topic=Research%20emes%20II#Protection>
- <sup>39</sup> Des commentaires pertinents avaient été faits par Jorge Plano.
- <sup>40</sup> hrea.org (2010) *Human rights of persons with disabilities*. Disponible sur: [http://www.hrea.org/index.php?base\\_id=152](http://www.hrea.org/index.php?base_id=152)
- <sup>41</sup> UN Enable (2010) *Rights and dignity of persons with disabilities*. Disponible sur: <http://www.un.org/disabilities/>

- <sup>42</sup> IGF (2010) *Dynamic Coalition on Accessibility and Disability*. Disponible sur: <http://www.intgovforum.org/cms/dynamic-coalitions/80-accessibility-and-disability>
- <sup>43</sup> ISOC (2010) *Internet Society Disability and Special Needs Chapter*. Disponible sur: <http://www.isocdisab.org>
- <sup>44</sup> W3C (1999) *Web Content Accessibility Guidelines 1.0*. Disponible sur: <http://www.w3.org/TR/WCAG10/>
- <sup>45</sup> Burks M, Waddell C (2001) *Universal design for the Internet*. ISOC Member Briefing No. 2. Disponible sur: <http://www.isoc.org/brie.ngs/002/isocbrie.ng02.txt>
- <sup>46</sup> Ce texte a été préparé par Vladimir Radunovic pour le cours avancé sur la Cyber-sécurité et la sûreté de l'Internet (Internet Governance Capacity Building Program – DiploFoundation).



## Section 7

---

# Les parties prenantes de la Gouvernance de l'Internet





# Les parties prenantes de la Gouvernance de l'Internet

L'une des caractéristiques particulières de la Gouvernance l'Internet a été la participation de multi parties prenantes, une facette naturelle des discussions de la Gouvernance de l'Internet, étant donné que des acteurs non étatiques ont joué un rôle essentiel dans le développement et la gestion de l'Internet. La société civile, particulièrement les institutions académiques, a été un acteur très important dans le domaine de l'Internet depuis ses débuts. Celle-ci a établi le noyau du protocole de l'Internet; (Protocole de Control de Transmission /Protocole de l'Internet TCP/IP) et les services (e-mail). Le secteur privé, quant à lui, met en place les infrastructures technologiques, y compris les ordinateurs, les réseaux, et logiciels. Les gouvernements sont relativement de nouveaux venus dans le domaine de la Gouvernance de l'Internet<sup>1</sup>.



La grande différence entre les pourparlers de la Gouvernance de l'Internet et les autres pourparlers globaux, tels que les pourparlers environnementaux, réside dans le fait que pendant que dans d'autres pourparlers, les régimes intergouvernementaux s'ouvraient graduellement aux acteurs non gouvernementaux, dans les négociations de la gouvernance de l'Internet, les gouvernements devaient intégrer un régime non gouvernemental existant, conçu au tour de l'IETF (le Groupe de Travail de l'Ingénierie de l'Internet), l'ISOC (l'Internet Society) et l'ICANN (la Corporation pour l'Assignation

## La Gouvernance de l'Internet – approche géométrique à plusieurs variables

La Gouvernance de l'Internet exige l'implication d'une variété de parties prenantes qui diffèrent sur plusieurs aspects, incluant le volet de la légitimité internationale, les intérêts dans certains aspects de la Gouvernance de l'Internet, la disponibilité de l'expertise requise. Une telle diversité pourrait être placée sous le chapeau d'une unique structure de Gouvernance de l'Internet utilisant une approche géométrique à plusieurs variables, qui reflèterait les intérêts des parties prenantes, leurs priorités et leur capacité à appréhender les questions de la Gouvernance de l'Internet, est incluse dans l'Article 49 de la déclaration du SMSI, qui spécifie les rôles suivants des principales parties prenantes:

- L'Etat – autorité chargée de l'élaboration de politiques publiques relatives à l'Internet (y compris les aspects internationaux).
- Le Secteur Privé – développement de l'Internet, que ce soit dans les aspects techniques que dans les aspects économiques et techniques.
- La Société Civile – rôle important dans les questions relatives à l'Internet, spécialement au niveau des communautés.
- Organisations Intergouvernementales - la coordination sur les aspects relatifs aux politiques publiques de l'Internet.
- Organisations Internationales – développement des standards techniques de l'Internet et des politiques y relatives.<sup>4</sup>

des Noms et Numéros Internet). Une fois la Gouvernance de l'Internet devenue un enjeu mondial, il y avait nécessité de faire converger ces deux régimes (non gouvernementaux et diplomatiques traditionnels) à travers le développement d'un cadre politique multi parties prenantes.

La première expérience réussie dans cette direction fut le Groupe de Travail sur la Gouvernance de l'Internet (GTGI) pendant le processus du Sommet Mondial sur la Société de l'Information (SMSI) (2002 – 2005). Le GTGI était plus qu'un groupe d'experts conseils, mais en même temps moins qu'un organe chargé de la prise de décision<sup>3</sup>. Il n'a pas produit de documents officiels des Nations Unies, mais il a influencé substantiellement les négociations du SMSI sur la Gouvernance de l'Internet. Le GTGI était un compromis dans lequel les gouvernements pro-ICANN laissent émerger officiellement les problèmes de la Gouvernance de l'Internet de l'agenda diplomatique multilatéral et dans lequel d'autres gouvernements, principalement ceux des pays en développement, acceptaient la participation des acteurs non étatiques. De ce compromis, il en a résulté la réussite du GTGI.

Comme processus issu du SMSI, la Gouvernance de l'Internet demeure sur l'agenda mondial à travers le Forum sur la Gouvernance de l'Internet (FGI).

Le FGI suit la structure de participation de GTGI. Le GTGI et l'IGF demeurent des exemples utiles pour le développement futur de processus multi parties prenantes au niveau international.

## Les gouvernements

Les huit années passées – depuis l'introduction en 2003 de la Gouvernance de l'Internet dans les agendas politiques – ont été un processus d'apprentissage pour beaucoup de Gouvernements. Même pour des grands pays riches, la prise en main des problèmes de la gouvernance de l'Internet a été un grand défi, notamment en ce qui concerne la gestion de la nature multidisciplinaire de la gouvernance de l'Internet (les aspects socioéconomiques, et technologiques), et a impliqué une grande variété d'acteurs. Plusieurs gouvernements devaient former leurs représentants officiels et cadres, développer des stratégies, et participer activement à divers forums de la gouvernance de l'Internet; tout en continuant à vouloir encore comprendre le nouveau phénomène de la gouvernance de l'Internet.

### Coordination nationale

En 2003, au début du processus du SMSI, beaucoup de pays ont abordé les problèmes de la gouvernance de l'Internet à travers les ministères 'techniques'. Se sont très souvent des pays qui avaient des relations avec l'Union Internationale des Télécommunications (UIT) dans leurs responsabilités. Graduellement, comme ils ont reconnu que la gouvernance de l'Internet était plus que des 'fils et des câbles', les gouvernements ont commencé à impliquer les représentants officiels d'autres ministères 'moins techniques', tels que ceux de la culture, des médias, et de la justice.

Le défi majeur de plusieurs gouvernements a été de développer une stratégie pour recueillir et coordonner efficacement le soutien des acteurs non étatiques, tels que les universités, les compagnies privées, et les organisations non gouvernementales (NGO) qui ont l'expertise nécessaire pour traiter des problèmes de la gouvernance de l'Internet. Pendant le processus du SMSI, la plus part des grands et moyens Etats ont pris soin de développer une capacité institutionnelle suffisante pour suivre les pourparlers sur la gouvernance mondiale de l'Internet. L'un d'eux, le Brésil, a développé une structure

## La géo-stratégie du câble et la (l'in) cohérence politique

L'Entente anglo-française fut établie en 1904. Cependant, en établissant une coopération étroite avec l'Allemagne, le Ministère français de la Télégraphie n'a pas suivi la politique générale du pays. Le Ministère a voulu réduire la domination anglaise dans la 'Géo - stratégie globale' du câble tout en déployant de nouvelles lignes télégraphiques en coopération avec l'Allemagne. L'historien Français Charles Lesage fit le commentaire suivant sur cette incohérence politique:

*La mésentente prolongée entre les principes généraux au niveau de la diplomatie française et les procédures de la politique générale de la télégraphie aurait été causée, selon mes pensées par le fait que dans ce pays, chaque ministère dispose d'une politique étrangère propre: le Ministère des Affaires Etrangères en a une, le Ministère des Finances en a une autre.... L'administration des Postes et de la Télégraphie a aussi de temps en temps une politique étrangère propre, comme cela a eu lieu dans les années passées, sans être totalement hostile à l'Angleterre, elle a fait preuve d'un penchant pour l'Allemagne.<sup>6</sup>*

nationale innovatrice pour suivre le débat de la gouvernance de l'Internet, impliquant le ministère de télécommunications, les services diplomatiques, le secteur privé, la société civile, et les institutions académiques.<sup>5</sup>

### Cohérence politique

La nature multidisciplinaire de la gouvernance de l'Internet et la grande diversité des acteurs des forums politiques est un défi pour la réalisation de la cohérence politique. Ceci exige de plusieurs gouvernements d'avoir une certaine flexibilité au niveau de la coordination politique, y compris la communication horizontale parmi les différents ministères, le secteur privé, et d'autres acteurs. Une structure gouvernementale traditionnelle, basée sur une forte hiérarchisation, pourrait être un obstacle au développement d'une telle flexibilité dans la coordination.

En dehors du défi de gestion, la réalisation de la cohérence politique est souvent limitée par l'existence d'intérêts politiques divergents. Ceci est surtout réel dans des pays où l'économie de l'Internet est bien-développée et diversifiée. Par exemple, la neutralité du réseau est l'une des questions dans laquelle le gouvernement des Etats-Unis est impliqué par un acte d'équilibrage délicat entre le secteur Internet de l'économie (Google, Yahoo !) qui en sont des grands supporters et le secteur des télécommunications/divertissement (Verizon et AT&T, le lobby Hollywood), qui le voit comme un obstacle pour le développement d'un nouveau modèle d'affaire basé sur un Internet très rapide pour la délivrance de contenus multimédias.

La convergence technologique entre plusieurs médias donnera un autre élan pour réaliser la cohérence politique. Les domaines ayant traditionnellement des politiques distinctes telles que les télécommunications et la radiodiffusion, devront émerger afin de refléter la convergence technologique.

### Importance des missions diplomatiques permanentes basées à Genève

D'après plusieurs gouvernements, leurs missions diplomatiques permanentes à Genève furent importantes, sinon vitales, en tant qu'acteurs dans les processus du SMSI et de la gouvernance de l'Internet. Plusieurs activités eurent lieu à Genève et l'IUT a joué un rôle primordial dans ce processus. Le premier SMSI en 2003 a eu lieu à Genève, mais surtout, toutes les réunions préparatoires étaient tenues à Genève, ce qui gardait les missions permanentes basées à Genève directement impliquées. Présentement, le secrétariat du FGI est basé à Genève et toutes les réunions préparatoires sont tenues dans cette ville.

Pour les grandes nations et pays développés, les missions permanentes faisaient partie du réseau général des institutions et des individus qui s'occupent du SMSI et des processus de la gouvernance de l'Internet. Pour les petits pays et pays en développement, les missions permanentes étaient en première ligne, et, dans quelques cas, les acteurs uniques dans ce processus. Le *portfolio* du SMSI fut ajouté à l'agenda surchargée des missions diplomatiques des pays en développement qui sont souvent de petites tailles. Dans beaucoup de cas, le même diplomate devait entreprendre des tâches associées avec le SMSI en parallèle avec d'autres problèmes, tels que les droits de l'homme, la santé, le commerce, et le travail.

### Diplomatisation du processus de la gouvernance de l'Internet

Le SMSI a placé l'Internet dans l'agenda diplomatique mondial. Bien avant le SMSI, l'Internet a été discuté premièrement dans des cercles non gouvernementaux ou au niveau national. La mise sur la scène diplomatique des enjeux de l'Internet a suscité différentes réactions. Dans la correspondance technologique pour *The Economist*, Kenneth Neil Cukier a insisté sur l'aspect négatif de la diplomatisation du débat sur gouvernance de l'Internet:

*... en élevant la question à un sommet formel des Nations unies, cela lui conféra une grande importance au sein des gouvernements. Comme résultat, les problèmes concernant la Société de l'Information, qui étaient traités par les parties des gouvernements qui jadis étaient par des départements peu politiques et moins visibles des gouvernements – comme politique sur la*

*science et la technologie ou comme une question relative aux media et affaires culturelles – étaient transférées aux ministères des affaires étrangères et aux diplomates de longue carrière, qui maîtrisent la politique mais maîtrisant moins les questions technologiques et l'exigence inhérente à Internet pour la coopération et l'interdépendance.<sup>7</sup>*

Le processus de la Diplomatisation avait certains aspects positifs pour les débats du SMSI, par exemple, les diplomates ont produit des contributions non partisans aux longs débats sur les problèmes relatifs à l'ICANN: nom de domaines, numéros de l'Internet, et les serveurs racines. Les contributions des diplomates étaient particulièrement remarquables dans les débats du GTGI. Le leadership diplomatique du GTGI (présidé par Nitin Desai et dont le Secrétaire Exécutif était Markus Kummer) a créé une atmosphère inclusive là où les différences parmi les représentants, y compris ceux de la communauté technique, n'ont pas bloqué le processus. Le résultat du processus du GTGI fut le rapport final qui a reflété les différentes opinions exprimées, mais a également fourni une solution relative au processus pour les futures discussions en établissant le FGI.

### La position du Gouvernement des Etats-Unis

L'Internet fut développé comme une partie du projet sponsorisé par le gouvernement des Etats-Unis. De l'origine de l'Internet jusqu'à ce jour, le gouvernement des Etats Unis a été impliqué dans la gouvernance de l'Internet à travers des départements variés et des agences; initialement, le Département de la Défense, plus tard, la Fondation Nationale pour la Science, et plus récemment le Département du Commerce. La 'Federal Communication Commission' (Commission Fédérale de la Communication) a aussi joué un rôle important dans la création du cadre de régulation pour le développement de l'Internet.

Une stratégie constamment gardée par le gouvernement des Etats-Unis a été une approche non interventionniste, souvent décrite comme 'observateur éloigné': il établit le cadre de travail, mais laisse la gouvernance de l'Internet à ceux qui y travaillent directement, surtout à la communauté de l'Internet. Cependant, le gouvernement des Etats-Unis est intervenu plus directement à certaines occasions, comme au milieu des années 90 lorsque le projet 'CORE' avait voulu faire déménager le serveur racine et la gestion de l'infrastructure principal de l'Internet des Etats-Unis vers Genève. Ce processus a été stoppé par une fameuse note diplomatique – ayant maqué l'histoire de l'Internet – envoyée par la Secrétaire d'Etat des Etats Unis, Madeleine Albright au Secrétaire Général de l'UIT.<sup>8</sup> Parallèlement à la mise en arrêt cette initiative,

le gouvernement des Etats-Unis a initié des consultations qui aboutirent à l'établissement de l'ICANN.

Depuis la création d'ICANN, le gouvernement des Etats-Unis a indiqué son intention de se retirer de la supervision de l'ICANN une fois que sa robustesse institutionnelle et fonctionnelle serait bien accomplie. Ce processus de retrait était indiqué au début d'octobre 2009 avec la signature de l' 'Affirmation d' Engagements' (Affirmation of Engagement) entre le Département de Commerce des Etats-Unis et de l'ICANN. Selon ce document, l'ICANN deviendra une organisation indépendante. Un autre élément de la relation spéciale entre le Département de Commerce des Etats-Unis et l'ICANN – l'IANA (Autorité des Numéros Internet Assignés: Internet Assigned Numbers Authority) – sera révisé en 2011.

Sur la scène mondiale, pendant le processus du SMSI, les Etats Unis se sont opposés à la probabilité de relèver des fonctions de l'ICANN par un corps intergouvernemental. Cependant, dans le processus du SMSI, le gouvernement des Etats-Unis a fait un premier pas à travers l'internalisation du rôle d'ICANN par la reconnaissance des droits des gouvernements nationaux sur leurs noms de domaines respectifs et a accepté la continuation des discussions internationales à travers l'établissement de la FGI.

### La position des autres gouvernements

Un spectre politique de la gouvernance de l'Internet commençait à prendre forme récemment car les gouvernements commençaient à développer leurs positions nationales. Du point de vue du spectre politique, il y avait un point de vue selon lequel une organisation intergouvernementale, telle que l'UIT devrait gouverner l'Internet. Ceci était la position initiale de beaucoup de pays en développement. Les plus grands supporters pour un rôle important de l'UIT étaient la Chine, l'Iran, et la Russie. Quelques pays en développement ont soutenu la création d'une nouvelle organisation internationale pour remplacer l'UIT, y compris l'établissement d'une nouvelle organisation basée sur un traité telle qu'une 'Organisation Internationale de l'Internet'. D'autres pays ont soutenu qu'un nouveau type d'organisation multi parties prenantes devrait gouverner l'Internet.

Au centre du spectre politique, certains gouvernements soutenaient que l'ICANN devrait garder ses fonctions techniques pendant qu'un corps international public devrait avoir la fonction de surveillance politique. Ceci est la position qui a été graduellement prise par l'Union Européenne.

De l'autre côté du spectre politique, les Etats-Unis ont soutenu que rien dans le régime basé sur l'ICANN ne devrait changer. Le Canada, l'Australie, et la Nouvelle Zélande ont développé des points de vue similaires, en plus du soutien pour une grande internalisation de l'ICANN. Ces pays, de concert avec l'Union Européenne, la Suisse et quelques pays en développement ont joué un rôle important dans l'établissement d'un compromis sur la gouvernance de l'Internet pendant le processus du SMSI.

### La position des petits Etats

La complexité des problèmes et la dynamique des activités accomplies a rendu presque impossible à beaucoup de petit pays et, particulièrement, à beaucoup de petits pays en développement de suivre les discussions, mis à part le pouvoir d'avoir un quelconque effet substantif. Comme résultat, quelques petits Etats ont soutenu la mise en place d'une structure unique, centrale en charge de toutes les questions de gouvernance de l'Internet.<sup>9</sup> Le grand volume de l'agenda et la capacité politique limitée des pays en développement et celle de leurs missions diplomatiques demeurent l'un des obstacles principaux à leur pleine participation dans le processus. Le besoin de la construction de capacité, y compris politique, dans le domaine de la gouvernance de l'Internet a été reconnue comme l'une des priorités dans l'agenda du SMSI de Tunis pour la Société de l'Information.

### Le secteur privé<sup>10</sup>

Lorsque l'ICANN fut établie en 1998, l'un des soucis pertinents du secteur privé était la protection de marques déposées. Beaucoup de compagnies ont fait face au 'cybersquatting'; le mauvais usage de leurs marques commerciales par les individus qui étaient plus rapides dans leur enregistrement. Dans le processus de la création de l'ICANN, le monde des affaires a clairement priorisé la protection des marques commerciales et, en commun accord, cette question fut immédiatement résolue lors de la création de l'ICANN.<sup>11</sup>

Aujourd'hui, avec le développement de l'Internet, l'intérêt du monde des affaires dans la gouvernance de l'Internet s'est étendu et diversifié, avec les principaux groupes des compagnies privées suivants: les compagnies des noms de domaine, fournisseurs des services Internet (FSI), les compagnies de télécommunications, les développeurs des logiciels, et les compagnies de contenu Internet.

## La Chambre Internationale de Commerce (ICC, en anglais)

**La Chambre Internationale de Commerce (ICC, en anglais)**, bien connue en tant qu'association représentative du secteur privé quel que soit les secteurs et au-delà des frontières géographiques, a pris position comme étant le principal représentant du secteur privé dans le processus de la Gouvernance de l'Internet sur le plan global. L'ICC a été activement impliquée dès les négociations préliminaires du GTGI et du SMSI, et continue à être un contributeur actif dans le processus en cours du FGI.

### Compagnies des noms de domaine

Les compagnies des noms de domaine comprennent les bureaux d'enregistrement et les registres qui vendent les noms de domaine Internet (ex: .com, .edu). Les principaux acteurs dans ce secteur sont VeriSign et Affiliis. Leurs affaires sont directement influencées par les décisions politiques de l'ICANN dans des secteurs tels que l'introduction des nouveaux domaines et la résolution des différends. Elles sont ainsi parmi les plus importantes parties prenantes dans le processus de mise en place des politiques de l'ICANN. Elles ont également été impliquées dans le processus de la politique globale de la gouvernance de l'Internet (SMSI, GTGI, FGI) avec l'objectif principal de réduire le risque potentiel que le rôle de l'ICANN puisse être joué par d'autres acteurs, surtout les gouvernements nationaux et les organisations internationales.

### Les fournisseurs de service Internet

Les FSI sont des compagnies ou des organisations qui fonctionnent comme portails à travers lesquels l'Internet est accessible. Puisque les FSI sont des intermédiaires clés permettant aux utilisateurs d'être en ligne, ceci les rend particulièrement importants pour la gouvernance de l'Internet.

Leur implication se remarque principalement au niveau national en traitant avec le gouvernement et les autorités légales. Au niveau mondial, quelques FSI, particulièrement ceux des Etats-Unis et d'Europe, ont été individuellement actifs dans les processus SMSI/GTGI/FGI, et même plus à travers la CIC et son initiative BASIS (Business Action to Support the Information Society), et à travers des organisations nationales et régionales du secteur privé telles que l'ETNO (European Telecommunication Network Operators Association - Association Européenne des Opérateurs des Réseaux de Télécommunications), l'ITAA (Information Technology Association of America - Association Américaine des Technologies de l'Information), et d'autres.

### Compagnies de télécommunication

Ces compagnies facilitent le trafic de l'Internet et font fonctionner les infrastructures Internet. Les acteurs principaux sont les compagnies telles que Verizon et AT&T.

Traditionnellement, les sociétés de télécommunication ont participé à la politique internationale de la télécommunication à travers l'UIT. Elles ont été fortement impliquées dans les activités de l'ICANN et du FGI. Leur intérêt primordial dans la gouvernance de l'Internet est d'assurer un environnement mondial propice aux affaires pour le développement de l'infrastructure de télécommunication de l'Internet.

### Compagnies de logiciel

Les sociétés telles que Microsoft, Adobe, et Oracle sont principalement impliquées dans les activités des différents corps de standardisation (W3C – Word Wide Web Consortium, l'IETF). Dès les premiers jours du processus du SMSI, leur problème fondamental était de trouver la possibilité d'engager une discussion sur les droits de propriété intellectuelle (DPI) sur l'Internet. Après qu'il eut été clair que le SMSI ne devait pas s'impliquer dans le domaine du DPI, l'intérêt de ces sociétés dans la participation au processus du SMSI a diminué. Cette tendance continue depuis le sommet.

### Les compagnies du contenu Internet

Celles-ci comprennent les principaux noms de marque Internet tels que Google, Facebook, et Twitter. Ce groupe de compagnies a pris de l'importance avec le développement des applications Web 2.0. Leurs priorités d'affaire sont étroitement liées aux problèmes variés de la gouvernance de l'Internet tels que la propriété intellectuelle, le respect de la vie privée et la cyber sécurité. Leur présence est très remarquable dans le processus de la gouvernance mondiale de l'Internet.

## La société civile

La société civile a été très active dans la promotion de l'approche multi parties prenantes à la gouvernance de l'Internet.

La critique habituelle de la participation de la société civile aux précédents forums multilatéraux avait été un manque de coordination approprié et la présence de beaucoup de voix souvent discordantes. Cependant, dans le processus du SMSI, la représentation de la société civile a réussi dépasser cette complexité interne et la diversité à travers quelques formes organisationnelles, y compris le Bureau de la Société Civile, la Plénière de la Société Civile, et les Groupes thématiques. Etant confronté aux possibilités limitées pour influencer le processus formel, les groupes de la société civile ont développé une approche à deux tendances. Ils continuaient leur présence dans le processus formel en utilisant les opportunités disponibles pour participer et à faire pression sur les gouvernements. En parallèle, ils ont préparé la Déclaration de la Société Civile comme une vision alternative à la déclaration principale adoptée au SMSI de Genève.

A cause de la nature multi parties prenantes, la société civile a atteint un haut niveau d'implication. Les groupes de la société civile ont proposé huit candidats au GTGI; tous les huit ont été subséquemment nommés par le Secrétariat Général des Nations unies. Durant la phase de Tunis (la seconde phase de SMSI, après Genève), les visions politiques principales des organisations de la société civile ont été transposées au GTGI, où elles ont influencé beaucoup des conclusions aussi bien que la décision d'établir le FGI comme espace multiples parties prenantes pour des discussions sur les problèmes de la gouvernance de l'Internet. La société civile a continué d'être activement impliquée dans les activités du FGI.

### Les ONG et le SMSI

La participation des ONG dans le SMSI a été relativement faible. Sur environ 3000 ONG qui disposent d'un statut consultatif au sein de l'ECOSOC des Nations Unies (Conseil Economique et Social), seules 300 ont participé au SMSI.

## Organisations internationales

L'UIT était l'organisation internationale centrale dans le processus du SMSI. Il a hébergé le secrétariat du SMSI et a produit des contributions sur les principaux problèmes pertinents. L'implication de l'UIT dans le processus du SMSI faisait partie de sa tentative de définir et de consolider sa nouvelle position face aux changements rapides intervenant dans le secteur des télécommunications de plus en plus façonné par l'Internet. Le rôle de l'UIT a été défié de plusieurs façons. Elle a perdu son traditionnel monopole à cause de la libéralisation du marché mondial des télécommunications par l'OMC. La dernière tendance étant de retirer le trafic téléphonique de la communication traditionnelle vers l'Internet (à travers le Protocole sur la voix sur IP- VoIP) ce qui a encore réduit son influence dans le domaine la régulation des télécommunications globales.

La possibilité que l'UIT ait émergé du processus du SMSI comme une 'organisation Internationale de l'Internet' *de facto* a causé des problèmes aux Etats-Unis et dans quelques pays développés; par contre cette option a reçu le soutien de quelques pays en développement. Durant le SMSI, ceci a créé des tensions politiques remarquables. Cela était particulièrement clair dans le domaine de la gouvernance de l'Internet, où la tension entre l'ICANN et l'UIT a existé depuis la création de l'ICANN en 1998. Le SMSI n'avait pas pu résoudre la tension. Avec la tendance croissante de la convergence des diverses technologies de communication, il est très probable que la question du rôle plus actif de l'UIT dans la gouvernance de l'Internet puisse resurgir dans les discussions politiques.

Un autre problème concernait l'ancrage de l'agenda multidisciplinaire du SMSI au sein de la famille des agences spécialisées des Nations unies. Les aspects non techniques des communications et de la technologie de l'Internet, tels que les aspects sociaux, économiques, et culturels, font parties du mandat des autres Organisations des Nations unies. L'acteur le plus dominant dans ce contexte est l'Organisation des Nations Unies pour l'Education, la Science, et la Culture (UNESCO) qui s'occupe des questions telles que le multilinguisme, la diversité culturelle, la société des savoirs, et le partage d'information. L'équilibre entre l'UIT et les autres organisations des Nations unies était soigneusement gérée. Les processus de suivi du SMSI reflètent également cet équilibre, avec les principaux acteurs parmi lesquels l'UIT, l'UNESCO, et le Programme des Nations Unies pour le Développement (PNUD).

## Autres participants

En plus des parties prenantes du SMSI, d'autres acteurs – la communauté Internet et l'ICANN – qui n'étaient pas officiellement reconnues comme parties prenantes ont participé au processus surtout à travers la société civile et le secteur des affaires.

## La communauté de l'Internet

La communauté de l'Internet comprend les institutions et les individus qui ont développé et fait la promotion de l'Internet depuis son commencement. Historiquement, les membres de la communauté de l'Internet étaient liés aux universités des Etats Unis, où ils ont travaillé, en premier lieu pour développer les normes techniques et établir les fonctionnalités de base de l'Internet. La communauté Internet a également créé l'esprit initial de l'Internet, basé sur les principes de partage de ressources, de l'ouverture de l'accès, et de l'opposition à l'implication de gouvernement dans la régulation de l'Internet. Depuis le début, ses membres ont protégé le concept initial de l'Internet contre la commercialisation abusive et de l'influence extensive des gouvernements.

Dans le concept des relations internationales, la communauté de l'Internet est une communauté épistémique.<sup>12</sup> La première communauté Internet était coordonnée par quelques règles, essentiellement tacites et une seule procédure formelle – Appel à commentaire (Request for Comments - RFC). Toutes les normes principales et de base de l'Internet sont décrites à travers les (RFC). Cependant, même sans régulation stricte ni structurelle formelle, les premières communautés de l'Internet étaient gouvernées par une culture commune et une pression réciproque. La plupart des participants dans ce processus ont partagé des valeurs communes, des systèmes de jugement et des attitudes.

### Terminologie

D'autres termes sont utilisés à la place de 'communauté de l'Internet' tels que 'développeurs de l'Internet', 'fondateurs de l'Internet', 'pères de l'Internet', et 'les technologistes'. Nous utilisons 'communauté de l'Internet' parce que cette communauté est basée sur des valeurs partagées par tous ses membres. Ce kit de valeurs partagées est l'une des caractéristiques distinctives de cette communauté.

La première forme de gestion de l'Internet par la communauté de l'Internet a été défiée au milieu des années 90 après que l'Internet soit devenue une infrastructure centrale de la vie sociale et économique au niveau mondial. Le développement fulgurant de l'Internet a fait émerger un groupe de nouvelles parties prenantes, tels que le secteur privé venu avec une culture professionnelle et une compréhension différente de l'Internet et sa gouvernance, ce qui a conduit à de grandes tensions. Par exemple, durant les années 90, les communautés de l'Internet et 'Network Solutions',<sup>13</sup> étaient impliquées dans ce qui fut appelé 'la guerre du DNS'. Un conflit pour le contrôle du serveur racine et du Système de Noms de Domaine.

Aujourd'hui, la communauté Internet est représentée à travers l'ISOC et l'IETF. ISOC a joué un rôle vital dans la normalisation de l'Internet et dans la promotion des valeurs principales de l'Internet, telles que l'ouverture. Il est aussi activement impliqué dans le renforcement des capacités et dans l'assistance aux pays en développement, surtout en Afrique, pour développer l'infrastructure Internet de base.

La communauté de l'Internet a été un acteur important dans le processus de l'établissement et du fonctionnement de l'ICANN. L'un des 'pères de l'Internet' Vint Cerf, était le Président du Conseil de l'ICANN de 2000 à 2007. Les membres de la communauté de l'Internet ont tenu des positions importantes dans des divers organes de prises de décision de l'ICANN.

Une autre critique se focalise sur le fait qu'avec 2 milliards d'utilisateurs, l'Internet a largement dépassé le cadre de base de l'ICANN se focalisant sur la communauté de l'Internet. Suivant cet argument, étant donné que la ligne de démarcation entre les citoyens et les utilisateurs de l'Internet s'est amenuisée, cela nécessite une plus grande implication des gouvernements et d'autres structures plus représentatives des citoyens, au-delà de celles représentant seulement les utilisateurs de l'Internet, fréquemment décrits comme la 'communauté de l'Internet'. Ceux qui plaident pour une grande implication du gouvernement dans la gouvernance de l'Internet utilisaient cette approche - représenter les citoyens plutôt que les utilisateurs et les communautés. La communauté de l'Internet justifie souvent sa position spéciale dans la gouvernance de l'Internet par son expertise technique. Elle plaide le fait que l'ICANN est une organisation spécifiquement technique; par conséquent, se sont les techniciens utilisant leurs connaissances techniques qui devraient la faire fonctionner. Avec la grande difficulté de maintenir l'ICANN en tant qu'organisation exclusivement technique, cette justification du rôle spécial de la communauté de l'Internet a rencontré des défis fréquents. Il est vraisemblable que les membres de la communauté

de l'Internet vont graduellement intégrer les principaux groupes de parties prenantes, surtout la société civile et le secteur privé, mais aussi les gouvernements. Cependant, si la probabilité de la disparition de la communauté Internet en tant que groupe distinct de partie prenante est très probable; il sera très important de préserver les valeurs qu'elle a défendues: ouverture, échange de connaissances, et la protection des intérêts des utilisateurs de l'Internet.

## **L'ICANN (Internet Corporation for Assigned Names and Numbers)**

L'ICANN est la principale institution de la gouvernance de l'Internet. Sa responsabilité est de gérer l'infrastructure principale de l'Internet, qui comprend les adresses du protocole Internet (IP), noms de domaine et les serveurs racines. Le regain d'intérêt pour le rôle de l'ICANN s'est développé en parallèle avec la croissance rapide de l'Internet au début des années 2000 et l'ICANN est venue à l'attention des cercles décisionnels mondiaux durant le processus SMSI (2002-2005).

Alors que l'ICANN est le principal acteur dans le domaine de la gouvernance de l'Internet, il ne gouverne pas tous les aspects de l'Internet. Il est parfois décrit par erreur comme le 'gouvernement Internet'. L'ICANN gère l'infrastructure Internet, mais il n'a pas l'autorité sur d'autres aspects de la gouvernance de l'Internet, tels que le cyber sécurité, la politique du contenu, la protection des droits d'auteurs, la protection de la vie privée, la maintenance de la diversité culturelle, ou la réduction de la fracture numérique.

L'ICANN est une corporation sans but lucratif enregistrée en Californie. Son autorité fonctionnelle repose sur son Mémoire d'Entente (Memorandum of Understanding - MoU) avec le département de Commerce des Etats-Unis, initialement signé en 1998 et prolongé deux fois, la seconde fois de septembre 2006 à septembre 2009. Depuis le 1er octobre 2009, la base formelle de fonctionnement de l'ICANN est l'Affirmation d'Engagement (Affirmation of Engagement) signé par l'ICANN et le Département de Commerce des Etats-Unis. Ce document met l'ICANN sur le chemin de sa transformation vers une institution indépendante.

L'ICANN est une institution multi parties prenantes impliquant une variété d'acteurs en termes de capacités et de rôles. Ils sont répartis en quatre groupes principaux.

- 1 Acteurs qui ont été impliqués depuis les premiers jours de l'ICANN, y compris la communauté Internet, le secteur privé, et le gouvernement des Etats-Unis.
- 2 Organisations internationales, parmi lesquelles l'UIT joue le rôle le plus prééminent et l'Organisation mondiale de la propriété intellectuelle (OMPI).
- 3 Gouvernements nationaux dont l'intérêt à jouer un grand plus grand rôle à l'ICANN a commencé avec le processus SMSI.
- 4 Utilisateurs de l'Internet (at-large community).

L'ICANN a expérimenté plusieurs approches pour impliquer les utilisateurs de l'Internet. Dans ses premiers jours, la première tentative était d'impliquer les utilisateurs de l'Internet à travers les élections directes de leurs représentants aux organes dirigeants de l'ICANN. C'était aussi une tentative pour sauvegarder une base légitime pour l'ICANN. Avec le faible engouement et le mauvais usage du processus, le vote direct a échoué car n'ayant pas fourni une représentation réelle des utilisateurs de l'Internet. Plus récemment, l'ICANN était entrain d'essayer d'impliquer les utilisateurs de l'Internet à travers une large structure de gouvernance. Cette expérimentation organisationnelle est en cours.

Le processus de prise de décisions de l'ICANN était influencé par les processus initiaux de la gouvernance de l'Internet basés sur une procédure de prise de décision ascendante, transparente, ouverte et inclusive. Une différence principale entre la première communauté Internet des années 80 et le présent contexte de prise de décision se situe au niveau du 'capital social'. Dans le passé, la communauté Internet avait atteint un haut niveau de confiance et de solidarité mutuelles qui rendaient la prise de décision et la résolution des différends beaucoup plus simplement qu'aujourd'hui. Le développement de l'Internet a fait intervenir d'autres parties prenantes et, par conséquent, il serait difficile d'identifier le capital social parmi les actuels utilisateurs de l'Internet. Ainsi, la requête de la communauté Internet de garder quelques procédures de prise de décision Internet héritées de la naissance de l'Internet est largement utopique. Sans capital social, l'unique moyen de s'assurer le plein fonctionnement du processus de prise de décision est de formaliser et de développer divers mécanismes de vérification et d'équilibrage.

Quelques corrections sur les procédures de prises de décision ont déjà été faites pour refléter la réalité de ce changement. La plus importante a été la réforme de l'ICANN de 2002, qui incluait le renforcement du Comité consultatif gouvernemental (Government Advisory Committee - GAC) et l'abandon du système de vote direct.

## Les enjeux

### La technologie face à la gestion des questions politiques

La dichotomie entre la technique et la gestion des questions politique a créé une tension continue dans les activités de l'ICANN. L'ICANN s'est donné le portrait d'un 'corps de coordination technique de l'Internet' qui s'occupe seulement des questions techniques et ne s'occupe pas des aspects de politiques publiques de l'Internet. Les présidents de l'ICANN considéraient cette nature technique spécifique comme le principal argument conceptuel pour défendre le statut unique de l'institution et sa structure organisationnelle. Le premier président de l'ICANN, Esther Dyson, déclarait que:

*ICANN n'aspire pas à s'occuper des problèmes de gouvernance de l'Internet; en effet, il gouverne la plomberie, pas le peuple. Il a le mandat très limité d'administrer certains aspects (largement techniques) de l'infrastructure de l'Internet en général et du DNS en particulier<sup>14</sup>*

Les critiques de cette assertion soulignent souvent le fait qu'il n'existe pas de solutions techniquement neutres. Quoi qu'il en soit, chaque solution ou décision technique promeut certains intérêts, rend puissant certains groupes, et affecte la vie sociale, politique et économique. Les décisions sur les problèmes tels que le .xxx (matériels adultes) illustrent clairement que l'ICANN devra s'occuper des aspects de politiques publiques découlant des problèmes techniques.

### Statut international de l'ICANN

Les liens spéciaux entre l'ICANN et le gouvernement des États-Unis ont fait l'objet de grandes critiques qui ont pris deux formes principales. La première se base sur les considérations de principes: l'élément vital de l'infrastructure Internet mondiale qui pourrait affecter la vie de toute nation doit être supervisé par un seul pays. Cette critique est apparue pendant le processus SMSI et mise en valeur par la suspicion générale de la politique étrangère des États-Unis après l'intervention militaire en Irak. A ce niveau de discussion, l'argument contraire est que l'Internet a été créé aux États-Unis avec le soutien financier du gouvernement. Ceci donne au

gouvernement des Etats-Unis les bases morales pour décider de la forme et du niveau de l'internalisation de la gouvernance de l'Internet. Cet argument est particulièrement puissant au Congrès des Etats-Unis qui s'est fortement opposé à toute forme d'internalisation.

La seconde forme de critique se situe au niveau des considérations politiques légales. Par exemple, quelques critiques évoquent le fait que si le pouvoir judiciaire des Etats-Unis exerce son rôle et exécute correctement le régime de sanctions contre l'Iran et Cuba, ceci forcerait l'ICANN – étant une entité privée des USA – à enlever les domaines nationaux de ces deux pays de l'Internet. Selon cet argument, en maintenant les noms de domaines iranien et cubain, l'ICANN est entrain de passer outre le régime de sanctions des Etats-Unis. Cependant, si le retrait des noms de domaines des pays n'est jamais survenu, cela demeure possible du fait de l'actuel statut légal de l'ICANN.

Un nouveau développement dans l'évolution par rapport au statut de l'ICANN est signalé par la signature de l'Affirmation d'Engagement. Il jette les fondations pour un ICANN indépendant et ouvre un nouveau type de problèmes concernant sa future supervision, et les relations avec les gouvernements, etc.

Les deux problèmes clés – concernant les affaires de politiques publiques et l'internationalisation – pourraient être résolus en changeant le statut de l'ICANN, qui pouvait réduire les ambiguïtés et améliorer la clarté de sa mission. Un futur développement de l'ICANN devra requérir la mise en place de solutions innovantes. Un possible compromis pourrait être de transformer l'ICANN en une organisation internationale *sui generis*, qui devrait préserver tous les avantages de l'actuelle structure de l'ICANN et en même temps combler ses lacunes et particulièrement le problème de sa légitimité internationale.

## Notes de fin

- <sup>1</sup> Les exceptions étaient le Gouvernement des Etats Unis et quelques pays développés (Australie, Nouvelle Zélande, et durant cette époque la Commission Européenne).
- <sup>2</sup> Le processus du SMSI a commencé avec la première réunion préparatoire tenue en Juillet 2002 à Genève. Un premier sommet s'est tenu à Genève (décembre, 2003) et le deuxième sommet en Tunisie (novembre 2005).
- <sup>3</sup> La sélection des membres du GTGI combinait à la fois la représentativité et les critères de l'expertise. La structuration pour une meilleure représentativité a été guidée par le principe d'un tiers des participants représentant les gouvernements, un tiers représentant la société civile et un tiers représentant le secteur privé. Les représentants des gouvernements ont été sélectionnés selon les critères habituels des groupes régionaux des Nations Unies. Tout en tenant compte de l'aspect de représentativité, les membres sélectionnés étaient censés être bien informés des sujets afin de contribuer de manière substantielle aux discussions du GTGI.
- <sup>4</sup> Déclaration de Principes, WSIS-03/GENEVA/DOC/4-E, 12 décembre 20 03, Article 49 disponible sur <http://www.itu.int/wsis/docs/geneva/o c l/dop.html>
- <sup>5</sup> Le modèle brésilien de gestion de son nom de domaine national est généralement considéré comme un exemple de réussite d'une approche multi parties prenantes. L'organisme national chargé de la gestion du nom de domaine du Brésil est ouvert à tous les utilisateurs, y compris les autorités gouvernementales, le secteur des entreprises et la société civile. Le Brésil a progressivement étendu ce modèle à d'autres domaines de la gouvernance de l'Internet, en particulier dans le processus de la préparation du FGI de 2007, qui a eu lieu à Rio de Janeiro.
- <sup>6</sup> Lesage (1991) *La rivalité franco-britannique. Les cables sous-marins allemands* (Paris, 1915) pp. 257 –258; cité dans Headrick DR, *The invisible Weapon: Telecommunications and International Politics 1851–1945*. Oxford University Press: Oxford, UK p. 110.
- <sup>7</sup> Cukier KN (2005) The WSIS wars: An analysis of the politicization of the Internet (Les guerres du SMSI: une analyse de la politisation de l'Internet) In *The World Summit on the Information Society: Moving from the past into the future*. Stauffacher D, Kleinwächter W(eds). United Nations ICT Task Force: New York, NY USA , p. 176.
- <sup>8</sup> Le Gouvernement des Etats Unis a critiqué l'implication de l'UIT dans la mise en place du projet CORE dans un télégramme: '*without authorization of member governments to hold a global meeting involving and unauthorized expenditure of resources and concluding international agreements*'. (Sans autorisation des Etats membres pour la tenue d'une réunion internationale et faire des dépenses non autorisées en vue d'aboutir à un accord international).
- <sup>9</sup> La commodité d'un guichet unique a été l'un des arguments pour désigner l'UIT comme acteur central de la gouvernance de l'Internet.
- <sup>10</sup> Des commentaires appréciables ont été produits par Ayesha Hassan.
- <sup>11</sup> Etablissement du ' Uniform Domain-Name Dispute-Resolution Policy (UDRP).

- <sup>12</sup> La communauté de l'Internet remplit tous les critères de définition d'une communauté épistémique de Peter Haas: un groupe de professionnels qui croient en une même cause et les relations effectives, le test de vérité est de les accepter et de partager des valeurs communes; ses membres partagent une compréhension commune du problème et des solutions à y apporter. Haas P (1990) *Saving the Mediterranean: the politics of international environmental co-operation*. Columbia University Press: New York, NY, USA , p. 55.
- <sup>13</sup> Network Solutions est une entreprise technologique fondée en 1979. Le service d'enregistrement de noms de domaine est devenu la division la plus importante de l'entreprise. En janvier 2009, Network Solutions gérait plus de 6,6 millions de noms de domaine (Source: Wikipedia).
- <sup>14</sup> Berkman Center for Internet and Society, *The debate over Internet governance: snapshot in the year 2000*. Disponible sur: [http://cyber.law.harvard.edu/is99/governance/introduction.html#\\_ftn10](http://cyber.law.harvard.edu/is99/governance/introduction.html#_ftn10)

## Section 8

---

# Le processus de la gouvernance de l'Internet





# Le processus de la gouvernance de l'Internet

Cette section présente les expériences du processus politique du Forum sur la Gouvernance de l'Internet (FGI), qui, quoique peu visible sur la scène politique mondiale, est une expérience pertinente dans la gouvernance globale. À une époque où l'on a besoin d'atteindre un niveau de gouvernance satisfaisant au plan global, le FGI peut apporter quelques leçons utiles.

## Ce que les décideurs peuvent apprendre du FGI

Le débat sur la réforme de la gouvernance globale, accéléré après l'échec en 2009 du sommet de Copenhague sur le changement climatique, bute principalement sur deux grandes questions:

- 1 Comment élargir suffisamment le concept de la gouvernance globale afin d'inclure tous les acteurs importants?
- 2 Comment organiser en profondeur la gouvernance globale afin qu'elle devienne un processus efficient et efficace de prise de décision.

Les recettes sont différentes. Nombreux sont ceux qui essaient de réduire cette complexité en introduisant un 'Comité mondial de gestion' du type G20 en se basant sur les contributions des groupes d'intérêts régionaux ou en réduisant le 'bruit' de la participation des acteurs non-étatiques.<sup>1</sup> D'autres pensent que les Nations Unies peuvent/devraient être reformées afin d'être le principal cadre de discussion et de gestion des problèmes globaux. Beaucoup cherchent encore de nouvelles approches innovatrices qui feraient que la gouvernance globale soit suffisamment inclusive (légitime) et profonde (efficace) de façon à répondre à la complexité des questions politiques telles que le changement climatique, les migrations et la santé mondiale.

## Qu'est-ce que le Forum sur Gouvernance de l'Internet?

Le Forum sur la Gouvernance de l'Internet est le principal organe universel qui s'occupe de la question des politiques publiques de l'Internet. Le FGI a été mis en place lors du Sommet Mondial sur la Société de l'Information de Tunis en 2005 en tant que résultat d'un compromis entre les acteurs gouvernementaux et non gouvernementaux<sup>2</sup>. Comme résultat de ce compromis, le FGI n'était ni une structure d'où devaient sortir de grandes décisions ni être une organisation imposante. Petit à petit, sans grand bruit, le *modus operandi* du FGI s'est développé. Jusqu'à maintenant, il y a eu quatre rencontres annuelles du FGI: Athènes (2006), Rio de Janeiro(2007), Hyderabad (2008), Sharm El Cheikh (2009). Le FGI dispose d'un petit Secrétariat basé à Genève. Le FGI a inspiré une série de FGI régionaux et nationaux, de réseaux académiques (GIGAnet) et d'autres activités connexes.

Lorsque l'on discute sur la manière dont les autres domaines de la gouvernance globale peuvent bénéficier de l'expérience du FGI, il est important de souligner deux différences entre la Gouvernance de l'Internet et le multilatéralisme traditionnel. S'agissant du dernier, un sujet tel que le changement climatique, s'est ouvert aux acteurs non-gouvernementaux. Dans le cas de la Gouvernance de l'Internet, les Etats se sont vus obligés d'intégrer une ONG existante, gérée par l'ICANN, l'IETF et d'autres entités. Ensuite, le FGI n'est pas un organe de prise de décisions. Il n'a pas de mandat pour adopter des traités internationaux ou des documents légaux. Il est une sorte de 'laboratoire de décision' qui, à travers ses délibérations, crée une base de décisions qui peuvent être adoptées par d'autres institutions telles que l'ICANN, l'UIT, l'OMPI, pour ne citer que celles-là.

L'expérience du FGI et les leçons apprises sont classées en quatre grands groupes:

- 1 Les approches pour résoudre les questions d'élaboration des politiques globales
- 2 Gestion des processus d'élaboration des politiques
- 3 Le traitement des aspects scientifiques et techniques des questions politiques
- 4 L'accroissement de l'inclusion et de la participation

## **Approches de résolution des questions de politiques globales**

### **Les défis globaux ne nécessitent toujours pas des solutions globales**

L'un des crédos de la gouvernance globale est que pour des problèmes globaux, nous avons besoin de solutions globales. Le changement climatique ne tient pas compte des frontières; les communications Internet contournent facilement les limitations des souverainetés traditionnelles. L'argument est que si la politique n'est pas globale, il y a un risque que les pratiques nationales et régionales sapent la cause globale. Par exemple, certains pays qui accroissent leurs émissions de CO<sub>2</sub> peuvent saper les effets des tentatives de réduction d'émission de CO<sub>2</sub> d'autres pays. Suivant cet argumentaire, le seul moyen de résoudre les problèmes globaux est de chercher des solutions globales. D'autres arguments peuvent paraître insensés.

Le problème est qu'en cherchant à aboutir à une solution globale, l'on peut rater de nombreuses autres solutions politiques locales, nationales ou régionales.

Les négociations de Copenhague sur le changement climatique ont montré qu'il n'était pas toujours facile de parvenir à un consensus global. Il est difficile d'incorporer la diversité des intérêts et des cultures professionnelles/nationales dans un seul document qui doit être signé par tout le monde. Dans le cadre du changement climatique, il y a plusieurs initiatives politiques non globales, parmi lesquelles celles du secteur privé, des autorités locales et du secteur privé. Le FGI est, à cet égard, un modèle à suivre.

**Le FGI n'a pas été conçu pour créer de consensus global et légalement contraignant. Il a plutôt fourni un espace qui tient compte des diverses initiatives nationales et régionales sur la gouvernance de l'Internet tout en créant des liens et des synergies entre ces différentes initiatives.** Le Brésil a une façon remarquable de conduire sa politique nationale de gouvernance de l'Internet. L'Égypte est leader dans le domaine de la protection des enfants. L'Amérique Latine a un excellent programme pour coordonner la gestion des noms de domaine Internet. L'Inde est entrain de réaliser une percée en la matière après avoir facilité l'accès à l'Internet aux plus pauvres de ses communautés. La liste est longue. Ces exemples ont été présentés au FGI, ils ont fait l'objet de discussions et dans plusieurs cas ont émulé la création d'initiatives similaires (Ex: La gestion nationale brésilienne). La défense de la cause mondiale du développement de l'Internet a été conduite sans pour autant atteindre un arrangement global, légalement contraignant.

### Accroître la cohérence politique au moyen de l'approche multi parties – prenantes

L'un des plus grands défis de tout processus de prise de décision aujourd'hui c'est de parvenir à une sorte de cohérence face à des questions multidisciplinaires. Le FGI sert de parapluie sous lequel différents régimes; TIC, droits humains, commerce, propriété intellectuelle, peuvent se croiser. A travers l'IGF, diverses communautés découvrent que leurs secteurs de politiques font en réalité partie du processus plus large de la gouvernance de l'Internet. Dans certains domaines, comme par exemple le multilinguisme, l'IGF a aidé des organisations très diverses, notamment des gouvernements, l'ICANN, l'UNESCO et l'UIT, à coordonner leurs activités sur le même thème. *La participation pluripartite exceptionnellement importante a permis de dissiper les tensions entre différentes organisations et a servi d'espace de rassemblement de diverses initiatives au sein d'un processus d'élaboration des politiques cohérent.* Elle a également permis de limiter le problème du double traitement des questions politiques.

### Faciliter la coordination entre les niveaux national, régional et global d'élaboration des politiques

Dans un monde de plus en plus intégré, les communications instantanées et l'influence grandissante des acteurs non-étatiques brouillent les lignes de démarcation entre les espaces nationaux, régionaux et globaux d'élaboration des politiques. Des problèmes de politique évoluent rapidement entre les différents niveaux. Quelques ONG utilisent le 'Forum Shopping' pour insérer leurs nouvelles initiatives d'élaboration de politiques à un niveau le plus favorable. Quelques gouvernements de l'Union Européenne par exemple, utilisent une sorte de 'blanchiment de politiques' si une initiative n'est pas adoptée au niveau national, elle est envoyée au niveau régional et ré-importée comme une 'obligation internationale au niveau du pays'.

Dans le domaine de la Gouvernance de l'Internet, le réseau des forums d'élaboration des politiques est complexe et a existé avant même que le FGI (les organisations internationales, l'ICANN, ISOC et plusieurs organismes de standardisation) ne soit institué. En plus, les acteurs politiques de la gouvernance de l'Internet sont très agiles, passant facilement d'un niveau et forum politique à un autre en usant des technologies modernes de communication. Le FGI a essayé de maximiser les acquis et de réduire les risques des processus politiques de différents niveaux. *Le FGI coordonne les activités globales, régionales et nationales dans une approche de la base-vers le sommet (dans la préparation du FGI) et du sommet vers la base (dissémination des savoirs à partir du FGI).* La transparence du FGI fait que le processus soit moins ouvert au 'forum shopping'.

## Gestion des processus d'élaboration des politiques

### Un leadership efficient et efficace: dynamique dans l'action sur la voie et guide sur le côté

L'une des raisons du succès du FGI c'est aussi le leadership de Nitin Desai, le Président, et Markus Kummer, le Coordonnateur Exécutif du Secrétariat. Les deux ont une grande expérience diplomatique qui se complète. Desai a été en charge de la préparation de plusieurs grands sommets des Nations Unies; Kummer a eu une brillante carrière diplomatique pour le compte de la Suisse. Tandis que Desai dirige les principaux événements du FGI, Kummer crée une atmosphère de compréhension et l'inclusion à travers des activités le plus souvent en ligne, et participe aux plus grands événements de diverses communautés professionnelles autour de la question du FGI. Leur profonde connaissance des règles, procédures et pratiques des Nations Unies les a aidé à trouver des solutions innovantes, quoique non-écrites, et de rendre efficace le *modus operandi* du FGI.

### Bâtir un climat de confiance par une meilleure programmation et organisation

Le FGI a réuni les participants de divers horizons professionnels et culturels autour d'une même table. Ces participants n'ont ni travaillé pour les mêmes institutions, ni fréquenté les mêmes universités; et ne vivent pas dans les mêmes sphères sociales et non pas non plus d'autres moyens de créer un climat de confiance mutuelle. La confiance doit être bâtie dans une atmosphère où les suspicions des disputes passées sont encore présentes (ex: UIT et ICANN) ou encore du sentiment général de 'géo-suspicion' causé par la guerre d'Irak, ou les clichés du genre 'nous contre eux'.

Bâtir un climat de confiance exige de la patience et une programmation minutieuse des activités. Chaque phase du processus du FGI visait à accroître la compréhension mutuelle afin d'apporter de nouvelles connaissances et informations sur la table. Le résultat a été l'établissement graduel de la confiance et un débat très inspiré. Certaines propositions, telles qu'un appel initial pour adopter une convention cadre pour l'Internet furent abandonnées: le temps n'était pas encore propice pour plus de formalisation du domaine du FGI. Il y a cinq ans, cela aurait pu créer une tension et rompre potentiellement le processus de la Gouvernance de l'Internet. Aujourd'hui, il y a un débat pour l'adoption d'un traité global sur la cyber sécurité. Une gestion intelligente du temps a été essentielle pour aborder la question très controversée du rôle central de l'ICANN (une institution basée aux Etats-Unis) dans la gestion

des noms et numéros de l'Internet, le noyau de l'infrastructure globale de l'Internet.

Il y a cinq ans de cela aurait été source d'une controverse majeure. Aujourd'hui, depuis que le gouvernement américain a commencé l'internationalisation du rôle et de la structure de l'ICANN, les choses ne sont plus aussi controversées qu'avant. Ceci est un bon exemple qui montre que les questions politiques peuvent être améliorées avec le temps, si elles sont abordées soigneusement et ne dégèrent pas en une crise politique. Le FGI a été un très bon succès à cet égard. [Les diplomates et les décideurs peuvent apprendre à partir du FGI, la création d'un climat de confiance à travers une bonne programmation des activités et d'un suivi minutieux.](#) Le temps est capital, bien que pas suffisant pour la création d'un climat de confiance.

### Laisser évoluer le processus d'élaboration de politiques

Dans la société moderne, on met l'accent sur l'élaboration de stratégies logiquement consistantes pour ensuite en mesurer leurs rendements. La gouvernance globale et la diplomatie ne font pas exception à cette règle. La crise financière mondiale de 2008 a donné un exemple sur comment un système, basé dans une large mesure sur le modèle mathématique, peut conduire à l'effondrement s'il ne considère pas la complexité des conditions sociales.

Dans l'histoire de la diplomatie, le risque lié à la gestion trop structurée des processus politiques est bien illustré par le succès du Congrès de Vienne (1814) et l'échec du Traité de Versailles (1919). Le Congrès de Vienne a créé les bases d'une des périodes les plus pacifiques de l'histoire européenne: presque 100 ans sans guerre majeure. D'autre part, le traité de Versailles a échoué juste quelques années après avoir été signé. A Vienne, lentement, sans un grand plan prédéterminé, mais avec beaucoup d'interactions sociales, les négociations ont créé un véritable accord de paix. Le génie diplomatique de Metternich et Talleyrand a aidé à atteindre cela. Cependant, à Versailles, les diplomates s'étaient engagés dans un processus extrêmement organisé dans lequel des centaines de scientifiques, statisticiens et cartographes ont collaboré pour créer une "paix construite scientifiquement". Ils ont essayé de quantifier la justice et en fin de compte, créé les conditions politiques qui ont conduit à la seconde guerre mondiale. Les différences notoires dans les manières même dans lesquelles les négociations à Vienne et à Versailles étaient menées fournissent un argument convaincant contre une trop grande structuration de processus diplomatiques.

Bien que le FGI ne puisse être comparé à ces grands événements diplomatiques, sa pratique est plus proche de l'approche du Congrès de Vienne. Le FGI a impliqué le minimum de planification et de structuration nécessaires. **Les processus du FGI se sont étendus et se sont développés à travers le modelage collectif des participants impliqués, y compris ceux qui avaient des points de vue opposés.**

### **Reconnaitre que le texte demeure essentiel à la diplomatie**

Malgré toutes les promesses de conférences virtuelles et d'autres technologies, aujourd'hui- même plus que dans le passé – le texte demeure l'outil essentiel de la diplomatie<sup>3</sup>. Le texte est essentiel au processus du FGI, même si le FGI n'a produit aucun document final officiel (c'est-à-dire convention, traité ou déclaration). La plupart des échanges entre les sessions préparatoires sont faits par les listes d'adresses et les e-mails. Le site web utilise beaucoup plus de texte avec un faible recours aux photos ou aux images. Le FGI est soutenu par des médias sociaux très actifs, utilisant les outils de texte tels les blogs et Twitter.

Un nouvel argument en faveur du texte a émergé à travers les rapports textuels faits de transcriptions des réunions du FGI, qui pourrait avoir un impact important sur la diplomatie multilatérale et les négociations. Le rapport textuel est la transcription simultanée et fidèle (mot à mot) de chaque intervention orale dans une réunion. En apprenant, à partir de la pratique de l'ICANN, le Secrétariat du Groupe de Travail sur la Gouvernance de l'Internet (GTGI) a introduit le rapport textuel en avril 2005. Le FGI a continué la pratique. Toutes les interventions verbales sont transcrites simultanément par les sténographes spécialisés et projetées immédiatement sur un écran géant dans la salle de conférence et diffusées aussi par Internet. Pendant que les délégués parlent, les transcriptions de leurs discours apparaissent sur l'écran.

Le rapport textuel a eu un effet important sur le *modus operandi* diplomatique. **L'idée que ce qui est dit sera conservé en textes imprimés rend beaucoup de participants plus prudents en choisissant le niveau et la durée de leurs interventions verbales. Le rapport textuel augmente aussi la transparence des rencontres diplomatiques.**

### Reconnaitre que l'informel dans les conférences internationales pourrait être source d'inégalité dans la participation

Un des défis auquel le FGI fait face est la juxtaposition de la culture diplomatique formelle des Nations Unies à la culture informelle de la communauté de l'Internet. Après cinq réunions annuelles du FGI, il semble que la culture informelle ait pris le dessus. Tandis que cette culture crée une ambiance inclusive et facilite la participation des jeunes et de diverses communautés, elle pose aussi quelques défis. Les participants dont les cultures nationales ont un fort respect pour la hiérarchie sociale peuvent se sentir mal à l'aise et hésitent à parler dans un environnement de travail très informel. En outre, dans les cultures diplomatiques, juridiques et dans certaines cultures professionnelles, la participation aux débats est structurée par des protocoles professionnels.

Paradoxalement, le caractère informel des réunions et des discussions peut empêcher la participation de certains délégués et créer une inégalité potentielle. Le FGI a pallié à ce risque en cherchant les moyens d'inclure plusieurs niveaux de formalité en offrant des cadres où les différentes parties prenantes pourraient participer aisément. Par exemple, le FGI a relevé le niveau de protocole dans certaines sessions, principalement la plénière en ajoutant plus de règles de procédure typiquement diplomatiques (exemple: le temps de parole, la représentation formelle) et les sessions spéciales organisées pour les parlementaires.

### Traitements des aspects scientifiques et techniques dans les processus d'élaboration des politiques

#### Reconnaitre que la science et la technologie sont rarement politiquement neutres

Le processus du FGI a encore confirmé que les questions de science et de technologie (S&T) ont des conséquences sur la prise de décision, rendant plus fort plusieurs groupes d'intérêts. À certains égards, la plupart des questions S&T deviennent des questions politiques; les questions politiques, à leur tour, exigent des décisions sur des valeurs et des intérêts en jeu.

Dans ce contexte, il est risqué de représenter les questions de S&T comme étant politiquement neutre. Si les arguments de S&T sont promus comme 'vérité suprême', cette approche peut avoir l'effet inverse. Par exemple, dans les négociations sur le changement climatique, une telle approche a contribué

à rendre les arguments scientifiques extrêmement vulnérables. Les e-mails divulgués de l'Université de East Anglia et les fausses données sur les glaciers de l'Himalaya, jettent le doute sur — les arguments scientifiques (considérés normalement comme solides) sur le changement climatique.

La question de l'interaction entre la science et la politique est aussi importante dans les processus d'élaboration des politiques tels que la sécurité alimentaire et la santé. Les scientifiques doivent augmenter leur présence dans l'arène diplomatique, tandis que les diplomates devront apprendre comment aborder les questions scientifiques.

Dans le processus du FGI, les S&T ont contribué à une prise de décision efficiente. Les questions techniques sont discutées dans un contexte socioéconomique plus large. *La composition multi parties prenantes du FGI, impliquant les scientifiques, les spécialistes en informatique, les diplomates, les économistes et les autres a créé un contexte favorable à une interaction efficace entre S & T et prise de décision.*

### **Améliorer la communication entre différentes cultures organisationnelles et professionnelles**

Un nombre important des livres ont été écrits au sujet de la communication transculturelle: comment parler aux Arabes, Chinois, Américains, etc. L'expérience du FGI montre cependant que dans un processus politique, le défi majeur est souvent de faciliter l'échange entre les différentes cultures professionnelles (exemple: les juristes, les ingénieurs) et les différentes cultures organisationnelles (exemple: les organisations internationales, les gouvernements, les compagnies). Dans le monde globalisé d'aujourd'hui, avec la communication instantanée, il est souvent plus facile de communiquer à l'intérieur des mêmes cercles professionnels, même au-delà les frontières nationales. Les professions partagent la même manière de cerner les problèmes et de trouver les solutions. Par exemple, un ingénieur en informatique allemand communique mieux avec un autre ingénieur en Chine que, disons, avec un diplomate allemand.

Comme les questions globales deviennent de plus en plus techniques (exemple: changement climatique, commerce et santé), une communication inter professionnelle efficace devient de plus en plus importante. Les améliorations dans la communication interprofessionnelle peuvent être atteintes à travers la formation, l'éducation et l'ouverture à d'autres cultures. La meilleure communication interprofessionnelle peut aussi contribuer à améliorer la cohérence politique entre les ministères et les organisations

internationales. Le FGI a fait des pas positifs dans la communication interprofessionnelle par une facilitation efficace d'échange des idées entre les spécialistes de diverses professions, y compris l'informatique, la diplomatie et l'économie. Le bon exemple de ceci est la grande diversité professionnelle et institutionnelle des invités impliqués dans les discussions du FGI.

### Faire un savant mélange entre connaissance technique et capacités diplomatiques

Dans la plupart des procédures globales d'élaboration de politiques, il y a un dilemme. Devraient-elles être gérées par les spécialistes (exemple: les scientifiques dans le changement climatique) ou les généralistes (diplomates).

L'argument pour spécialistes est que pour parler des questions techniques, on a besoin de la connaissance approfondie de ces questions. Selon ce point de vue, par exemple, l'expérience scientifique est nécessaire pour négocier les questions du changement climatique. Les diplomates traitent généralement les aspects politiques, sociaux et autres non techniques des questions négociées.

La réussite du leadership du FGI – Desai et Kummer – a défié le mythe de gouvernance estimant que les questions techniques devraient être gérées par les experts techniques. En tant que nouveaux venus dans le champ de la gouvernance de l'Internet, Desai et Kummer ont fourni une contribution non partisane à un débat de longue date sur les sujets comme la position de l'ICANN, la régulation des noms de domaine, etc. Parfois, comme le FGI le montre, la "diplomatisation" du traitement des questions techniques peut aider à surmonter les conflits traditionnels dans les communautés techniques. L'expérience du FGI confirme qu'il n'y a pas une recette-miracle d'engagement de spécialistes et de généralistes. C'est une interaction dynamique qui dépend des contextes précis et des individus impliqués. L'unique 'astuce' est de sensibiliser à l'idée du risque d'accorder aux spécialistes ou aux généralistes un rôle exclusif.

## Augmenter l'inclusion et la participation

Renforcer les 'marques diplomatiques' nationales par l'implication des acteurs non-étatiques dans les initiatives diplomatiques<sup>4</sup>

Avec plus d'acteurs et plus de sujets complexes à traiter, l'approche diplomatique traditionnelle est limitée. Même les services diplomatiques les

plus efficaces ne peuvent fournir autant de 'bandes passantes diplomatiques' (c'est-à-dire les ressources humaines qualifiées) exigées. Une plus large bande passante diplomatique peut être fournie par l'inclusion des acteurs de la société civile, le secteur commercial, les autorités locales et d'autres entités impliquées dans les procédures de politique globale.

Certains pays, tels que le Canada, la Suisse et les pays scandinaves, ont reconnu cette évolution plus tôt et ont déjà intégré les acteurs non-étatiques dans leurs activités de politiques étrangères. Cette pratique n'est pas courante dans beaucoup de pays en développement, où les services diplomatiques sont de petite taille avec des ressources financières et humaines limitées, et où les structures multi parties prenantes nationales ne sont apparues qu'au cours de ces dernières années.

Le FGI a contribué d'une manière pratique à la prise de conscience des avantages de l'approche multi parties prenantes dans les cercles gouvernementaux, en particulier dans les pays en développement. **En dehors du principe de l'inclusion, l'approche multi parties prenantes du FGI s'est révélée être une solution pratique qui aide les pays à augmenter leurs marques diplomatiques sans allouer de ressources supplémentaires.** Les structures nationales multi parties prenantes du FGI sont en train d'apparaître. Les gouvernants se concertent plus avec les privés et la société civile. Certains petits Etats et les Etats en développement sont représentés aux processus politiques de la Gouvernance de l'Internet par des experts du milieu académique et des ONG.

Parfois, encourager une telle inclusion est souvent une affaire de coordination, et de création d'un cadre de parties prenantes nationales. Le renforcement des capacités à travers les programmes de formation qui impliquent divers décideurs du même Etat aide aussi: les co-participants dans un programme de formation tendent à développer la confiance mutuelle et un esprit d'équipe.

### **Renforcer la participation à distance par l'établissement des hubs<sup>5</sup>**

C'est dans la nature d'un forum qui examine la Gouvernance de l'Internet que d'utiliser l'Internet pour étendre la participation aux réunions du FGI au-delà de ceux qui peuvent participer physiquement. De nos jours, en plus de la diffusion régulière par Internet des réunions, la principale innovation du FGI a été l'introduction des hubs à distance. Les hubs à distance sont définis comme étant des rencontres locales qui ont lieu pendant et parallèlement aux réunions du FGI, organisées par les universités, les centres d'accès aux Technologies de l'Information et de la Communication (TIC), les ONG et

d'autres acteurs qui traitent les questions politiques et de Gouvernance de l'Internet. Ils projettent une diffusion simultanée sur le web de la réunion pour que les participants à distance puissent être informés sur ce qui est débattu. Les participants à un hub peuvent envoyer les questions par texte ou par vidéo et recevoir les réponses des panélistes en temps réel. De plus, les hubs et les tables-rondes animent des discussions correspondant aux thèmes du FGI d'un point de vue local. A travers ces activités, les hubs locaux enrichissent la coordination entre les procédures de la politique globale et locale. Par exemple, pendant le FGI de 2008, le hub à distance de Madrid a suivi la session sur la cyber sécurité et a poursuivi les débats dans un contexte spécifiquement espagnol. Un total de huit hubs opéraient en parallèle au FGI de 2008 (Madrid, Lahore, Barcelone, Belgrade, Buenos Aires, São Paulo, Bogota et Pune). Plus de 450 heures d'événements étaient diffusées pour la participation à distance et un total de 522 participants à distance ont rejoint la réunion durant les quatre jours.<sup>6</sup>

Après le succès du test en 2008, le concept de hubs a été adopté par le Secrétariat du FGI. En tant que résultat du fort soutien du pays hôte et la participation à distance des groupes de travail (Remonte Participation Working Group: RPWG), le FGI de Sharm El Sheikh en 2009 a vu une augmentation du niveau de participation à distance de 12 hubs venant de tous les continents. La diffusion sur Internet des réunions fut amplement améliorée, et les gens pouvaient participer à distance aux sessions principales ainsi qu'aux ateliers. L'incorporation de la diffusion sur le web en temps réel du transcrit fut une autre amélioration qui a augmenté l'accès pour les malentendants ainsi que la compensation des difficultés techniques (audio) pour ceux ayant des connexions Internet lentes.

L'expérience du FGI montre que la participation à distance augmente considérablement l'inclusion et l'ouverture des rencontres internationales. Elle crée un lien directe entre le global et le local, qui manque souvent dans la diplomatie multilatérale.

### Récolter une grande variété de contributions à travers la 'longue concertation'

Le concept d'une politique de 'longue concertation' est inspiré par un marketing mené patiemment et fait allusion à la possibilité de récolter une grande variété des contributions politiques qui seraient normalement perdues dans les procédures intergouvernementales traditionnelles. *Les individus et les groupes ont été capables d'exprimer leurs opinions directement au FGI à travers une implication personnelle dans les événements, la communication*

par le web et la participation à distance. Ces nouvelles idées et ces nouveaux paradigmes, qui n'atteindraient pas le sommet des forums mondiaux dans la plupart des procédures politiques, ont considérablement enrichi la procédure du FGI. Une des leçons que le FGI peut transmettre est que le premier pas vers un processus de politique plus inclusive est la facilitation d'une participation ouverte. Le bienfait complet de la participation ouverte et inclusive n'est atteint que si une grande variété de contributions sont collectées, considérées, et si possible, comprises dans les délibérations politiques. L'inclusion augmente la légitimité du processus et le sentiment d'appartenir aux parties prenantes.

### Assurer la participation significative des Etats en développement: partir de l'égalité formelle à l'égalité fonctionnelle

Dans le contexte des Nations Unies, les petits états et les états en développement assurent généralement leur statut égalitaire en insistant sur la représentation formelle et les procédures. A la différence des Etats développés et des grands Etats, ils manquent d'un réseau organisé de représentation parallèle de leurs intérêts sociaux au sens large à travers le secteur privé, la société civile et les communautés académiques. Il n'est donc pas surprenant, qu'ils aient des réserves sur une participation multi parties prenantes. Dans les réunions à grande échelle qui rassemblent des milliers de participants sur une base égale, un petit Etat ou un Etat en développement perd la sauvegarde des procédures des Nations Unies où il est l'un des 194 représentants d'Etat avec le statut formel égal, indépendamment de sa taille ou de sa puissance.



Quelques Etats son plus nombreux que d'autres

**Egalité formelle/Egalité fonctionnelle dans les pourparlers sur le changement climatique.**

Au début du processus de SMSI à la fin de 2002, beaucoup de petits états et états en développement se sont fortement opposés à l'initiative d'introduire la participation équitable des représentants du privé et de la société civile. Certains de ces Etats ont soutenu l'approche 'one-stop-shop' qui leur fournirait une 'adresse unique', de préférence intergouvernementale, où ils pourraient discuter toutes les questions y relatives.<sup>8</sup>

Depuis 2002, le SMSI, le GTGI et le FGI en particulier ont fait des progrès considérables en renforçant des aspects pro-développement du processus multi parties prenantes, y compris la recherche de solution sur le risque de sous représentation de petits Etats et des Etats en développement.

Au niveau formel, le FGI s'assure de la participation adéquate des divers acteurs des pays en développement à toutes les sessions et discussions. Le niveau croissant de la participation des pays en développement était visible aux FGI de Rio et à Hyderabad.

Le processus du FGI a aidé beaucoup de petits Etats et des Etats en développement à faire bon usage des ressources humaines disponibles. Ceux-ci peuvent ne pas être des diplomates, mais d'autres nationaux avec une certaine expertise dans la Gouvernance de l'Internet, travaillant dans les organisations de l'Internet ou des universités à travers le monde. Profiter des experts qui travaillent à l'étranger est vital, surtout pour les petits Etats.

Une participation physique c'est-à-dire être présent aux réunions ne s'assimile pas nécessairement à une participation égalitaire. La participation égalitaire exige une connaissance adéquate, les aptitudes et la confiance de la part de chaque délégué à s'engager dans ce processus politique. Le FGI a essayé d'assurer la participation égalitaire à travers des activités de renforcement de capacités. Depuis 2002, plus de 850 officiels et professionnels de petits Etats et des Etats en développement se sont impliqués dans la formation et d'autres activités de renforcement de capacités qui vont au-delà des formations traditionnelles de type académique, par une combinaison avec de la recherche et de l'immersion dans les instances d'élaboration de politiques, tout cela visant à aider les participants à comprendre la dynamique du FGI et gagner la confiance nécessaire pour une participation complète et significative dans les principes politiques. L'implication de plusieurs acteurs (diplomates, officiels, ingénieurs) dans le processus de la formation donne aux participants une compréhension des avantages d'une approche multi parties prenantes et leur apporte la confiance de participer aux réunions avec d'autres communautés professionnelles.

Le processus du FGI a aussi visé le renforcement et le développement des communautés de praticiens de la gouvernance de l'Internet dans le Sud en général et au niveau des régions (ex: l'Ouest de l'Afrique, l'Est de l'Afrique, et l'Amérique Latine) et des pays (ex: Kenya, Brésil, Sénégal). Ces communautés ont aidé beaucoup de petits Etats ainsi que des pays en développement à développer leur propre représentation multi parties prenantes en identifiant les experts non-gouvernementaux déjà impliqués dans les recherches académiques sur l'Internet ainsi que sur le processus politique de la gouvernance de l'Internet.

Au FGI, en augmentant les niveaux de participation, en encourageant le renforcement de capacités et en encourageant le développement des réseaux et des communautés, beaucoup des pays en développement ont évolué d'une participation formelle à une participation fonctionnelle dans la Gouvernance de l'Internet.

## Notes de fin

- <sup>1</sup> Ministre Norvégien des affaires étrangères, Johan Gahre Store, critique fortement le manque de la légitimité du G20 dans son article intitulé: *'One of the greatest setbacks since World War II (un de plus grands échecs depuis la 2<sup>ème</sup> guerre mondiale)*. Disponible sur: <http://www.siegel.de/international/europe/0,1518,702104,00html>
- <sup>2</sup> Le compromis était trouvé entre deux approches de prise de décision. L'approche 'gouvernementale', promue essentiellement par les pays en développement, a soutenu que l'Internet devrait être gouverné par les organisations internationales telles que l'UIT. L'approche non gouvernementale, favorisée par les pays développés et en particulier les Etats Unis, a soutenu une Gouvernance de l'Internet avec une grande implication du secteur privé et de la société civile. Ils se sont opposés au rôle exclusif des organisations telles que l'UIT. Chaque côté a obtenu gain de cause dans la création du FGI comme solution de compromis. L'approche 'gouvernementale' a obtenu que le FGI soit ancré dans le système des organisations internationales. Le FGI est sous la direction du Secrétaire Général des Nations Unies. L'approche non-gouvernementale a obtenu l'approche multi parties prenantes du FGI avec l'implication du secteur privé et de la société civile.  
  
Certains considèrent que dans ce compromis, on a aussi gagné en liant le FGI au Secrétariat Général des Nations Unies pour empêcher à l'UIT d'avoir un rôle plus proéminent de dans la Gouvernance de l'Internet.
- <sup>3</sup> Un aspect intéressant est l'usage des services SMS sur les téléphones mobiles, à travers lequel le texte demeure essentiel à la communication humaine malgré de puissants outils basés sur la vidéo et la voix.
- <sup>4</sup> L'approche multi parties prenantes est conceptualisée comme étant la meilleure approche à la gouvernance, et est décrite comme: *la sommation de plusieurs façons où beaucoup d'individus et d'institutions, publiques et privées, gèrent leurs affaires communes. C'est un processus continu à travers lequel l'on peut concilier les intérêts conflictuels et divers et à partir desquels des actions de coopération peuvent être entreprises. Il comprend des institutions et des régimes formels encouragés à faire appliquer la conformité aussi bien que les arrangements informels que les individus et les institutions ont acceptées ou perçoivent être dans leur intérêt* (Commission sur la Gouvernance Globale, 1995).
- <sup>5</sup> Voir [www.igfremote.com](http://www.igfremote.com) pour des commentaires importants et substantiels fournis par Ginger Paque et Marilia Marcel, qui sont aussi la force conductrice du RPWG.
- <sup>6</sup> Un rapport détaillé sur la participation à distance au FGI de 2008 est disponible au: <http://www.igfremote.com/ReportRPIGF-final.pdf>
- <sup>7</sup> <http://www.igfremoti.info>
- <sup>8</sup> Des enquêtes préliminaires montrent que 80 à 100 organisations internationales, organismes de standardisation, forums et autres entités couvrent les différents aspects de la Gouvernance de l'Internet. Même pour les grands Etats développés, ce vaste champ est presque impossible à couvrir. Le FGI a essayé de réduire et maîtriser sa complexité en séparant les aspects relatifs à la Gouvernance de l'Internet d'autres processus de politique (respect de la vie privé, la propriété intellectuelle, des droits humains, le développement, le commerce électronique, etc.)

# Section 9

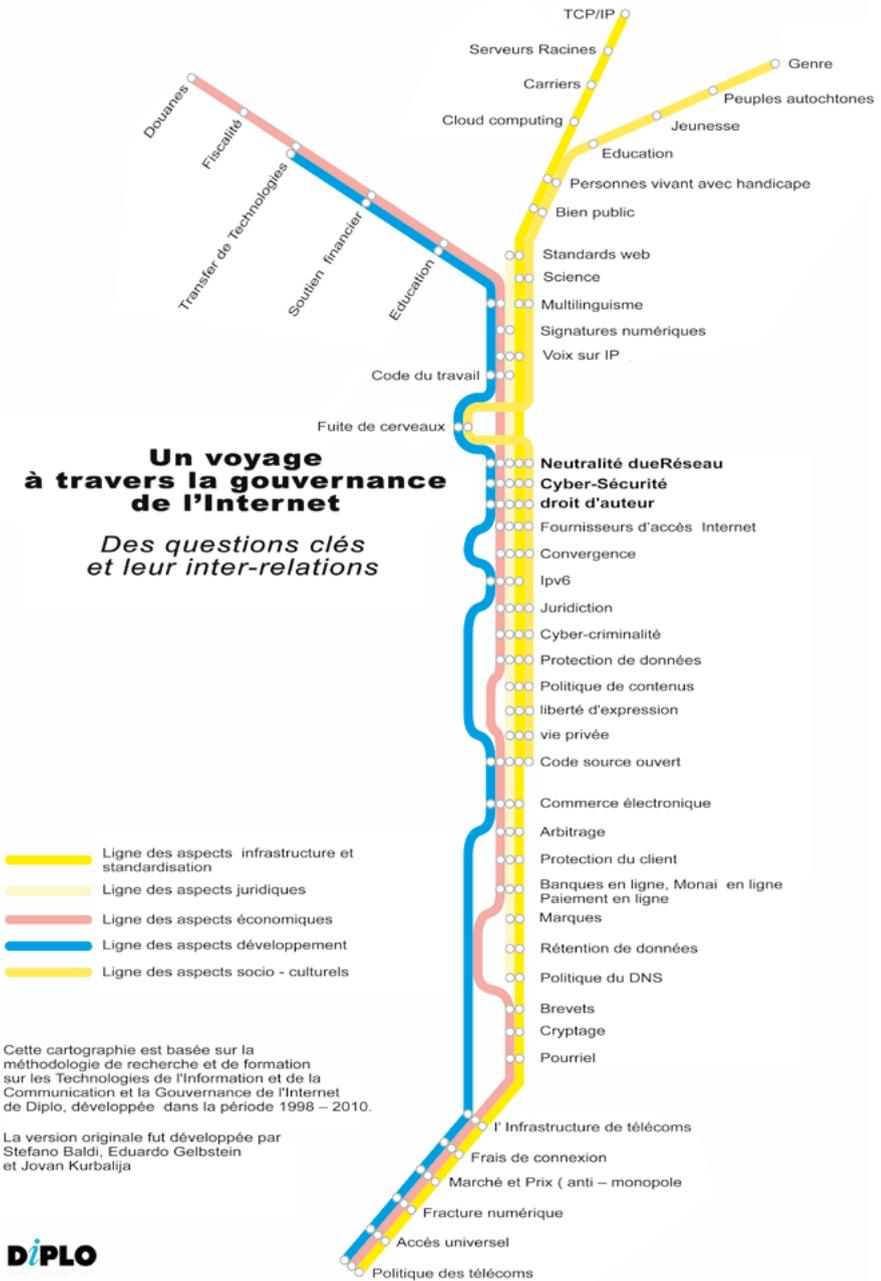
---

# Annexes

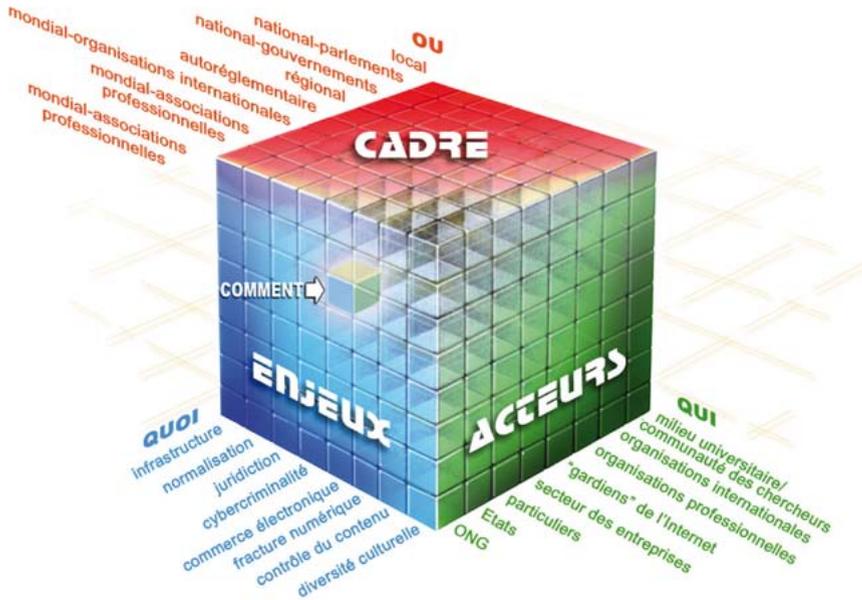




# Annexes



## Le cube de la gouvernance de l'Internet



L'axe **QUOI (What)** a trait aux ENJEUX de la Gouvernance de l'Internet (ex: infrastructure, droits d'auteur, vie privée). Il traduit l'aspect **multidisciplinaire** de cette approche.

L'axe **QUI (Who)** du cube se focalise sur les principaux acteurs (Etats, organisations internationales, société civile, secteur privé). C'est le **multi partites**.

L'axe **OU (Where)** du cube traite du cadre dans lequel les questions de l'Internet devraient être traitées (Autorégulation, locale, nationale, régionale ou mondiale). Ceci est une approche **multi stratifiée** de la Gouvernance de l'Internet.

Quand nous déplaçons les pièces dans ce cube de la Gouvernance de l'Internet, nous obtenons l'intersection **COMMENT (How)**. C'est la face du cube qui peut nous aider à percevoir comment devraient être réglementées les questions particulières, à la fois en termes de techniques cognitives et légales (les analogies), ainsi qu'en termes d'instrument (ex: loi molle, les traités et les déclarations). Ainsi par exemple, une intersection précise peut nous aider à voir **COMMENT** les questions de vie privée (**QUOI**) devraient être traitées par la société civile (**QUI**) à un niveau national (**OU**).

Le cinquième composant, **QUAND (When)**, est séparé du cube de la Gouvernance de l'Internet.

## Un aperçu de l'évolution de la GI

Acteur						
Période	Etats-Unis	Gardiens de l'Internet	Organisations	Secteur privé	Les pays	La société civile
	Le Ministère de la Défense gère le système des noms de domaine					
1986	La 'National Science Foundation' (NSF) prend le dessus sur le Ministère de la Défense (Department of Defense - DoD)					
1994				Le NSI (Network Solutions Inc.) signe un contrat avec le NSF (National Science Foundation) pour gérer le DNS pour la période 1994-1998		

### Le début de la guerre du DNS

Après que la NSF eut légué la gestion du DNS à la NSI (une société privée), la communauté de l'Internet (principalement ISOC – Internet Society) a lutté pendant plusieurs années afin de ramener la gestion du DNS au domaine public. Elle a réussi après quatre ans. Le processus a impliqué un certain nombre de techniques diplomatiques telles que: la négociation, la création de coalition, l'usage d'influence, la mise en place du consensus, etc.

Juin 1996	L'IANA (Internet Assigned Number Authority)/ISOC projettent de prendre le relais du NSI une fois que son contrat serait fini; des domaines supplémentaires sont introduits, le secteur de la Marque Déposée présente une forte opposition aux nouveaux domaines du premier niveau comme le fait l'UIT
Printemps 1997	<p>Une proposition d'un Comité Ad hoc International [IAHC] (CAHI).</p> <p>Les participants à l'IAHC, deux représentants des groupes d'intérêt pour les Marques Déposées, de l'Organisation Mondiale pour la Propriété Intellectuelle (OMPI), de l'UIT et du 'National Science Foundation' et cinq représentants de l'IETF.</p> <p>Mise en place d'un Mémoire d'Entente pour les domaines génériques de premier niveau gTLD qui deviennent une 'ressource publique', mise en place de sept nouveaux domaines et forte protection des marques déposées.</p> <p>Mise en place du CORE (Council of Registers) (Cérémonie de signature en mars 1997 à l'UIT, Genève). CORE a immédiatement échoué.</p> <p>Forte opposition du gouvernement des Etats-Unis, du NSI et de l'UE.</p>

Acteur	Etats Unis	Gardiens de l'Internet	Organisations internationales	Secteur privé	Les pays	La société civile
Période						
1997	Le gouvernement américain transfère la gestion du DNS au Ministère du Commerce (Department of Commerce - DoC)					
Jun 1998	Le Livre blanc du Ministère du Commerce invite les principaux acteurs à proposer leurs propres solutions		Les propositions sont reçues par l'International Forum on the White Paper (IFWP), de l'Open Root Server Confederation (ORSC) - et du Boston Working Group (BWG).			
			<p>Au lieu de préparer un nouveau document, l'ISOC se focalise sur:</p> <ul style="list-style-type: none"> <li>• La mise en place d'une large coalition impliquant les organisations internationales (partie de l'initiative IAHC), le secteur privé (IBM) et les pays clés (Japon, Australie et l'Union Européenne).</li> <li>• La création d'une nouvelle organisation.</li> </ul>			
Deuxième partie de 1998			<p>Septembre 1998 – Accord d'avant-projet commun ISOC-NSI                  Octobre 1998 – L'ISOC abandonne les accords et crée l'ICANN (Internet Corporation for Assigned Names and Numbers)</p>			
15 novembre 1998	Le Ministère du Commerce transfère l'autorité à ICANN	<p>L'ICANN acquiert deux nouvelles fonctions cruciales:</p> <ol style="list-style-type: none"> <li>1. L'Autorité d'accréditation des registres pour le (gTLD)</li> <li>2. La gestion de la fonction autoritaire (l'aspect politique) est gardée par le Ministère de commerce</li> </ol>				
Avril 1999	Accord DoC-ICANN-NSI et introduction d'un système d'enregistrement commun ; le NSI perd son monopole mais obtient un arrangement de transition/.....(gestion de quatre domaines, etc.					

### STRUCTURE ET FONCTIONNEMENT DE L'ICANN

Jun 1998	Formation du PSO (Protocol Supporting Organisation: Organisation de soutien au protocole) composé de l'IETF, le W3C (World Wide Web Consortium) et les autres pionniers de l'Internet	Initialisation du processus des noms de domaine de l'Internet à l'OMPI	ASO (Address Support Organisation) créée pour représenter l'association des registres de DNS (ARN, RIPE, NCC) DNSO (Domain Name Support) - établies pour protéger les Marques Déposées et les intérêts commerciaux	Trente pays établissent un Comité de conseil gouvernemental (Government Advisory Committee - GAC) pour bénéficier de plus d'influence dans la gestion des domaines nationaux, L'ICANN réagit en établissant un sous comité du DNSO pour les ccTLDs
----------	---	--	--	--

#### La fin de la guerre du DNS

La guerre prit fin par le compromis. ISOC a réussi à prendre plus de contrôle public de la gestion du DNS mais les intérêts commerciaux sont restés très forts. D'où les intérêts correctement protégés du secteur privé et des communautés des gardiens. Ceci n'était pas le cas avec la position des Etats nations et la communauté de l'Internet en général. Ce sont les deux aspects les plus faibles de la gouvernance de l'ICANN.

Acteur	Etats Unis	Gardiens de l'Internet	Organisations internationales	Secteur privé	Les pays	La société civile
<b>Période</b>						
2000-2003			L'émergence d'une plus grande attention sur l'Internet à l'UIT, OMPI, l'UNESCO, l'OCDE, le Conseil de l'Europe et la Banque Mondiale	Forte campagne par le secteur privé pour un Internet régulé (lois sur les droits d'auteur, le commerce en ligne, etc.)	Développement de la législation de l'Internet, procès, etc.	ONG impliquées dans le fossé numérique, droits humains, les questions de genre sur l'Internet
			Initiatives multisectorielles et globales centrées sur le développement de l'Internet et de la gouvernance, etc.: G8 DOT Force, Forum économique Mondial, UNICT – Task Force, SMSI, Global Knowledge Partnership			
Juin 2002–Nov. 2003	La première PrepCom pour le SMSI fut tenue en juin 2002. La Gouvernance de l'Internet a émergé comme un sujet durant la première PrepCom pour l'Asie de l'Ouest à Beyrouth (février 2003) Lors de la tenue du premier sommet à Genève (2003), la décision a été prise d'établir le Groupe de Travail sur la Gouvernance de l'Internet (GTGI) Les initiatives multisectorielles et globales portent sur le développement et la GI, etc.: le G8 DOT Force, le Forum Economique Mondial, le UN ICT Task Force.					
2004-2005	Le GTGI a modelé les discussions sur la GI à cette phase du SMSI. Le GTGI était un corps multi parties prenantes composé des représentants de gouvernements, du secteur privé et de la société civile. Le SMSI a tenu quatre réunions préparatoires et produit un rapport qui a servi comme outil de prise de décision à propos la GI au SMSI – Tunisie (2005).  En Tunisie, le compromis de la GI de Tunis a présenté le FGI comme un compromis entre ceux qui s'opposaient à tout changement au régime centré sur l'ICANN et ceux qui plaidaient pour que l'Internet soit gouverné par une entité intergouvernementale.					
2006-2009	Après la conclusion du SMSI, à Tunis (2005), le FGI fut établi afin de poursuivre le processus d'élaboration de la GI. Jusque-là quatre FGI se sont tenus: Athènes (2006), Rio de Janeiro (2007), Hyderabad (2008) et Sharm El Sheikh (2009).  Le 30 septembre 2009, le Gouvernement Américain et l'ICANN ont signé <i>l’Affirmation of commitments</i> (l'affirmation des engagements) qui a mis fin à la supervision américaine de l'ICANN, l'une des questions les plus controversées de la GI. L'ICANN a introduit une nouvelle phase vers une organisation indépendante avec plus de questions que de réponses sur sa position et son rôle futur.					
2010	Le 5 <sup>e</sup> FGI se tiendra à Vilnius (Lituanie). Son but visait essentiellement la révision des cinq premières années, les Nations Unies décideront en automne 2010 sur l'avenir du FGI.					



Le groupe des Etats **Afrique, Caraïbe, Pacifique (ACP)** est composé d'Etats signataires de l'Accord de Georgetown entre les ACP et l'UE, officiellement appelé Accord de partenariat ACP-UE ou Accord de Cotonou. Le groupe des Etats ACP est composé de 79 Etats membres dont 48 d'Afrique sub-saharienne, 16 des Caraïbes et 15 du Pacifique. A l'origine, le groupe était créé avec l'objectif de coordonner la coopération entre leurs membres et l'UE en se focalisant sur la négociation et la mise en œuvre des accords de coopération avec l'UE. Quelques années après, le groupe des Etats ACP a étendu son champ d'activités au-delà de la coopération de développement avec l'UE, et traite désormais d'autres questions telles que le commerce, l'économie et la culture dans divers forums internationaux tels que l'Organisation Mondiale du Commerce (OMC).

Les principaux objectifs du groupe des Etats ACP:

- Promouvoir le développement durable de ses Etats membres ainsi que de leur intégration progressive dans l'économie mondiale, qui fait de la question de la réduction de la pauvreté, une question prioritaire; ainsi qu'un nouvel ordre mondial plus juste et équitable.
- Coordonner les activités des Etats ACP dans le cadre des accords de partenariat ACP-UE.
- Encourager et renforcer la solidarité entre les Etats ACP et l'entente entre les peuples et les gouvernements ACP.



**DiploFoundation** est une organisation à but non lucratif qui travaille pour renforcer la participation multi parties prenantes dans la pratique diplomatique et les relations internationales. Nos activités s'intègrent dans nos objectifs, l'éducation, la formation et le renforcement des capacités.

- **Les cours:** Nous offrons des cours universitaires de deuxième cycle et organisons des ateliers sur plusieurs domaines liés à la diplomatie pour des diplomates, des fonctionnaires, des employés d'organisations internationales, les ONG et les étudiants. Nos programmes de formations se font soit en ligne, soit de manière mixte.
- **Le renforcement des Capacités:** avec le soutien des donateurs et des partenaires, nous offrons des programmes de renforcement des capacités pour les participants des pays en développement dans plusieurs domaines dont la Gouvernance de l'Internet, les droits de l'Homme, la diplomatie publique et la diplomatie de la santé.

- **La recherche:** Au moyen de nos recherches et conférences, nous faisons des recherches sur des sujets liés à la diplomatie, aux relations internationales ainsi qu'à l'enseignement à distance sur Internet.
- **Les publications:** Nos publications vont de l'examen des développements contemporains en diplomatie, aux analyses récentes des aspects traditionnels de la diplomatie.
- **Le développement de logiciels:** Nous avons créé un ensemble de logiciels clients destinés aux diplomates et les autres travailleurs des relations internationales. Nous excellons aussi dans la production de plateformes d'enseignement à distance.

Diplo est basé à Malte, avec des bureaux à Genève et à Belgrade. Diplo a vu le jour à partir d'un projet qui consistait à introduire les outils des technologies de l'information et de la communication dans la pratique de la diplomatie initié, en 1993, à l'Académie Méditerranéenne des Etudes Diplomatiques de Malte. En novembre 2002, Diplo s'est établi et reconnue comme fondation indépendante à but non lucratif par les gouvernements de Malte et de Suisse. Notre intérêt s'est étendu de l'application des technologies de l'information et de la communication dans la diplomatie, à l'introduction de nouvelles approches d'enseignement des pratiques traditionnelles de la diplomatie et des relations internationales.



Le **Fonds Européen de Développement de l'UE (FED)** est le principal instrument de financement dans le cadre de l'Accord de Cotonou (Accord de partenariat ACP-UE) pour fournir de l'aide (européenne) au groupe des Etats des ACP ainsi qu'aux pays et territoires d'outre-mer (PTO). L'un des objectifs du FED est de promouvoir le développement économique, social et culturel des Etats ACP.

## Bref aperçu sur l'auteur



Jovan Kurbalija est le directeur fondateur de DiploFoundation. C'est un ancien diplomate ayant de l'expérience académique et professionnelle en droit international, en diplomatie, ainsi qu'en ce qui concerne les technologies de l'information. En 1992, il a établi une cellule pour d'étude des technologies de l'information et de la diplomatie à l'Académie Méditerranéenne des Etudes Diplomatique de Malte.

Après plus de 10 ans de formation, de recherches et de publications, la cellule s'est développée, en 2002, en DiploFoundation.

Depuis 1994, le Dr Kurbalija donne des cours sur l'impact des TIC/de l'Internet sur la diplomatie ainsi que sur les TIC/la Gouvernance de l'Internet. Il a enseigné à l'Académie Méditerranéenne des Etudes Diplomatique de Malte, à l'Académie de Diplomatie de Vienne, à l'Institut néerlandais des relations internationales (Clingendael), à l'Institut universitaire des études internationales et de développement à Genève, à l'Institut de développement du Staff des Nations Unies ainsi qu'à l'Université de Californie du Sud. Il a conceptualisé et dirige actuellement le programme de renforcement des capacités de la Gouvernance de l'Internet de DiploFoundation (2005-2011).

Les principaux intérêts de recherche du Dr Kurbalija comprennent le développement d'un régime international pour l'Internet, l'usage de l'Internet dans la diplomatie et dans les négociations modernes, ainsi que l'impact de l'Internet sur les relations internationales modernes.

Le Dr Kurbalija a publié et édité plusieurs livres, articles et chapitres, parmi lesquels: *Le guide d'Internet pour les diplomates (The Internet Guide for Diplomats)*, *Connaissance et diplomatie (Knowledge and Diplomacy)*, *L'influence des Technologies de l'Information sur les pratiques diplomatiques (Influence of IT on Diplomatic Practices)*, *L'influence des TIC sur les services diplomatiques des pays en développement (The Influence of IT on Diplomatic Services for Developing Countries)*, *La diplomatie moderne, Langage et diplomatie (Modern Diplomacy and Language and Diplomacy)*.

En collaboration avec Stefano Baldi et Eduardo Gelbstein, il est co-auteur de *La bibliothèque de la société d'information (Information Society Library)*, un ensemble de huit brochures couvrant une variété de questions relatives à l'Internet.

[jovank@diplomacy.edu](mailto:jovank@diplomacy.edu)





**DIPLO**  
www.diplomacy.edu



9 7 8 9 9 9 3 2 5 3 2 5 9