GOUVERNANCE DE L'INTERNET

ENJEUX, ACTEURS ET FRACTURES

Jovan Kurbalija • Eduardo Gelbstein

GOUVERNANCE DE L'INTERNET

ENJEUX, ACTEURS ET FRACTURES

Jovan Kurbalija • Eduardo Gelbstein

ISBN 9932-53-14-6

Publié par DiploFoundation et Global Knowledge Partnership

DiploFoundation

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

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

Courriel: diplo@diplomacy.edu
Site Web: http://www.diplomacy.edu

Secrétariat du Global Knowledge Partnership

Level 23, Tower 2, MNI Twins
11, Jalan Pinang
50450 Kuala Lumpur, Malaysia

Courriel: gkps@gkps.org.my
Site Web: http://www.globalknowledge.org

Avec l'aimable parrainage de la Direction suisse pour le développement et la coopération

Directeurs de la publication: Dejan Konstantinović et Steven Slavik
Illustrations: Zoran Marčetić – Marča
Conception de la couverture: Nenad Došen
Mise en page & maquette: Aleksandar Nedeljkov
Traduit de l'anglais par Maryck Nicolas-Holloway, Tradwïse Plus Ltd.
© Copyright 2005, DiploFoundation

Toute référence à un produit particulier dans cet ouvrage est purement donnée à titre d'exemple et ne saurait être traitée comme une quelconque recommandation dudit produit.

TABLE DES MATIERES

Introduction

L'évolution de la gouvernance de l'Internet 8
Négociations internationales sur la gouvernance de l'internet 9
Que veut dire la gouvernance de l'Internet? 11
Boîte à outils pour la gouvernance de l'Internet 13
Approches et modèles 16
Principes directeurs 21
Analogies 25
La classificatiotn des enjeux de la gouvernance de l'Internet. 30
"Bâtiment en construction" 33

La corbeille infrastructure et normalisation

Introduction 37
L'infrastructure des télécommunications 38
Normes et services techniques (L'infrastructure de l'Internet) 41
Transport Control Protocol / Internet Protocol (TCP/IP). 42
Le système des noms de domaine (DNS) 46
Les serveurs racines 51
Les fournisseurs d'accès à l'Internet (FAI) 53
Les fournisseurs de bande passante sur l'Internet (IBP). 55
Modèle économique pour la connectivité Internet 56
Normes du web 59
Open Source 60
Convergence: Internet–Télécommunications–Multimédia 61
Sécurité de l'Internet 64
Cryptage 68
Pollupostage. 69

La corbeille juridique

Introduction 77
Mécanismes juridiques 78
Législation 78
Normes sociales (Coutumes) 79
Autorégulation 79
Jurisprudence 80
La réglementation internationale 80
Juridiction. 82
Arbitrage 88

Droits de propriété intellectuelle 90
Marques déposées 90
Droits d'auteur 91
Brevets 97
Cybercriminalité 98
Signatures numériques 100
Droit du travail 103
Respect de la vie privée et protection des données 104

La corbeille économique

Introduction 113
Commerce électronique 114
Protection des consommateurs 118
Fiscalité 119
Douanes 120
La monétique: monnaie et transactions bancaires électroniques . . . 121

La corbeille développement

Introduction 127
La fracture numérique 129
Accès universel 130
Stratégies pour surmonter la fracture numérique 131
Developpement des infrastructures de télécommunications et de l'Internet 131
Appui financier 132
Aspects socioculturels 133
Politique et réglementation des télécommunications 134

La corbeille socioculturelle

Introduction 137
La politique du contenu 137
Droits de l'homme 144
Multilinguisme et diversité culturelle 145
Biens publics universels 146
Enseignement 148

Annexes

"Les aveugles et l'elephant" de John Godfrey Saxe 155
Synthèse de l'évolution de la gouvernance de l'Internet 156
Feuille de route pour un voyage à travers la gouvernance de l'Internet 158
Cube Diplo de la gouvernance de l'internet 159

A propos des auteurs 160

SECTION 1

Introduction

La gouvernance de l'Internet n'est pas un sujet simple. Bien qu'elle traite d'une notion qui se veut être un symbole représentatif majeur du monde NUMERIQUE, elle ne peut pas être abordée avec une simple logique numérique binaire qui ne reconnaît que le vrai et le faux, le bon et le mauvais. Au lieu de cela, la très grande subtilité du sujet et ses innombrables nuances de sens et de perception exigent une approche ANALOGIQUE, englobant une suite d'options et de compromis.

Par conséquent, ce livret ne cherche pas à fournir de déclarations arbitraires sur les questions liées à la gouvernance de l'Internet. Il entend plutôt proposer un cadre pratique pour l'analyse, la discussion et la résolution des problèmes clés dans ce domaine.

INTRODUCTION

> En quelques années seulement, l'Internet a révolutionné le commerce, la santé, l'éducation, et plus encore, le tissu même de la communication et des échanges. De surcroît, son potentiel est bien plus puissant que ce que nous avons pu entrevoir dans le laps de temps relativement court depuis sa création. Pour gérer, promouvoir et protéger sa présence dans notre vie quotidienne, nous devons faire preuve d'une créativité tout aussi grande que celle de ses inventeurs. De toute évidence, une forme de gouvernance s'impose, mais rien ne dit que cette gouvernance doit intervenir de manière classique, puisque nous avons affaire à quelque chose de radicalement différent.
>
> Kofi Annan - Forum mondial sur la gouvernance de l'Internet (New York, 24 Mars 2004)

Dans un laps de temps relativement court, l'Internet est devenu un instrument indispensable de la société d'aujourd'hui. A la mi-2005, il était estimé que l'Internet:

- comptait environ un milliard d'internautes à travers le monde;
- était à l'origine d'un commerce électronique dont le chiffre d'affaires était estimé à US$150 milliards et devrait connaître une croissance rapide;
- avait des répercussions sociales majeures dans l'éducation, la santé, l'administration et d'autres domaines d'activité;
- permettait la cyberdélinquance, telle que la fraude, les jeux d'argent, la pornographie, et le vol d'identité;
- permettait un emploi abusif ou à mauvais escient sous forme de code malveillant et de pollupostage.

L'Internet et les statistiques ne font pas bon ménage. Dès les premiers balbutiements de l'Internet, il a été difficile de recenser le nombre exact d'internautes, d'hôtes de site Web, le volume de trafic et les informations financières, pour ne citer que ces éléments. En outre, les chiffres sont souvent utilisés pour faire du battage sur la croissance de l'Internet. Certains chercheurs attribuent d'ailleurs l'éclatement de la bulle des dot-com à l'utilisation de statistiques exagérées concernant le potentiel de croissance de l'Internet.

La prise de conscience croissante de l'impact social, économique et politique de l'Internet sur la société a porté la question de la gouvernance de l'Internet sur le devant de la scène.

Dans le cas de l'Internet, on a besoin de gouvernance pour, entre autres

- empêcher ou, tout au moins, minimiser, le risque de fragmentation de l'Internet;
- maintenir la compatibilité et l'interopérabilité entre les systèmes
- sauvegarder les droits et définir les responsabilités des différents acteurs;
- protéger les utilisateurs finals d'une utilisation abusive et/ou à mauvais escient;
- encourager tout nouveau développement.

Le processus qui consiste à aborder les questions juridiques et les conséquences sociales du progrès technologique est toujours à la traîne par rapport aux innovations technologiques. Cela vaut également pour l'Internet.

Nous sommes actuellement dans la phase préliminaire des négociations internationales concernant la gouvernance de l'Internet, qui se caractérise par le besoin d'élaborer et de convenir d'un cadre élémentaire et de sélectionner des instruments appropriés afin de débattre des innombrables questions qu'elle soulève. Quels sont les acteurs probablement les mieux placés pour influencer le développement futur de l'Internet? Quelles seront leurs politiques en matière de connectivité, de commerce, de contenu, de financement, de sécurité et autres questions essentielles pour notre société de l'information émergente. Ce sont là de certains des principaux points qu'il convient d'aborder dans le cadre de la gouvernance de l'Internet.

L'EVOLUTION DE LA GOUVERNANCE DE l'INTERNET

l'IETF (Internet Engineering Task Force). L'IETF était chargé de gérer la poursuite du développement de l'Internet par le biais d'un processus coopératif et consensuel de prise de décisions appelant la participation d'une foule de gens. Il n'existait aucune administration centrale, aucune planification centralisée et pas l'ombre d'une conception ambitieuse.

A ce stade, tout restait relativement simple. Toutefois, en 1994, la Fondation nationale des sciences des Etats-Unis décida de faire appel au secteur privé en sous-traitant la gestion du système de noms de domaine (DNS) à Network Solutions Inc (NSI). Cette démarche fut très mal vue par la communauté internaute et déclencha une véritable "guerre du DNS".

Le lecteur trouvera une étude détaillée de l'évolution de la gouvernance de l'Internet aux pages 140-141.

Cette "guerre du DNS" fit intervenir d'autres acteurs: le monde des affaires, des organisations internationales et des Etats nations. Elle déboucha, en 1998, sur la création d'une nouvelle organisation chargée de l'attribution des noms et numéros sur l'Internet, l'ICANN (Internet Corporation for Assigned Names and Numbers).

Depuis 1998 et la création de l'ICANN, le débat sur la gouvernance de l'Internet s'est caractérisé par une mobilisation plus active des gouvernements nationaux, notamment par le biais du cadre onusien.

NEGOCIATIONS INTERNATIONALES SUR LA GOUVERNANCE DE L'INTERNET

Le Sommet mondial sur la société de l'information (SMSI), organisé à Genève en décembre 2003, a officiellement porté la question de la gouvernance de l'Internet à l'ordre du jour diplomatique. La Déclaration de principes et le Plan d'action adoptés au SMSI proposaient un certain nombre de mesures dans le domaine de la gouvernance de l'Internet, y compris la création d'un groupe de travail sur la gouvernance de l'Internet (GTGI).

Ci-dessous figure un extrait de la Déclaration de principes du SMSI concernant la gouvernance de l'Internet:

> 50. Les problèmes internationaux liés à la gouvernance de l'Internet devraient être traités de manière coordonnée. Nous demandons au Secrétaire général des Nations Unies de créer un groupe de travail sur la gouvernance de l'Internet, dans le cadre d'un processus ouvert et inclusif prévoyant un mécanisme qui garantira la participation pleine et active des représentants

des Etats, du secteur privé et de la société civile tant des pays développés que des pays en développement et qui fera intervenir les organisations intergouvernementales et internationales et forums intéressés pour, d'ici à 2005, étudier la gouvernance de l'Internet et éventuellement proposer des mesures à prendre.

Ci-dessous figure un extrait du Plan d'action du SMSI concernant la gouvernance de l'Internet:

13. b) Nous demandons au Secrétaire général des Nations Unies de créer un groupe de travail sur la gouvernance de l'Internet, dans le cadre d'un processus ouvert et inclusif qui garantisse la participation pleine et entière des pouvoirs publics, du secteur privé et de la société civile tant des pays en développement que des pays développés, et qui fasse intervenir les organisations intergouvernementales et internationales et les forums intéressés afin, d'ici à 2005, d'étudier la gouvernance de l'Internet et de formuler des propositions concernant les mesures à prendre. Ce groupe devrait notamment:

i. élaborer une définition pratique de la gouvernance de l'Internet;

ii. identifier les questions d'intérêt général qui se rapportent à la gouvernance de l'Internet;

iii. élaborer une conception commune des rôles et des sphères de responsabilité respectives des gouvernements, des organisations intergouvernementales, des organisations internationales et des autres forums existants, ainsi que du secteur privé et de la société civile, tant des pays en développement que des pays développés;

iv. élaborer un rapport sur les résultats de cette activité, lequel serait soumis pour examen et suite à donner à la seconde phase du SMSI (Tunis, 2005).

Il est très probable que le SMSI et le GTGI constituent la première phase du processus de gouvernance de l'Internet qui devrait permettre de clarifier les enjeux liés à la gouvernance de l'Internet, de définir l'ordre du jour et d'introduire des procédures et des mécanismes.

Le processus de négociations multilatérales et la gouvernance de l'Internet

PHASE DE NEGOCIATION	TRAVAUX DU SMS
Négociations préliminaires	De 1998 jusqu'au SMSI de Genève (2003)
Définition de l'ordre du jour et clarification des enjeux	Phase entamée en décembre 2003 lors du SMSI de Genève avec la décision de créer le Groupe de travail sur la gouvernance de l'Internet (GTGI); Le GTGI a présenté son rapport en juin 2005; Cette phase du processus prendra fin à Tunis.
La recherche de formules	Après Tunis 2005
Négociation des détails	
Accord	
Mise en œuvre	

QUE VEUT DIRE LA GOUVERNANCE DE L'INTERNET?

Lors du Forum mondial sur la gouvernance de l'Internet, qui s'est tenu aux Nations Unies à New York les 24 et 25 mars 2004, plusieurs conférenciers ont donné des versions différentes de l'apologue des aveugles et de l'éléphant.

Il ressort clairement de la morale de cette fable que tout débat sur la signification de l'expression "Gouvernance de l'Internet" n'est pas simplement un caprice linguistique. Différente perceptions du sens de l'expression peuvent engendrer des approches et des attentes différentes en termes de politique.

Un jour six hommes de l'Hindoustan
Tous enclins à apprendre,
S'en vinrent voir l'Eléphant
(Tant bien même qu'ils étaient tous aveugles),
.....
Et ainsi ces hommes de l'Hindoustan
Se disputèrent fort et longtemps,
Chacun soutenant son opinion
Obstinément et à l'excès.
Quoique chacun ait eu en partie raison,
Pour l'ensemble ils avaient tous tort!

Extrait du poème "The Blind Men and the Elephant" écrit par le poète américain John Godfrey Saxe (1816-1887); le texte intégral est donné à l'Annexe I.

Les experts en télécommunications considèrent la gouvernance de l'Internet du point de vue du développement des infrastructures techniques. Les experts en informatique se concentrent sur le développement de différentes normes et applications, telles que XML ou Java. Les experts en communications donnent plus de poids à la simplification des communications. Les militants des droits de l'homme considèrent la gouvernance de l'Internet du point de vue de la liberté d'ex-

pression, du respect de la vie privée et autres droits fondamentaux. Les juristes s'attardent sur la juridiction et la résolution des différends. Les politiques du monde entier donnent généralement la préférence aux médias et aux questions qui leur gagnent des points auprès de leur électorat, par exemple le techno-optimisme (plus d'ordinateurs = plus d'éducation) et les menaces (sécurité de l'Internet, protection des enfants). Les diplomates s'intéressent davantage au processus et à la protection des intérêts nationaux. La liste des différentes optiques professionnelles sur la gouvernance de l'Internet susceptibles d'entrer en conflit est interminable.

Le GTGI a formulé la définition pratique suivante de la gouvernance de l'Internet: "Il faut entendre par "gouvernance de l'Internet" l'élaboration et l'application par les Etats, le secteur privé et la société civile, dans le cadre de leurs rôles respectifs, de principes, normes, règles, procédures de prise de décisions et programmes communs propres à modeler l'évolution et l'utilisation de l'Internet."
Cette définition pratique est un bon point de départ pour le débat sur la gouvernance de l'Internet, qui va inévitablement déboucher sur une description plus détaillée de chacun des deux termes: "Internet" d'une part et "gouvernance" d'autre part.

Chacun des deux termes, tant "Internet" que "gouvernance", sont sujets à controverse du point de vue de leur interprétation. Certains auteurs soutiennent que le premier élément, la notion d'"Internet", n'englobe pas tous les aspects existants des développements mondiaux en matière de TIC. Deux autres expressions: "société de l'information" et "technologie de l'information et des communications" sont généralement présentées comme ayant une sens plus large. Elles comprennent des domaines qui vont au-delà de l'Internet, tels que la téléphonie mobile.

Toutefois, l'argument en faveur de l'utilisation du terme "Internet" est appuyé par la transition rapide des communications mondiales vers l'utilisation du protocole TCP/IP comme principale norme technique de communications. L'Internet, déjà omniprésent, continue son expansion à très vive allure, non seulement du point de vue du nombre d'internautes mais encore en termes des services qu'il est en mesure d'offrir, notamment le système VoIp (voix sur Internet), qui pourrait bien à terme remplacer la téléphonie classique.

Le second élément de l'expression, le terme "gouvernance," a été très controversé dans les débats récents, notamment lors du SMSI. Le malentendu vient principalement du fait de l'utilisation du terme gouvernance comme synonyme de gouvernement. Lorsque le terme de "gouvernance de l'Internet" a été introduit dans le cadre du processus SMSI, nombreux sont les pays, notamment les pays en développement, qui ont associé cette notion au concept de gouvernement. L'une des conséquences d'une telle approche a été de

croire que les problèmes liés à la gouvernance de l'Internet devaient être abordés au niveau intergouvernemental avec une participation limitée des autres acteurs, principalement issus du secteur privé et de la société civile.

Quelles étaient les principales raisons à l'origine de ce malentendu terminologique? Est-il évident que le terme "gouvernance" ne veut pas dire "gouvernement"? Pas nécessairement. Le terme "bonne gouvernance" a été adopté par la Banque mondiale pour promouvoir la réforme des Etats par l'introduction d'une plus grande transparence, la réduction de la corruption et le renforcement de l'efficacité administrative. Dans ce contexte, le terme "gouvernance" est directement associé à des fonctions qui sont au cœur même du gouvernement.

Une autre source potentielle de malentendus réside dans la traduction du terme "gouvernance" dans les autres langues. En espagnol, le terme fait principalement référence à la fonction publique ou au gouvernement (gestión pública, gestión del sector público et función de gobierno). La référence à la fonction publique et au gouvernement se retrouve aussi en français (gestion des affaires publiques, efficacité de l'administration, qualité de l'administration et mode de gouvernement). Le portugais suit un modèle semblable en faisant référence au secteur public et au gouvernement (gestao pública et administraçao pública). Cet écart dans l'interprétation du terme "gouvernance" explique peut-être pourquoi, d'un point de vue linguistique, tant de délégations du SMSI ont associé la question de la gouvernance de l'Internet au secteur public et axé leurs délibérations sur le besoin d'une intervention des pouvoirs publics.

BOITE A OUTILS POUR LA GOUVERNANCE DE L'INTERNET

Un régime de gouvernance de l'Internet est à un stade embryonnaire de développement. L'expérience acquise par d'autres régimes internationaux (par ex. en matière d'environnement, de transport aérien, de contrôle des armes) a démontré que de tels régimes tendent à élaborer un cadre commun de référence, valeurs, perception des relations de cause à effet, modes de raisonnement, terminologie, vocabulaire, jargon et abréviations.

Dans nombre de cas, le cadre commun est influencé par la culture professionnel spécifique (les modèles de connaissances et de comportement partagés par les membres d'une même profession). L'établissement d'un cadre commun permet généralement de promouvoir une meilleure communication et une meilleure compréhension. Toutefois, il sert aussi parfois à protéger son propre "territoire" et à écarter l'influence de tiers. Citons à cet égard le linguiste américain, Jeffrey Mirel, qui affirme: "Toute langue professionnelle se veut territoriale".

Tout régime de gouvernance de l'Internet sera complexe car il aura besoin de faire intervenir beaucoup de questions, d'acteurs, de mécanismes, procédures et instruments.

Les questions relatives à l'Internet comportent au moins cinq dimensions: les infrastructures, le plan juridique, le plan économique, le développement et le plan socioculturel. Chacune de ces dimensions est abordée dans les chapitres qui suivent. Bon nombre des acteurs, qu'ils émanent du secteur privé ou du secteur public, ont un rôle à jouer dans chacune de ces dimensions. La plupart d'entre eux (responsables des serveurs racines, fournisseurs d'accès à l'Internet, juristes spécialisés dans les marques de fabrique, experts en développement, militants de la société civile, etc.) ont des cultures professionnelles très spécifiques et très développées.

Chaque combinaison de problèmes et d'acteurs a son but, ses objectifs, sa terminologie propre et ses sphères de collaboration et d'influence. Il semble que bon nombre, sinon la plupart, de ces combinaisons fonctionnent actuellement en vase clos par rapport aux autres. Si l'on ajoute à cela la multiplicité des langues de travail qui reflète la nature mondiale des problèmes, le défi qui consiste à regrouper tous ces éléments en une architecture cohérente de gouvernance devient manifeste; toutefois, si tous les intéressés y mettent de la bonne volonté, il ne saurait être insurmontable.

L'illustration ci-dessous, inspirée de l'artiste néerlandais M.C. Escher, démontre certaines des perspectives paradoxales qui sont associées à la gouvernance de l'Internet.

La complexité de la mise en oeuvre de la gouvernance de l'Internet indique qu'un raisonnement linéaire, fondé sur une seule cause et sur le principe du "soit l'un/soit l'autre", est fort mal adapté à la résolution des problèmes associés à la gouvernance de l'Internet. Par conséquent, il

convient de faire appel à de nouveaux outils cognitifs qui savent tenir compte de cette complexité et introduire des approches communes et des principes directeurs.

Le principal objectif d'une boîte à outils pour la gouvernance de l'Internet serait:

- d'organiser les outils actuellement utilisés dans le débat sur la gouvernance de l'Internet;
- de créer des outils cognitifs supplémentaires;
- de promouvoir le caractère ouvert à tous du processus de gouvernance de l'Internet en offrant aux parties qui le souhaitent des outils pour comprendre les problèmes, les positions et les développements

La boîte à outils pour la gouvernance de l'Internet se compose de:

- modèles et d'approches;
- principes directeurs;
- analogies.

Tout comme le processus de gouvernance de l'Internet, la boîte à outils est en perpétuelle mutation. Les approches, modèles, principes direc-

teurs et analogies apparaissent et disparaissent au gré de leur pertinence du moment dans le cadre du processus de négociation.

APPROCHES ET MODELES

Il y a déjà longtemps que la gouvernance de l'Internet d'un point de vue global et des questions spécifiques de la gouvernance de l'Internet font partie des débats de politiques et des échanges entre universitaires. Un certain nombre d'approches et de modèles ont progressivement vu le jour et représentent les points où il est possible d'identifier des différences dans les positions de négociation et dans les cultures nationales et professionnelles. L'identification d'approches et de modèles communs peut réduire la complexité des négociations et permettre de créer un système commun de références.

Approche étroite ou approche large?

La question de savoir s'il fallait adopter une approche étroite ou large en matière de gouvernance de l'Internet figure à ce jour parmi les principaux enjeux, traduisant les approches et intérêts multiples représentés au sein du processus de gouvernance de l'Internet. L'approche "étroite" se concentre sur les infrastructures de l'Internet (système de noms de domaine, adresses IP et serveurs racines) et sur la position de l'ICANN en tant qu'acteur prépondérant dans ce domaine.

Selon l'approche dite "large", les négociations relatives à la gouvernance de l'Internet devraient aller au-delà des questions d'infrastructures et aborder d'autres enjeux d'ordre juridique, économique, socioculturel et de développement. Il est particulièrement important de faire une distinction entre ces deux approches dans la phase préliminaire de définition de l'ordre du jour des négociations liées à l'Internet.

L'approche plus large est implicitement soutenue par la Déclaration du SMSI qui donne pour mandat au GTGI "d'identifier les questions d'intérêt général qui se rapportent à la gouvernance de l'Internet". Cette approche est aussi celle qui prévaut dans les discussions des milieux politiques et universitaires sur la gouvernance de l'Internet.

Le débat actuel a dépassé le stade du "soit l'un/soit l'autre" pour recenser des priorités et un équilibre adéquat entre l'approche "étroite" (questions ayant trait à l'ICANN) et l'approche "large" (autres aspects de la gouvernance de l'Internet).

Aspects techniques ou aspects politiques?

Un défi notable posé par le processus de gouvernance de l'Internet sera l'intégration des aspects techniques et politiques car il est difficile de bien les distinguer. Les solutions techniques ne sont pas neutres. Au bout du compte, chaque solution ou option technique promeut un groupe d'intérêts, habilite certains groupes et, dans une certaine mesure, a des répercussions sur la vie sociale, politique et économique.

Dans certains cas, un objectif initial qui se voulait politique pour une solution technique a évolué. Ainsi par exemple, l'architecture Internet à réseaux de bout en bout et à commutation par paquets a été conçue dans le souci politique de créer un réseau robuste capable de résister à une attaque nucléaire. Par la suite, cette même architecture est devenue la base du développement de la créativité et de la liberté d'expression sur l'Internet.

D'autres solutions techniques, telles que des moyens électroniques pour la protection des droits d'auteur, sont délibérément créées afin de remplacer ou de faire appliquer certaines politiques (en l'espèce, une protection plus rigoureuse des droits d'auteur).

Dans le cas de l'Internet, pendant longtemps, les questions aussi bien techniques que politiques étaient régies par un seul et même groupe social - la communauté Internet d'origine. Avec la croissance de l'Internet et l'apparition de nouvelles parties prenantes dans les années quatre-vingt-dix, issues principalement du secteur des affaires et des pouvoirs publics, cette unité technologique et politique s'est trouvée rompue. La réforme de la gouvernance de l'Internet, y compris la création de l'ICANN, marquait un effort pour tenter de rétablir l'équilibre perdu. Cette question reste ouverte et il est fort probable qu'elle sera l'un des sujets de controverse potentiels lors du SMSI/GTGI.

Approche du "vieux réel" contre "nouveau cybernétique"

Presque toutes les questions liées à la gouvernance de l'Internet présentent deux approches. L'approche du "vieux réel" - ou "du vin nouveau dans de vieux flacons" - soutient que l'Internet n'introduit rien de neuf dans le domaine de la gouvernance. L'Internet n'est rien d'autre qu'un nouveau dispositif, qui, du point de vue de la gouvernance, n'est pas différent de ses prédécesseurs: le télégraphe, le téléphone ou la radio.

Ainsi par exemple, dans les discussions juridiques, cette approche soutient que les lois existantes peuvent s'appliquer à l'Internet moyennant un minimum d'ajustements. Tant qu'il concerne la communication en-

tre des personnes, l'Internet n'est pas différent du téléphone ou du télégraphe et il peut donc être réglementé comme tout autre dispositif de télécommunications. Dans le domaine économique, cette approche soutient qu'il n'existe aucune différence entre le commerce ordinaire et le commerce électronique. Par conséquent, il n'est pas nécessaire que le commerce électronique fasse l'objet d'un traitement juridique spécial. L'approche "concrète" est également opposée aux moratoires fiscaux sur le commerce électronique.

L'approche "nouveau-cybernétique" - ou "vin nouveau dans un nouveau flacon" - soutient que l'Internet est un dispositif radicalement différent de tous ses prédécesseurs. Par conséquent, il nécessite un gouvernance radicalement différente. Cette approche était particulièrement prisée dans les débuts de l'Internet. Il était même espéré que la méthode novatrice initiale pour régir l'Internet -"consensus sur l'essentiel plus règle évolutive" - servirait de modèle à la réglementation de certains autres secteurs d'activités humaines. Le principe de base de l'approche "cybernétique" est que l'Internet a dissocié notre réalité sociale et politique du monde des Etats souverains. L'espace cybernétique est différent de l'espace réel, par conséquent il nécessite une autre forme de gouvernance.

L'influence de cette approche s'est tout particulièrement ressentie dans le processus de création de l'ICANN, organisme qui, par exemple, a minimisé l'influence des gouvernements du monde "réel". L'approche "cybernétique" a été quelque peu adoucie par la réforme de l'ICANN en 2002, réforme qui a permis de renforcer le rôle des gouvernements et rapprocher l'ICANN de la réalité politique.

Dans le domaine juridique, les partisans de l'approche "cybernétique" arguent que les lois existantes en matière de juridiction, de cyberdélinquance et de contrats ne peuvent pas s'appliquer à l'Internet et qu'il est donc impératif de créer de nouvelles lois.

Compte tenu de l'interaction permanente entre ces deux approches, le dilemme "vieux-réel" contre "nouveau- cybernétique" va probable-

ment continuer et fortement influencer les négociations sur la gouvernance de l'Internet.

Structure décentralisée ou centralisée de la gouvernance Internet?

De l'avis de ceux qui prônent une approche décentralisée, la structure de la gouvernance devrait traduire la nature même de l'Internet: un réseau de réseaux. Un agencement aussi complexe ne saurait être placé sous un organisme de tutelle unique, comme une organisation internationale. Un autre argument soutient que l'absence de gouvernance centralisée est l'un des principaux facteurs à l'origine de la forte croissance de l'Internet. Cet avis est principalement partagé par la communauté technique de l'Internet et les pays industrialisés.

Une approche centralisée, quant à elle, est en partie basée sur les difficultés pratiques qu'éprouvent les pays ayant des ressources humaines et financières limitées pour suivre les débats sur la gouvernance de l'Internet dans un contexte multi-institutionnel fortement décentralisé. Ces pays ont beaucoup de mal à assister aux réunions organisées dans les principaux centres diplomatiques (Genève, New York), sans parler du suivi des activités des autres institutions, telles que l'ICANN, W3C et l'IETF. Les partisans de cette approche centralisée, principalement des pays en développement, plaident pour une "boutique tout-en-un", qui relèverait de préférence du cadre d'une organisation internationale.

L'Internet et l'intérêt public

L'essentiel des infrastructures techniques par lesquelles passe le trafic Internet appartient à des sociétés publiques ou privées, le plus souvent des opérateurs de télécommunications. Ceci n'est pas sans rappeler une compagnie maritime assurant le transport de conteneurs. Toutefois, les voies maritimes sont ouvertes et réglementées par le droit de la mer, qui stipule que le grand large est res communis omnium (une chose qui appartient à tout le monde), alors que les dorsales du réseau sur lequel transitent les données sont la propriété des sociétés de télécommunications. Cet état de fait soulève un certain nombre de questions:

- Peut-on demander à des sociétés privées de gérer leur propriété privée - les dorsales de l'Internet - dans l'intérêt public?
- L'Internet, en tout ou partie, peut-il être considéré comme un bien public universel?

- Le vieux concept romain de res communis omnium peut-il s'appliquer à l'Internet comme c'est le cas avec certains éléments du droit de la mer?

Le principal défi dans ce dilemme public/privé consistera, d'un côté, à fournir au secteur privé un environnement commercial adéquat, mais, d'un autre côté, à veiller à la poursuite du développement de l'Internet comme ressource publique, composée de fonds communs de savoir et d'information. Pour en savoir plus, veuillez vous reporter à la page 131.

La géographie et l'Internet

L'une des hypothèses initiales concernant l'Internet était qu'il surmontait les frontières nationales et érodait le principe de souveraineté. Dans sa célèbre "Déclaration d'Indépendance du cyberespace", John Perry Barlow envoyait le message suivant à tous les gouvernements: "Vous n'êtes pas les bienvenus parmi nous. Vous n'avez aucune souveraineté sur le territoire où nous nous rassemblons. Vous n'avez aucun droit moral de nous gouverner et vous ne possédez aucun moyen de faire respecter votre autorité que nous ayons de bonnes raisons de craindre. Le cyberespace ne se trouve pas à l'intérieur de vos frontières".

Cette déclaration est un exemple du techno-optimisme général caractéristique du milieu de années quatre-vingt-dix. Depuis la déclaration de Barlow, il y a eu bien des développements, y compris des logiciels de géolocalisation plus sophistiqués. Aujourd'hui, il est encore difficile d'identifier précisément qui se tient derrière l'écran mais il est relativement aisé de détecter quel fournisseur d'accès a servi à accéder l'Internet. En outre, aux quatre coins du monde, les législations nationales les plus récentes exigent des fournisseurs d'accès qu'ils identifient leurs utilisateurs et, le cas échéant, qu'ils communiquent aux autorités les informations requises à leur sujet.

Au plan géographique, plus l'Internet aura de points d'ancrage, moins sa gouvernance sera unique. Ainsi par exemple, avec la possibilité de localiser l'emplacement géographique des internautes et de leurs transactions, la question complexe de juridiction sur l'Internet devient plus facile à résoudre par le biais des lois existantes.

Prêcher par l'exemple

L'approche qui consiste à prêcher par l'exemple encourage l'utilisation d'outils en ligne pour la négociation de questions liées à l'univers cyber-

nétique. Le processus de négociation de la gouvernance de l'Internet présente un défi considérable en matière de diplomatie multilatérale, qui fait appel à l'usage de techniques de négociations éprouvées et efficaces et à l'introduction d'approches novatrices. L'une des principales techniques novatrices pourrait être l'usage d'outils en ligne dans le cadre des négociations.

Les négociations à partir de l'Internet devraient faciliter la participation d'un groupe plus large de parties prenantes, notamment celles qui ne peuvent pas se permettre d'assister aux conférences diplomatiques traditionnelles. Une priorité consistera à aider les pays en développement à participer de façon véritable au processus de négociation de la gouvernance de l'Internet.

PRINCIPES DIRECTEURS

Les principes directeurs représentent certaines valeurs et certains intérêts qu'il convient de promouvoir par le biais du régime émergent de gouvernance de l'Internet. Certains de ces principes ont été adoptés par le SMSI, tels que la transparence et l'intégration. D'autres ont été introduits, le plus souvent de façon tacite, par le biais de débats sur la gouvernance de l'Internet.

"Ne pas réinventer la roue"

Toute initiative dans le domaine de la gouvernance de l'Internet devrait prendre comme point de départ la réglementation existante, laquelle peut se diviser en trois grands groupes:

a) les règles qui ont été inventées pour l'Internet (par ex. l'ICANN);
b) les règles qui nécessitent des amendements considérables pour s'attaquer aux enjeux liés à l'Internet (par ex. la protection des marques de fabrique, la fiscalité du commerce électronique);
c) les règles qui peuvent s'appliquer à l'Internet sans amendement significatif (par ex. la protection de la liberté d'expression).

L'utilisation des règles existantes augmenterait sensiblement la stabilité juridique et réduirait la complexité de l'élaboration du régime de gouvernance de l'Internet.

"Si ce n'est pas cassé, inutile de réparer!"

La gouvernance de l'Internet doit maintenir la fonctionnalité et la robustesse actuelles de l'Internet; dans le même temps, elle se doit de rester suffisamment flexible pour adopter des changements débouchant sur une fonctionnalité accrue et une légitimité renforcée. Un consensus reconnaît que la stabilité et la fonctionnalité de l'Internet devraient figurer parmi les principes directeurs de la gouvernance de l'Internet. La stabilité de l'Internet devrait être préservée par le biais de l'approche initiale de l'Internet, à savoir une "règle évolutive" qui implique l'introduction progressive de changements éprouvés dans l'infrastructure technique.

Toutefois, certains acteurs craignent que l'adoption du slogan "Si ce n'est pas cassé, inutile de réparer" ne fournisse une immunité totale contre toute modification du régime actuel de gouvernance de l'Internet, y compris des changements n'ayant pas nécessairement trait à 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 décisions).

La gouvernance de l'Internet et le développement

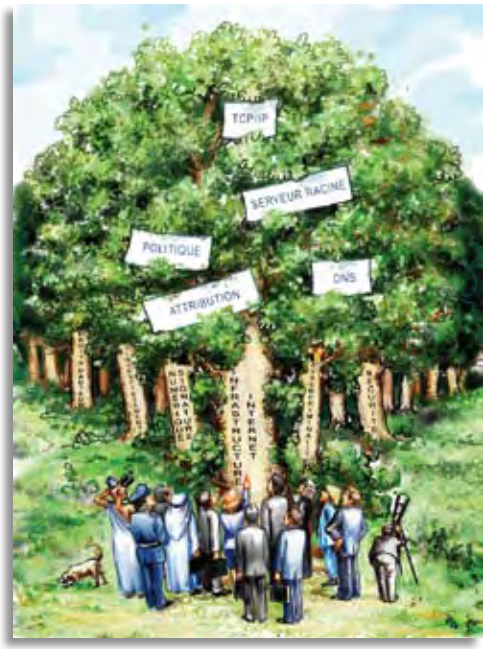
Le débat actuel sur la gouvernance de l'Internet met en exergue la très grande pertinence pour le développement que revêtent les questions liées à la gouvernance de l'Internet, à savoir: les frais d'interconnexion, la distribution d'adresses IP, les investissements, la protection de la propriété intellectuelle et la promotion du commerce électronique. Le processus de gouvernance de l'Internet devrait être guidé par les objectifs globaux du SMSI en matière de développement et les objectifs du Millénaire pour le développement prescrits par les Nations Unies.

Promotion d'une approche holistique et définition de priorités

Une approche holistique devrait permettre de s'atteler aux aspects du développement de l'Internet qui touchent à des questions techniques mais aussi à des considérations juridiques, sociales, économiques et liées au développement. Cette approche devrait aussi prendre en compte la convergence croissante des technologies numériques, y compris la migration des services de télécommunications vers des protocoles Internet.

Tout en maintenant une approche holistique à l'égard des négociations relatives à la gouvernance de l'Internet, les parties prenantes devraient

identifier les questions qu'ils considèrent comme prioritaires en fonction de leurs intérêts propres. Ni les pays en développement ni les pays industrialisés ne forment des groupes homogènes. Au sein des pays en développement, il existe des différences considérables en termes de priorités, de niveau de développement et d'aptitude à l'informatique (par ex. l'écart qui existe entre des pays avancés du point de vue des TIC comme l'Inde, la Chine et le Brésil et certains pays les moins avancés d'Afrique subsaharienne).



"Les arbres qui cachent la forêt"

A holistic approach and prioritisation of the Internet Governance agenda should help stakeholders from both developed and developing countries to focus on a particular set of issues. This should lead towards more substantive and, possibly, less politicised negotiations. The stakeholders would group around issues rather than around the traditional highly politicised division-lines (e.g. developed - developing countries, governments - civil society).

PRINCIPES DIRECTEURS DE L'ICANN

Le livre blanc des Etats-Unis sur la gouvernance de l'Internet (1998) stipule les principes directeurs suivants pour l'établissement de l'ICANN:

- Stabilité: le fonctionnement de l'Internet ne doit pas être perturbé, notamment dans l'opération de ses structures cruciales, y compris les "domaines racines";
- Concurrence: il est important d'encourager la créativité et la flexibilité, qui seront propices à la poursuite du développement de l'Internet;
- Prise de décisions: le nouveau système devrait tenir compte de certains des principes et règlements initiaux de l'Internet, y compris une organisation de type communautaire, un caractère ouvert, etc.;
- Représentativité: le nouveau cadre devrait accueillir les principales parties prenantes, aussi bien au plan géographique (les différents pays) qu'au plan professionnel (les différentes communautés professionnelles).

Transformer des solutions techniques implicites en principes politiques explicites

La communauté des internautes s'accorde généralement pour dire que certaines valeurs sociales, telles que la liberté de communication, se trouvent facilitées par la manière dont l'Internet est techniquement conçu (le principe de "bout en bout"). Ce point de vue pourrait déboucher sur une conclusion erronée selon laquelle les solutions technologiques suffisent à promouvoir et protéger les valeurs sociales. Les tout derniers développements dans le domaine de l'Internet, tels que l'utilisation des technologies pare-feu pour restreindre le flux d'informations, prouvent que la technologie peut être utilisée de multiples façons, qui peuvent sembler contradictoires. Des principes comme la liberté de communication devraient être clairement énoncés au niveau politique, et non présumés de façon implicite au niveau technique.

Le principe de la neutralité technologique

Ce principe est étroitement lié au précédent. La neutralité technologique veut que la politique ne dépende pas d'un dispositif technique ou technologique spécifique. Ainsi par exemple, la réglementation relative à la protection de la vie privée devrait stipuler ce qu'il convient de protéger (par ex. les données personnelles, les registres de santé), et non la méthode de protection (par ex. en réglementant l'accès aux bases de données, par crypto-protection, etc.).

La neutralité technologique offre plusieurs avantages du point de vue de la gouvernance. Tout d'abord, elle dissocie la gouvernance de toute technologie particulière, de sorte qu'elle est prête à accueillir les développements technologiques futurs. De surcroît, la neutralité technologique est le principe réglementaire qui convient le mieux à la convergence future des principales technologies (télécommunications, médias, Internet, etc.).

L'Union européenne a introduit la neutralité technologique comme l'une des pierres angulaires de sa politique des télécommunications. Si la neutralité technologique est manifestement un principe approprié, on peut entrevoir de nombreuses difficultés dans le cadre du passage de la réglementation existante des télécommunication vers de nouvelles. Ces problèmes se font déjà sentir dans des domaines tels que la téléphonie sur Internet.

Le risque de déshumaniser la gestion de la société

Un aspect primordial de la relation entre la technologie et la politique a été identifié par Lawrence Lessig, qui observait que, du fait de sa dépendance croissante à l'égard de l'Internet, la société moderne pourrait finir par être réglementée par un code logiciel et non plus par des lois. Certaines fonctions législatives du parlement et du gouvernement pourraient de facto être assumées par des sociétés informatiques et des éditeurs de logiciels. Par le jeu d'un panachage de solutions logicielles et techniques, éditeurs et sociétés seraient en mesure d'influencer la vie dans des sociétés de plus en plus basées sur l'Internet. Si jamais la société venait à être gérée par un code et non plus par des lois, cela bouleverserait radicalement le fondement même de l'organisation politique et juridique de la société moderne.

ANALOGIES

> Si l'analogie est bien souvent trompeuse, c'est la chose la moins trompeuse que nous ayons.
>
> *Samuel Butler*

L'analogie nous aide à appréhender les nouveaux développements à partir de ce que nous connaissons déjà. Dresser des parallèles entre des exemples passés et présents, malgré les risques inhérents, constitue un processus mental primordial en droit comme en politique. La plupart des affaires juridiques ayant trait à l'Internet sont résolues en ayant recours à des analogies.

L'usage d'analogies dans la gouvernance de l'Internet présente toutefois quelques limitations importantes. Tout d'abord, l'Internet est un terme très vaste, qui englobe toute une variété de services, y compris le courrier électronique (voir l'analogie à la téléphonie), le Web (voir l'analogie aux services de diffusion - la télévision) et les bases de données (voir l'analogie à une bibliothèque). Une analogie à un système particulier peut parfois simplifier à l'extrême notre entendement de l'Internet.

Deuxièmement, avec la convergence croissante des différents services de télécommunications et des médias, les différences traditionnelles entre eux tendent à s'estomper. Ainsi par exemple, avec l'introduction du service Voix sur IP, il est de plus en plus difficile de faire une distinction entre l'Internet et la téléphonie.

Malgré ces facteurs limitatifs, les analogies restent de puissants alliés et le principal outil cognitif pour résoudre les affaires juridiques et élaborer un

régime de gouvernance de l'Internet. Certaines des analogies les plus fréquemment utilisées sont abordées ci-dessous.

L'Internet et la téléphonie

Similitudes: au tout début de l'Internet, cette analogie était influencée par le fait que le téléphone servait à l'accès par ligne commutée. De surcroît, il existe une analogie fonctionnelle entre le téléphone et l'Internet (courrier électronique et clavardage ou chat), les deux étant des moyens de communication directe et personnelle.

Une analogie plus récente entre le téléphone et l'Internet met l'accent sur l'utilisation possible du système de numérotation de la téléphonie en guise de solution pour l'organisation du système de noms de domaine.

Différences: l'Internet utilise des paquets et non des circuits comme le fait le téléphone. A la différence de la téléphonie, l'Internet ne peut pas garantir ses services; il peut uniquement garantir de "tout mettre en oeuvre". L'analogie ne met en exergue qu'un seul aspect de l'Internet: la communication par courrier électronique ou par clavardage. D'autres applications Internet primordiales, comme le World Wide Web, les services interactifs, etc. n'ont rien de commun avec la téléphonie.

Utilisée par: ceux qui s'opposent à la réglementation du contenu de l'Internet (principalement aux Etats-Unis). Si l'Internet était analogue au téléphone, la teneur des communications Internet ne pourrait pas être contrôlée, comme c'est le cas avec le téléphone.

Cette analogie est également employée par ceux qui soutiennent que l'Internet devrait être régi comme les autres systèmes de communication (par ex. téléphonie, services postaux), par les autorités nationales en attribuant un rôle coordonnateur à des organisations internationales comme l'UIT.

L'Internet et le courrier/ les services postaux

Similitudes: il existe une analogie en termes de fonction, à savoir la fourniture de messages. A lui seul, le nom "courriel" ou courrier électronique souligne cette similitude.

Différences: cette analogie ne couvre toutefois qu'un seul service Internet - le courrier électronique. En outre, les services postaux ont une structure intermédiaire beaucoup plus sophistiquée entre l'émetteur et le destinataire du courrier que le système électronique, où la fonction intermédiaire est simplement assurée par un fournisseur d'accès à l'Internet ou

par un prestataire de service de courrier électronique comme Yahoo! ou Hotmail.

Différences: cette analogie ne couvre toutefois qu'un seul service Internet - le courrier électronique. En outre, les services postaux ont une structure intermédiaire beaucoup plus sophistiquée entre l'émetteur et le destinataire du courrier que le système électronique, où la fonction intermédiaire est simplement assurée par un fournisseur d'accès à l'Internet ou par un prestataire de service de courrier électronique comme Yahoo! ou Hotmail.

> Le Président de l'ICANN, Paul Twomy, a eu recours à l'analogie suivante entre le système postal et la fonction de l'ICANN: "Si l'on assimile l'Internet à un bureau de poste ou à un système postal, en gros le nom de domaine et l'adresse IP sont des moyens de garantir que l'adresse qui figure sur l'enveloppe fonctionne bien. Il ne s'agit en rien de ce qui se trouve à l'intérieur de l'enveloppe, de qui envoie l'enveloppe, de qui est autorisé à lire le contenu de l'enveloppe, de combien de temps il faut pour que l'enveloppe arrive à destination, ni du prix de l'enveloppe. Aucune de ces questions ne sont importantes pour les fonctions de l'ICANN. Sa fonction consiste purement à veiller à ce que l'adresse fonctionne bien."

Les familles des soldats américains morts en Irak ont également tenté d'exploiter l'analogie entre le courrier postal (lettres) et le courrier électronique afin de gagner accès aux messages électroniques et blogues privés de leurs chers défunts, arguant qu'elles devraient pouvoir en hériter tout comme elles auraient pu le faire s'il s'était agi de lettres et de journaux intimes.

Les fournisseurs d'accès à l'Internet ont éprouvé beaucoup de difficultés à traiter de ce problème fortement émotif. Au lieu d'accepter d'emblée l'analogie entre les lettres et le courrier électronique, la plupart des fournisseurs d'accès ont refusé l'accès aux familles en invoquant l'accord de confidentialité passé avec leurs utilisateurs.

L'Internet et la télévision

Similitude: au départ, l'analogie était liée à la ressemblance visuelle entre un moniteur d'ordinateur et un écran de télévision. Une analogie plus sophistiquée s'inspire de l'utilisation des deux médias - le Web et la télé - à des fins de diffusion.

Différences: tout comme dans le cas de la téléphonie, l'Internet renferme un concept plus vaste que la télévision. Abstraction faite de la similitude entre un moniteur d'ordinateur et un écran de télévision, il existe des différences structurelles fondamentales entre les deux appareils. Une télévision est un support de diffusion d'un individu vers un grand nombre

de téléspectateurs, alors que l'Internet permet de nombreux types de communication différents (d'un individu à un autre, d'un individu à plusieurs, de plusieurs individus à plusieurs autres).

Utilisée par: cette analogie est adoptée par ceux qui souhaite introduire un contrôle plus strict du contenu de l'Internet. A leurs yeux, du fait de son pouvoir en guise d'outil médiatique des masses comparable à celui de la télévision, l'Internet devrait être strictement réglementé. Le gouvernement américain a tenté d'employer cette analogie dans l'affaire retentissante "Reno c. ACLU". Cette affaire reposait sur la Loi américaine sur la décence des communications passée par le Congrès qui prévoit un contrôle très strict du contenu afin d'empêcher que les enfants ne soient exposés à du matériel pornographique par le biais de l'Internet. Le tribunal a refusé de reconnaître l'analogie avec la télévision.

L'Internet et les bibliothèques

Similitudes: l'Internet est parfois perçu comme un vaste fonds documentaire et le terme de "bibliothèque" est souvent utilisé pour le décrire - "gigantesque bibliothèque numérique", "cyber-bibliothèque," "Bibliothèque alexandrine du 21ème siècle", etc.

Différences: le stockage de l'information et des données n'est qu'un seul aspect de l'Internet et il existe des différences majeures entre les bibliothèques et l'Internet:

a) les bibliothèques classiques entendent servir des particuliers qui résident dans un lieu donné (ville, pays, etc.), alors que l'Internet est mondial;
b) les livres, articles et journaux sont publiés suivant des procédures permettant de garantir leur qualité (éditeurs). L'Internet n'a pas d'éditeurs;
c) les bibliothèques sont organisées selon des schémas précis de classification, qui permettent à leurs usagers de trouver un livre particulier dans leur collection. Hormis quelques catalogues ou annuaires comme celui de Yahoo! et Google qui ne couvrent qu'une infime fraction des informations disponibles sur l'Internet, ce schéma de classification n'existe pas sur l'Internet;
d) Hormis une description par mots clés, le contenu d'une bibliothèque (texte figurant dans des livres et des articles) n'est accessible qu'une fois qu'un usager emprunte un ouvrage donné. Le contenu de l'Internet est immédiatement accessible par le biais des moteurs de recherche.

Utilisée par: différents projets qui entendent créer un vaste système détaillé d'informations et de connaissances sur des questions précises (portails, bases de données, etc.).

L'Internet et les magnétoscopes ou photocopieuses

Similitudes: cette analogie est axée sur la reproduction et la dissémination du contenu (par ex. les textes et les livres). Les ordinateurs ont simplifié la fonction de reproduction par l'opération "copier-coller". A son tour, celle-ci a nettement simplifié la dissémination de l'information par le biais de l'Internet.

Différences: l'ordinateur a une fonction beaucoup plus vaste que la simple copie de documents, bien que l'opération de copie soit beaucoup plus simple sur l'Internet qu'avec un magnétoscope ou une photocopieuse.

Utilisée par: cette analogie a été appliquée dans le contexte de la "Loi américaine sur la protection des droits d'auteur du millénaire numérique" (DMCA), qui pénalise les institutions qui contribuent à la violation des droits d'auteur (édition de logiciel permettant de surmonter les dispositifs de protection des droits d'auteur, etc.). Le contre-argument dans de tels cas tient au fait que les éditeurs de logiciel, tout comme les fabricants de magnétoscopes et de photocopieuses, ne peuvent pas prédire si leurs produits seront utilisés de façon illégale. Cette analogie est utilisée dans des procès intentés à l'encontre d'éditeurs de programmes de type Napster pour l'échange de fichiers entre particuliers (P2P), comme Grokster et StreamCast.

L'Internet et l'autoroute

Similitudes: cette analogie est née de la culture américaine et de l'importance qu'elle attache aux autoroutes et aux liaisons ferroviaires, révélant ainsi la fascination nationale exercée par la découverte de nouvelles contrées et de nouvelles frontières.

Différences: hormis l'aspect lié au transport de l'Internet, il n'existe pas d'autres similitudes entre l'Internet et les autoroutes. L'Internet déplace des choses incorporelles (des données) alors que les autoroutes facilitent l'acheminement de personnes et de marchandises.

Utilisée par: l'analogie avec l'autoroute a été très communément utilisée au milieu des années quatre-vingt-dix lorsqu'Al Gore a introduit le concept "d'autoroute de l'information". Le terme "d'autoroute" a également été utilisé par le gouvernement allemand afin de justifier l'introduction d'une lé-

gislation plus stricte pour le contrôle du contenu de l'Internet en juin 1997: "Il s'agit d'une loi libérale qui n'a rien à voir avec la censure mais qui énonce clairement les conditions dans lesquelles les fournisseurs de services peuvent ou ne peuvent pas faire certaines choses. L'Internet est un moyen qui permet de véhiculer et de transmettre des connaissances... comme dans le cas des autoroutes, il faut établir des lignes directrices pour les deux types de trafic."

LA CLASSIFICATION DES ENJEUX DE LA GOUVERNANCE DE L'INTERNET

La gouvernance de l'Internet est un nouveau domaine complexe qui exige une cartographie et une classification conceptuelles initiales. La complexité de la gouvernance de l'Internet est liée à sa nature multidisciplinaire, qui englobe toute une variété d'aspects, y compris la technologie, l'économie sociale, le développement, le droit et la politique.

Le besoin d'une cartographie initiale de la gouvernance de l'Internet est à la fois académique et pratique. Au plan académique, il est produit un volume croissant de recherche sur la gouvernance de l'Internet mais ces travaux sont principalement axés sur l'ICANN et sur d'autres enjeux qui relèvent de ce qu'on peut appeler une approche "étroite" de la gouvernance de l'Internet. Il manque toujours un cadre théorique plus large, en particulier pour ce qui concerne les aspects internationaux de la gouvernance de l'Internet. Le besoin pratique de classification a été clairement démontré durant le processus SMSI. Nombre d'acteurs, y compris des Etats nations, ont eu du mal à saisir la complexité de la gouvernance de l'Internet. Une cartographie conceptuelle du domaine permettrait d'évoluer vers des négociations plus efficaces dans le contexte du SMSI tout comme dans d'autres processus de négociations multilatérales sur des questions ayant trait à l'Internet.

Une classification pourrait aider les acteurs de la gouvernance de l'Internet dans les domaines suivantes:

- identifier de manière plus précise les principaux enjeux à négocier;
- réduire le "bruit de fond" dans les négociations, provoqué par une interprétation disparate des principaux concepts;
- éviter de dupliquer les efforts en s'attaquant aux mêmes questions dans de multiples enceintes;

- préserver un équilibre adéquat entre une perspective plus large et des questions spécifiques, en évitant ainsi le problème des "arbres qui cachent la forêt".

En fin de compte, une cartographie rigoureuse des enjeux de l'Internet devrait rendre plus performant le processus de négociation de la gouvernance de l'Internet. D'un point de vue économique, cela devrait réduire le coût de transaction - en d'autres termes, réduire le temps total passé à négocier. Ceci présenterait un avantage tout particulier pour les pays ayant des ressources humaines et financières limitées en leur permettant une participation renforcée. Des processus de négociation confus et flous nécessitent des ressources humaines excessivement lourdes et davantage de temps.

La classification de la gouvernance de l'Internet adoptée par Diplo regroupe tous les enjeux en cinq grands domaines de classification. S'efforçant d'aligner la terminologie au monde de la diplomatie, Diplo a retenu le terme "corbeille" pour signifier ces grands domaines. (Le terme "corbeille" a été introduit dans la pratique diplomatique dans le cadre des négociations de l'Organisation pour la sécurité et la coopération en Europe - OSCE). Les cinq corbeilles suivantes ont été retenues depuis 1997, lorsque Diplo a démarré l'élaboration d'un schéma de classification:

1) infrastructure et normalisation;
2) législation;
3) économie;
4) développement;
5) aspects socioculturels.

La classification de Diplo en matière de gouvernance de l'Internet est la base conceptuelle de l'approche globale adoptée par Diplo dans ce domaine, y compris en termes de formation/éducation, recherche et développement d'outils. Depuis son introduction en 1997, la classification a été utilisée lors de cours auxquels ont participé plus de 300 étudiants et par de nombreux chercheurs. Des réactions périodiques à ce schéma de classification servent de base à des ajustements permanents. Par conséquent, la classification actuelle est fondée sur de nombreuses itérations et sur un cumul de connaissances et d'expériences.

Le modèle à cinq corbeilles est représenté comme une métaphore par le biais de l'illustration "Bâtiment en construction" à la page suivante.

GOUVERNANCE DE LA SOCIÉTÉ
DE L'INFORMATION
ÉDUCATION
SOCIO
CULTUREL
MULTILINGUISME
ÉCONOMIQUE
TRANSFERT DE TECHNOLOGIES
FISCALITÉ
SAVOIR FAIRE
DÉVELOPPEMENT
PROTECTION DES DONNÉES
DROIT DU TRAVAIL
HACKING
IDENTITÉ
CYBER
JURIDICTION
JURIDIQUE
DROITS D'AUTEUR
INTERFACES DE CONNEXION
XSLT
HTML
XML
SMTP
TCP/IP
DNS
FTP
CRYPTAGE
COURRIEL
INTEROPÉRABILITÉ
INFRASTRUCTURE ET NORMES
SITE EN CONSTRUCTION PAR
UNESCO
OCDE
OMC
ONG

"Bâtiment en construction": la gouvernance de l'Internet - Sommes-nous en train de construire la tour de Babel du 21ème siècle?

Un tableau de Bruegel l'Ancien (1563), exposé au Kunsthistorisches Museum de Vienne, dépeint la construction de la tour de Babel. (Un autre, de moindre taille, réalisé la même année et sur le même thème est exhibé au Boijmans Van Beuningen Museum à Rotterdam). Le livre de la Genèse (11.7) évoque la construction de la tour de Babel: "Allons! Descendons, et là confondons leur langage afin qu'ils n'entendent plus la langue, les uns les autres."

L'analogie avec la construction de la tour de Babel semble tout à fait appropriée lorsque l'on considère les défis que soulève l'Internet. Cette comparaison a incité les auteurs à se pencher sur un autre bâtiment en construction - non pas un destiné à gagner les cieux mais un se bornant à atteindre chaque résident de la planète. Diplo a élaboré un cadre de discussion de la gouvernance de l'Internet, illustré par le tableau représenté à la page précédente. Chaque étage de ce bâtiment est abordé dans les chapitres qui suivent. Il est important de comprendre que tous les étages du bâtiment sont interconnectés et que la construction est un processus permanent et éternel.

SECTION 2

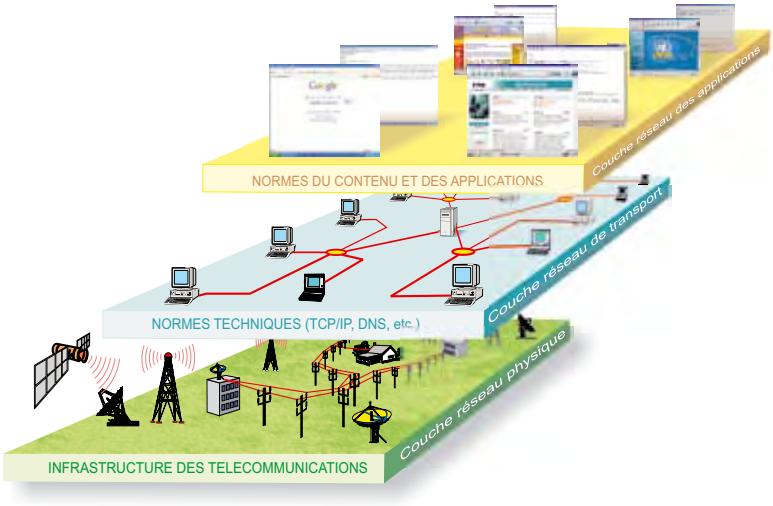
La corbeille infrastructure et normalisation

LA CORBEILLE INFRASTRUCTURE ET NORMALISATION

La corbeille infrastructures et normalisation englobe les enjeux élémentaires, à caractère principalement technique, associés au fonctionnement de l'Internet. Dans l'illustration de la gouvernance de l'Internet "Bâtiment en construction" adoptée par Diplo, le rez-de-chaussée représente les infrastructures et la normalisation (voir page 28).

Les enjeux de cette corbeille se divisent en deux groupes. Le premier, qui comprend les questions primordiales sans lesquelles l'Internet et le World Wide Web ne pourraient pas exister, est représenté par les trois strates suivantes:.

1. les infrastructures de télécommunications, par le biais desquelles transite tout le trafic Internet
2. les normes et services techniques (les infrastructures qui permettent à l'Internet de fonctionner (par ex. TCP/IP, DNS, SSL); et



L'une des forces de l'Internet réside dans son architecture stratifiée. La couche concernant les infrastructures de l'Internet demeure indépendante de la couche des infrastructures de télécommunications (la couche au-dessous) et de celle des normes applicatives (la couche au-dessus).

3. le normes régissant le contenu et les applications (par ex. HTML, XML).

Le deuxième groupe renferme les questions associées à la sauvegarde d'un fonctionnement sûr et stable des infrastructures de l'Internet, y compris la sécurité Internet, le cryptage et le pollupostage.

LES INFRASTRUCTURE DE TELECOMMUNICATIONS

LA SITUATION ACTUELLE

Les données Internet peuvent circuler par le biais d'une foule de supports de communication: fils téléphoniques, câbles à fibres optiques, satellites, microondes et liaisons sans fil. Même le réseau électrique de base peut servir à relayer le trafic Internet. L'essor rapide de l'Internet a déclenché une augmentation notable des capacités de télécommunications. Il est estimé que depuis 1998, la capacité des télécommunications a été multipliée par 500 sous l'effet conjugué de l'innovation technologique et des investissements dans de nouvelles installations de télécommunications.

Compte tenu du fait que la couche des télécommunications assure le transit du trafic Internet, toute nouvelle réglementation affectant les télécommunications aura immanquablement un impact sur l'Internet. Les infrastructures des télécommunications sont réglementées à l'échelon national et international par une variété d'organismes publics et privés.

De par tradition, les télécommunications internationales ont été coordonnées par l'Union internationale des télécommunications (UIT), qui a élaboré des règles sophistiquées régissant les relations entre les opérateurs nationaux, la gestion du spectre des fréquences radioélectriques et des orbites de satellites.

Finalement, l'approche libérale a eu gain de cause sur les monopoles des télécommunications. Le processus de libéralisation a été officialisé à l'échelle internationale en 1998 par le biais d'un Accord sur les télécommunications de base (ATB) de l'Organisation mondiale du commerce (OMC). Suite à l'adoption de l'ATB, plus de 100 pays ont entamé un processus de libéralisation, caractérisé par la privatisation des mo-

nopoles nationaux de télécommunications, l'introduction de la concurrence et la création d'organismes nationaux de régulation.

L'OMC s'est progressivement immiscée au coeur du régime des télécommunications internationales, traditionnellement gouvernées par l'UIT. Pourtant, les rôles de l'OMC et de l'UIT sont très différents. L'UIT définit des normes techniques détaillées, des réglementations internationales propres au secteur des télécommunications et fournit une aide aux pays en développement. L'OMC offre un cadre pour l'établissement de règles générales du marché.

La Réglementation internationale de l'UIT, à compter de 1988 facilitait la libéralisation internationale des prix et des services et permettait une utilisation plus novatrice des services de base, tels que les lignes internationales louées, dans le domaine de l'Internet.

Suite à la libéralisation, le quasi-monopole de l'UIT, en tant que principale institution chargée de la définition de normes dans le secteur des télécommunications, s'est trouvé érodé par d'autres organes et agences professionnels, tels que le European Telecommunications Standardisation Institute (ETSI), qui a mis au point la norme GSM, le European Telecommunications Standardisation Institute (IEEE), qui a élaboré la norme WiFi et le (Internet Engineering Task Force (IETF), qui a élaboré le protocole TCP/IP et bien d'autres propres à l'Internet.

La libéralisation des marchés nationaux des télécommunications a permis aux grosses entreprises de télécommunications, comme AT&T, Cable and Wireless, France Telecom, Sprint et WorldCom d'élargir leur couverture du marché à l'échelle mondiale. Compte tenu du fait que l'essentiel du trafic Internet passe par les infrastructures de télécommunications de ces sociétés, elles ont une influence de poids sur la gouvernance de l'Internet.

LES ENJEUX

Le "dernier kilomètre" - Dégroupement des boucle locales

La "boucle locale" (ou "dernier kilomètre") est la connexion entre les fournisseurs de service Internet et leurs clients individuels. Les problèmes liés aux "boucles locales" font obstacle à l'utilisation plus généralisée de l'Internet dans bon nombre de pays, pour l'essentiel en développement. Ceci s'explique généralement par un réseau national des télécommunications sous-développé. Dans certains pays en développement avec de vastes territoires, il est difficile de connecter des villes et villages re-

culés par le biais des liaisons traditionnelles de télécommunications terrestres.

La communication sans fil s'impose de plus en plus comme la meilleure solution à bas prix du problème que pose la "boucle locale". Outre les options techniques qui se multiplient, la solution du problème de la "boucle locale" dépend aussi de la libéralisation de ce segment du marché des télécommunications.

La libéralisation des marchés des télécommunications

Un nombre important de pays ont libéralisé leurs marchés des télécommunications. Toutefois, bon nombre de pays en développement ayant encore un monopole des télécommunications sont confrontés à un choix délicat: comment libéraliser les marchés des télécommunications et les rendre plus performants tout en préservant l'importante source de revenu budgétaire que constituent les monopoles existants des télécommunications.

L'aide étrangère, une transition progressive et l'association du processus de libéralisation à la protection de l'intérêt public sont autant d'options qui ont été mises en avant pour résoudre cette question complexe.

Technologie, normes et politiques

Le débat concernant les protocoles de réseau illustre en quoi les normes peuvent être une autre forme de politique. Alors que d'autres interventions des pouvoirs publics dans le monde de la technologie et des affaires (par ex. les réglementations en matière de sécurité et les mesures antitrust) sont très vite perçues comme ayant une signification politique et sociale, les normes techniques sont généralement supposées être socialement neutres et par conséquent n'avoir qu'un intérêt historique fort modeste. Or, les décisions techniques peuvent avoir des conséquences économiques et sociales de grande portée, capables de modifier l'équilibre des pouvoirs entre des sociétés ou des nations rivales et de brider la liberté des utilisateurs. Les efforts déployés afin de créer des normes officielles placent les décisions techniques privées des architectes de système dans le domaine public; de cette façon, la bataille des normes peut faire la lumière sur des présomptions tacites et des conflits d'intérêt latents. La passion manifeste avec laquelle les parties prenantes contestent les décisions liées aux normes devrait nous alerter sur la signification plus profonde qui se cache derrière les aspects pratiques du problème. (Source: Janet Abbate Inventing the Internet, MIT Press)

L'établissement de normes techniques d'infrastructures

TLes normes techniques sont de plus en plus souvent établies par des organismes privés et professionnels. Ainsi par exemple, la norme WiFi, IEEE 802.11b, a été mise au point par le Institute of Electrical and Electronics Engineers (IEEE). La certification du matériel compatible avec la norme WiFi incombe à la WiFi Alliance. Le fait même qu'elles soient chargées d'établir ou de mettre en oeuvre des normes dans un marché qui connaît un rapide essor confère à ces institutions une influence considérable sur le marché.

NORMES ET SERVICES TECHNIQUES - Les infrastructures de l'Internet

C'est sur cette couche que l'Internet prend forme. La plupart des questions qui y sont liées sont les enjeux primordiaux de la gouvernance de l'Internet, généralement recensés dans une définition "étroite" de la gouvernance de l'Internet. Elles sont divisées en deux groupes. Le premier comprend les questions primordiales associées aux normes et services techniques: TCP/IP, DNS et serveurs racines alors que le deuxième cou-

Vues divergentes à propos du rôle de l'ICANN dans la gouvernance de l'Internet

VUE ETROITE - TECHNIQUE	VUE LARGE - POLITIQUE
L'ICANN est simplement un organe de coordination qui s'occupe de l'administration technique des adresses IP et des noms de domaine. Selon ce point de vue, l'ICANN se contente de coordonner, et non de régir, l'Internet. L'ICANN est simplement un organe de coordination qui s'occupe de l'administration technique des adresses IP et des noms de domaine. Selon ce point de vue, l'ICANN se contente de coordonner, et non de régir, l'Internet.	Les travaux de l'ICANN vont plus loin qu'une simple fonction de coordination technique. Si l'ICANN devrait pouvoir conserver ses responsabilités techniques fondamentales comme la gestion des serveurs racines et l'attribution des adresses IP, la politique de l'Internet devrait être définie par un organe international légitime représentant tous les Etats. Ceci pourrait être assuré soit au sein même de l'ONU soit au sein d'un cadre international nouvellement créé. Point de vue exprimé par bon nombre de pays en développement

vre les aspects commerciaux des infrastructures de l'Internet, notamment: les rôles des fournisseurs d'accès à l'Internet et des opérateurs de système Internet à fréquence porteuse à large bande ainsi que les aspects économiques de la connectivité Internet (frais de connectivité à l'Internet et points d'échange Internet).

L'ICANN est probablement l'organisme le plus fréquemment mentionné dans le cadre des débats sur la gouvernance de l'Internet. Ceci s'explique par le rôle crucial de l'ICANN dans la gestion des adresses numériques de l'Internet (adresses IP) et des systèmes de noms de domaine.

TRANSPORT CONTROL PROTOCOL/ INTERNET PROTOCOL (TCP/IP)

LA SITUATION ACTUELLE

La principale norme technique de l'Internet qui stipule comment les données sont acheminées sur l'Internet est TCP/IP, une suite de protocoles fondée sur trois principes: la commutation de paquets, la mise en réseau de bout en bout et la robustesse.

La commutation par paquets est la méthode qui sert à transmettre des données sur l'Internet. Toutes les données envoyées d'un ordinateur sont découpées en paquets qui circulent sur l'Internet et sont ensuite ré-assemblés lorsqu'ils atteignent l'ordinateur destinataire.

La notion de réseau de bout en bout met sophistication, intelligence et innovation au service d'un réseau. C'est ce principe qui a rendu possible toutes les innovations associées à l'Internet. Entre les deux extrémités, le réseau est neutre et il n'empêche pas le développement et la créativité aux deux extrémités. Cela signifie que les applications qui sont gérées sur l'Internet peuvent être conçues aux extrémités du réseau sans nécessiter l'autorisation des opérateurs de réseau ou d'un tiers quelconque.

La robustesse est assurée par le biais d'un routage dynamique. Au départ, l'ancêtre de l'Internet, ARPANET, a introduit le routage dynamique afin de développer des réseaux de défense robustes capables de résister à une attaque nucléaire éventuelle. Le routage dynamique a servi à interconnecter un ensemble divers de réseaux.

Du point de vue de la suite TCP/IP, la gouvernance de l'Internet présente deux aspects importants: a) l'introduction de nouvelles normes; et b) l'attribution d'adresses IP.

Les normes associées à la suite TCP/IP sont définies par le groupe IETF (Internet Engineering Task Force). Compte tenu de l'importance vitale que TCP/IP revêt pour l'Internet, il est soigneusement gardé par le groupe.

Une adresse IP est une adresse numérique dont doit être doté chaque ordinateur relié à l'Internet. Les adresses IP sont uniques - deux ordinateurs reliés à l'Internet ne peuvent pas avoir la même adresse IP - ce qui en fait une ressource potentiellement rare.

Le système adopté pour l'attribution des adresses IP présente une structure hiérarchique. Tout en haut de la structure se trouve l'IANA (Internet Assigned Numbers Authority - une filiale de l'ICANN), qui alloue des blocs d'adresses IP aux différents registres Internet régionaux (RIR - Regional Internet Registries).

Les RIR existants sont l'ARIN (American Registry for Internet Numbers qui couvre l'Amérique du Nord), l'APNIC (Asia Pacific Network Information Centre qui couvre l'Asie Pacifique), le LACNIC (the Latin American and Caribbean IP Address Regional Registry qui couvre l'Amérique du Sud et les Caraïbes) et le RIPE NCC (Réseaux IP Européens Network Coordination Centre - qui couvre l'Europe et le Moyen-Orient). Un registre africain, AFRINIC, est en cours d'établissement.

Les RIR allouent des adresses IP aux gros fournisseurs d'accès à l'Internet ainsi qu'aux registres d'adresses Internet locaux et nationaux. Aux échelons inférieurs, on retrouve des fournisseurs d'accès de moindre taille, des compagnies et des particuliers.

LES ENJEUX

Existe-t-il suffisamment d'adresses IP?

Sous IPv4 (protocole Internet version 4), la réserve d'adresses IP compte quelque 4 milliards d'adresses et pourrait devenir épuisée avec l'introduction d'appareils pouvant accéder à l'Internet, tels que les téléphones portables, les PDA, les consoles de jeux voire les appareils électroménagers.

La crainte de voir se tarir le nombre d'adresses IP au risque d'entraver le développement futur de l'Internet a incité la communauté des informaticiens à prendre deux mesures radicales.

- La première a été une rationalisation de l'utilisation de la réserve existante d'adresses IP, ce qui a été possible grâce à l'introduction de NAT (Network Address Translation), un système capable de connecter un réseau privé (par ex. celui d'une compagnie ou d'une université) par le biais d'une seule adresse IP. Sans NAT, chaque ordinateur d'un réseau privé aurait eu besoin d'avoir sa propre adresse IP.
- La deuxième mesure a été l'introduction d'IPv6 (une nouvelle version du protocole IP) qui offre un nombre beaucoup plus important d'adresses IP (43.000.000.000.000.000.000).

La réaction de la communauté des techniciens de l'Internet au problème posé par une pénurie potentielle d'adresses IP est un bon exemple de gestion prévoyante et dynamique. L'approche de type "deux précautions valent mieux qu'une" (que l'on appelle le "principe de précaution" dans la langue de la diplomatie de l'environnement) a été respecté même s'il était difficile de savoir avec quelle vitesse le nombre d'adresses Ipv4 serait finalement épuisé.

Toutefois, on pourrait assister à une rareté "artificielle" si ceux qui sont chargés de l'attribution des adresses IP au niveau local, par exemple les fournisseurs d'accès, décidaient d'abuser de leur pouvoir et de subordonner l'attribution à la souscription d'un autre service par exemple, ce qui affecterait à la fois la disponibilité et le prix des adresses IP.

Modifications de TCP/IP et la sécurité Internet

La sécurité n'était pas une préoccupation majeure pour les premiers développeurs de l'Internet car, à l'époque, l'Internet consistait simplement en un réseau fermé d'institutions de recherche. La sécurité était principalement assurée en limitant l'accès physique aux réseaux et aux ordinateurs connectés. Les ordinateurs étaient l'apanage d'un nombre restreint d'experts en informatique. Les données étaient échangées sans protection particulière.

Du fait de son essor, l'Internet a vu son nombre d'utilisateurs croître au-delà de toutes les attentes de sa communauté fondatrice, pour atteindre environ un milliard d'usagers à travers le monde. L'Internet est aussi devenu un outil commercial important.

Tout ceci place la question de la sécurité au premier rang de la liste des enjeux ayant trait à la gouvernance de l'Internet. La sécurité s'est progressivement renforcée par le biais de différentes solutions, le plus souvent ponctuelles. Certaines d'entre elles, comme les pare-feux, les anti-virus et les logiciels de cryptage ont été d'une efficacité considérable.

Compte tenu du fait que l'architecture de l'Internet n'avait pas été conçue dans un souci de sécurité, l'intégration de mécanismes sécuritaires intrinsèques exigera des changements substantiels dans le fondement même de l'Internet, TCP/IP. Un nouveau protocole (IPv6) offre certaines améliorations en termes de sécurité sans toutefois assurer une solution infaillible. Pour un tel niveau de protection, il faudra apporter des modifications considérables à la suite TCP/IP.

Modifications de TCP/IP et le problème d'une bande passante limitée

Pour faciliter la fourniture d'un contenu multimédia (par ex. téléphonie sur Internet ou vidéo à la demande), il est nécessaire d'assurer une qualité de service (de l'anglais Quality of Service - QoS) capable de garantir un niveau minimal de performances. QoS stipule la disponibilité (le temps utilisable), la bande passante (débit), le temps de réponse (délai) et les états d'erreur. Ceci est tout particulièrement important pour les applications sensibles aux temps de réponse, telles que les diffusions en direct. Les images figées ou au ralenti et la présence d'un écho dans la bande sonore sont les conséquences de restrictions en termes de bande passante. L'introduction de la QoS pourrait exiger des changements des protocoles Internet, y compris l'introduction d'un compromis touchant l'un des principes fondamentaux de l'Internet, le réseau de bout en bout.

EVOLUTION FUTURE POSSIBLE

On s'attend à des pressions croissantes pour modifier l'architecture de réseau actuelle de l'Internet. Certaines solutions qui visent une sécurité renforcée et une augmentation de la bande passante ne pourront être atteintes sans modifications radicales de la suite IP.

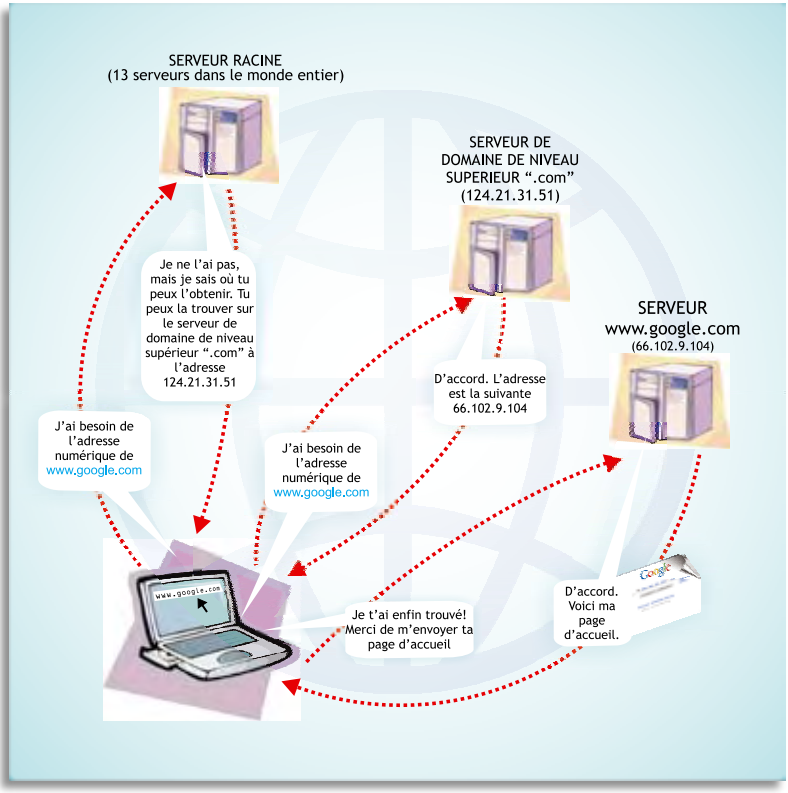
Une autre solution émergente est la construction de différentes options de réseau en plus du protocole TCP/IP actuel. Il est très probable que des sociétés privées continueront à mettre au point de telles initiatives, qui surmonteront à la fois les limites imposées par l'Internet tel qu'il existe actuellement et la réticence dont font preuve les organes de normalisa-

tion de l'Internet pour modifier les principes intrinsèques de l'Internet, tout particulièrement le "réseau de bout en bout".

LE SYSTEME DES NOMS DE DOMAINE (DNS)

LA SITUATION ACTUELLE

Le DNS gère les adresse Internet (comme www.google.com) et les convertit en adresses IP. Ainsi, pour accéder à un site Web donné, un ordinateur doit d'abord accéder à un serveur DNS. Ce serveur DNS trouve



ensuite l'adresse numérique (196.23.121.5 dans le cas de Google) du site concerné. Le DNS se compose de serveurs racines, de serveurs de domaine de niveau supérieur et d'un certain nombre de serveurs DNS répartis autour du monde. La gestion du DNS a été un sujet brûlant au cœur du débat sur la gouvernance de l'Internet. L'une des principales controverses tient à l'organisation hiérarchique du DNS et au fait que l'autorité finale appartient au gouvernement américain (par l'intermédiaire du Ministère du Commerce).

Le DNS implique deux sortes de domaines de niveau supérieur. L'un est générique; l'autre est basé sur les codes pays. Les domaines génériques de niveau supérieur (gTLD) comprennent:

- .com, .edu, .gov, .mil, et .org (en 1984);
- .net et .int (ajoutés en 1985); et
- .biz, .info, .name, .pro, .museum, .aero et .coop (ajoutés en 2000).

Pour chaque gTLD, il existe un registre qui gère une liste d'adresses. Ainsi par exemple, le gTLD ".com" est géré par VeriSign. La fonction de "commercial" est assurée par les responsables des registres. L'ICANN assure la coordination globale du système DNS en signant des accords et en agréant des registres et leurs responsables. En outre, il fixe le prix de gros auquel le registre (en l'espèce, VeriSign) "loue" les noms de domaine aux prestataires d'enregistrement et impose certaines conditions sur les services offerts par le registre et par les prestataires d'enregistrement. Cela revient à dire que l'ICANN agit comme régulateur économique et juridique du système de noms de domaine pour les gTLD.

Un élément important de la gestion des domaines concerne la protection des marques commerciales et le règlement des différends. Au tout début de l'Internet, l'enregistrement des noms de domaine était basé sur le principe du "premier arrivé premier servi" suivant lequel quiconque pouvait enregistrer n'importe quel nom.

La valeur potentielle des noms de domaine a donné naissance au phénomène que l'on appelle cybersquattage, la pratique qui consiste à enregistrer des noms de domaine susceptibles d'être revendus par la suite. L'impossibilité d'avoir deux domaines portant le même nom a débouché sur un débat sur les droits d'enregistrement. Le problème était tout particulièrement pertinent pour les noms de domaine basés sur des noms de marques célèbres (par ex. Microsoft, Nike, Toyota, Rolex).

La réforme de la gestion du DNS, avec l'adoption de la procédure UDRP (Uniform Dispute Resolution Policy), a introduit des mécanismes qui

ont sensiblement réduit l'attrait du cybersquattage. La procédure UDRP est uniquement ouverte aux domaines .com, .net et .org et elle ne couvre pas les domaines dits nationaux. La compétence de l'UDRP est reconnue dès lors qu'un particulier, une société, ou une organisation signe l'accord d'enregistrement de nom de domaine. L'UDRP présente quelques avantages pour ceux qui souhaitent faire opposition à des noms précédemment enregistrés, habituellement les titulaires de marques commerciales traditionnelles; parmi ceux-ci on peut citer la résolution rapide de conflits par le biais d'une procédure d'arbitrage et la simple application des décisions d'arbitrage par le biais de la modification directe du DNS (pour éviter des procédures judiciaires de longue haleine).

Un autre élément important de l'étude sur l'organisation actuelle de la gouvernance du DNS concerne la gestion des domaines nationaux de niveau supérieur (ccTLD). Actuellement, les codes pays sont gérés par une variété d'institutions agréées à l'époque des premiers balbutiements de l'Internet, lorsque certains gouvernements n'étaient guère intéressés par ces questions. Parmi ces organisations, on peut citer: des institutions universitaires, des associations techniques, des ONG et même des particuliers. Dans bon nombre de cas, la responsabilité de la gestion des codes pays a été attribuée sur une base "premier arrivé premier servi.

LES ENJEUX

La création de nouveaux noms de domaine génériques

Au milieu des années quatre-vingt-dix, l'un des pères fondateurs de l'Internet, Jon Postel, tenta en vain d'ajouter quelques nouveaux domaines à la liste existante (.com, .edu, .org et .int). La principale opposition émanait du monde des affaires qui craignait qu'un plus grand nombre de domaines vienne encore compliquer la protection de leurs marques commerciales. Une approche restrictive a donc prévalu et seuls quelques nouveaux domaines furent finalement introduit par l'ICANN en 2000 (.biz, .info, .name, .pro, .museum, .aero et .coop).

Un autre problème lié à la création de nouveaux domaines concerne l'association des noms de domaine au contenu. Ainsi par exemple, le Congrès américain a adopté une loi introduisant le domaine "kids.us," réservé aux sites dont le contenu sera adapté aux enfants. La principale difficulté associée à cette proposition concerne la question de savoir ce qui constitue un contenu adapté aux enfants. Des controverses liées aux aspects conceptuels et pratiques du contrôle du contenu pourraient bien se

faire jour. Jusqu'à présent, le domaine "kids" n'a été utilisé que comme sous-domaine du domaine national américain.

La gestion des domaines nationaux

La gestion des domaines nationaux de niveau supérieur présente trois enjeux importants. Le premier concerne la décision très souvent politiquement sensible quant à la question de savoir exactement quels codes pays devraient être enregistrés lorsque l'on a affaire à des pays et des entités dont le statut international est flou voire contesté (par ex. les Etats nouvellement indépendants, les mouvements de résistance, etc.). Jon Postel prônait l'attribution de noms de domaine nationaux en conformité avec la norme ISO, qui constitue une source commune de codes pays à deux lettres pour les pays et autres entités. L'approche de Postel a été couronnée de succès et continue d'être pratiquée, bien que la liste de l'ISO recense des "aires économiques distinctes" plutôt que des nations souveraines.

Le deuxième enjeu concerne la question de savoir qui devrait gérer les codes pays. Bon nombre de pays ont tenté de devenir maîtres de leurs domaines nationaux, lesquels sont considérés comme des ressources nationales. Ainsi par exemple, l'Afrique du Sud a invoqué ses droits souverains pour tenter de reconquérir le contrôle de son domaine national. Une nouvelle loi stipule que l'utilisation du domaine national en dehors des paramètres prescrits par le gouvernement sud-africain sera traité comme un délit. Le modèle brésilien de gestion des domaines nationaux est souvent désigné comme un exemple réussi d'approche multipartite. L'organe national chargé des domaines brésiliens est ouvert à tous les principaux acteurs, y compris les pouvoirs publics, le monde des affaires et la société civile. En revanche, le transfert par le Cambodge de la gestion du domaine national d'un contrôle non gouvernemental à un contrôle gouvernemental est souvent donné comme un exemple de transition ratée. Le gouvernement a réduit la qualité des services et introduit des droits d'enregistrement plus élevés, qui ont rendu l'enregistrement de domaines au Cambodge beaucoup plus difficile.

Dans certains cas, les codes pays ont été utilisés à mauvais escient pour procéder à l'enregistrement de domaines génériques de niveau supérieur, comme ceux énumérés dans le tableau ci-dessous:

CODE PAYS	PAYS	ZONE DE DOMAINE
Tv	Tuvalu	Stations de télévision
Mu	Maurice	Musique
Md	Moldavie	Médecine et santé
Fm	Fédération de Micronésie	Radio
Tm	Turkménistan	Marque commerciale

La plupart des pays sus-mentionnés ont tenté de regagner le contrôle de leurs domaines nationaux. Ainsi par exemple, Maurice a monté une très vive campagne de pression diplomatique dans ce sens.

Le troisième enjeu à trait à la réticence de bon nombre d'opérateurs de domaines nationaux à l'idée d'être intégrés au système de l'ICANN. Jusqu'ici l'ICANN n'a pas réussi à rassembler tous les opérateurs de domaines nationaux sous sa tutelle. Certains opérateurs de domaines nationaux ont démarré leur propre organisation régionale; citons par exemple le CENTR (le Conseil des registres européens de TLD nationaux).

Le problème des langues: les noms de domaine multilingues

L'une des principales limitations pour le développement futur de l'Internet réside dans le manque de fonctions multilingues pour gérer les infrastructures de l'Internet. Les noms de domaine sont enregistrés et utilisés en anglais. Même les caractères non-ASCII de la langue française ou allemande ne peuvent pas être utilisés dans les adresses Internet (par ex. café devient cafe). La situation se complique encore davantage avec les caractères non latins comme le japonais, l'arabe et le chinois.

Parmi les différentes solutions envisagées pour les noms de domaine multilingues, les plus pertinentes sont les systèmes IDN (Internationalised Domain Name) et NLIA (Native Language Internet Address). Le système IDN, option technique proposée par l'IETF, s'impose de plus en plus comme la solution retenue. Il traduit les noms natifs en noms de domaine anglais sur la machine cliente et transmet le nom de domaine en anglais pour résolution sur le DNS. Un obstacle à l'utilisation plus large de l'IDN réside toutefois dans son intégration technique avec les principaux navigateurs Internet tels qu'Internet Explorer.

Outre les difficultés techniques, le prochain défi, sans doute encore plus complexe, sera le développement de politiques et de procédures de gestion. Il existe des pressions croissantes pour que le système IDN soit géré par des pays ou des groupes de pays parlant la même langue. Ainsi par

exemple, le gouvernement chinois a indiqué à plusieurs reprises que l'IDN en chinois devrait être géré par la Chine. L'introduction d'une politique IDN sera l'un des principaux défis de l'ICANN et mettra à l'épreuve son approche internationale favorable à l'intégration.

LES SERVEURS RACINES

Parce qu'ils sont tout en haut de l'arborescence hiérarchique du système de noms de domaine, les serveurs racines suscitent beaucoup d'intérêt. Ils figurent au cœur de la plupart des débats universitaires et politiques sur les questions liées à la gouvernance de l'Internet.

LA SITUATION ACTUELLE

La fonctionnalité et la robustesse du DNS peuvent être mieux appréhendées lorsqu'on analyse la crainte de voir l'Internet s'écrouler si jamais les serveurs racines venaient à être désactivés. Tout d'abord, il existe 13 serveurs racines répartis à travers le monde (10 aux Etats-Unis, 3 ailleurs; sur les 10 serveurs des Etats-Unis, plusieurs sont gérés par des agences gouvernementales américaines). Si l'un des serveurs venait à tomber en panne, les 12 ordinateurs restants continueraient de fonctionner. Même si les 13 serveurs racines se plantaient simultanément, la résolution des noms de domaine (principale fonction des serveurs racines) se poursuivrait sur d'autres serveurs de noms de domaine, répartis de façon hiérarchique sur l'ensemble de l'Internet.

Par conséquent, des milliers de serveurs de noms de domaine renferment des copies du fichier de la zone racine et un effondrement immédiat et catastrophique de l'Internet est tout simplement impossible. Il faudrait un certain temps pour que les conséquences fonctionnelles graves éventuelles soient détectées et, dans l'intervalle, il serait possible de réactiver les serveurs d'origine ou d'en créer de nouveaux.

En outre, le système de serveurs racines est sensiblement renforcé par le système "Anycast", qui duplique les serveurs racines dans plus de 80 emplacements à travers le monde. Cette structure offre de nombreux avantages, y compris une robustesse accrue du système DNS et une résolution plus rapide des adresses Internet (grâce au système Anycast, les serveurs résolveurs sont plus proches de l'utilisateur final).

Les 13 serveurs racines sont gérés par une grande variété d'organisations: institutions universitaires/publiques (six serveurs), sociétés commerciales (quatre serveurs) et institutions gouvernementales (trois serveurs).

Les institutions qui gèrent les serveurs racines reçoivent un fichier de la zone racine proposé par l'IANA (ICANN) et approuvé par le gouvernement américain (ministère du Commerce, en anglais Department of Commerce DoC). Une fois le contenu agréé par le DoC, il est entré sur un serveur racine maître géré par VeriSign mandaté par le DoC. Le fichier figurant sur le serveur racine maître est alors automatiquement dupliqué sur tous les autres serveurs racines. De cette façon, le gouvernement américain est en mesure d'apporter des changements unilatéraux au DNS. C'est là une source de préoccupation pour de nombreux gouvernements.

LES ENJEUX

Should the Policy Supervision of Root Servers Be Internationalised?

Nombre de pays se sont déclarés perturbés par le dispositif actuel aux termes duquel la prise de décision finale concernant le contenu des serveurs racines demeure la responsabilité du ministère du Commerce américain et ils ont suggéré l'adoption d'une "Convention sur les serveurs racines" qui conférerait à la communauté internationale le contrôle de la politique des serveurs racines ou, tout au moins, accorderait aux Etats nations des droits sur leurs propres noms de domaine nationaux. Il est fort peu probable que les institutions américaines (le Congrès en particulier) accepteront de telles propositions. Un compromis possible pourrait se baser sur deux éléments:

- le transfert du contrôle des serveurs racines du ministère américain du Commerce à l'ICANN, comme envisagé au départ;
- une réforme radicale de l'ICANN, qui déboucherait sur la création d'un organisme international sui generic, qui constituerait un cadre institutionnel acceptable pour tous les pays.

.

Quelles sont les chances de pouvoir créer des serveurs racines alternatifs (une sorte d'Internet B)?

Comme nous l'avons évoqué plus haut, techniquement, la création de serveurs racines alternatifs n'a rien de compliqué. La principale question est de savoir combien "d'adeptes" aurait un serveur alternatif, ou, plus précisément, combien d'ordinateurs de l'Internet pointeraient vers eux

au moment de résoudre les noms de domaine. Sans utilisateurs, tout DNS alternatif n'a aucune raison d'être. Quelques tentatives de création d'un DNS alternatif ont été faites: Open NIC, New. net et Name.space. La plupart d'entre elles se sont soldées par un échec, ne comptant que pour un pourcentage minime d'utilisateurs de l'Internet.

LES FOURNISSEURS D'ACCES A L'INTERNET (FAI)

Les fournisseurs d'accès à l'Internet connectent les utilisateurs à l'Internet et hébergent des sites Web. C'est la raison pour laquelle, pour bon nombre de gouvernements, les FAI sont l'option la plus simple et la plus directe pour faire appliquer la législation et le contrôle gouvernemental sur l'Internet. Dans le présent ouvrage, par FAI nous entendons à la fois les sociétés qui fournissent un accès aux particuliers et les fournisseurs d'accès institutionnels (universités, services gouvernementaux, etc.).

Au cours du boom de l'Internet dans les années quatre-vingt-dix, les FAI n'assumaient aucune responsabilité en termes de contenu ou de violation des droits d'auteur. Il était estimé que des pressions supplémentaires sur les FAI risquaient d'entraver le développement futur de l'Internet. Avec l'importance commerciale croissante de l'Internet et les préoccupations accrues en termes de sécurité, de nombreux pays ont commencé à concentrer leurs efforts de répression sur les FAI.

LES ENJEUX

Le marché des FAI et le monopole des télécommunications

Dans les pays ayant des monopoles dans le secteur des télécommunications, il est fréquent que ces monopoles assurent aussi l'accès à l'Internet. Leur situation de monopoles empêche d'autres FAI d'entrer sur le marché et entrave la concurrence. Ceci donne lieu à des prix plus élevés, à une qualité de service souvent inférieure et cela ne résout en rien la fracture numérique. Dans certains cas, les monopoles des télécommunications tolèrent l'existence d'autres FAI mais ils s'immiscent dans leurs affaires au niveau opérationnel (par ex. en leur fournissant des bandes passantes restreintes ou en perturbant les services).

La responsabilité des FAI en matière de droits d'auteur

La plupart des systèmes juridiques ont en commun le principe qu'un FAI ne peut pas être tenu responsable de l'hébergement d'un contenu qui est en violation des droits d'auteur dans la mesure où le FAI n'en a pas conscience. La principale différence réside dans les mesures juridiques prises une fois que le FAI est informé que le contenu qu'il héberge est en violation d'un droit d'auteur.

Les législations américaine et européenne adoptent la procédure dite de "Notice-Take-Down" (notification et retrait), aux termes de laquelle le FAI est prié de retirer le contenu litigieux pour éviter les poursuites. Les législations américaine et européenne accordent une plus grande protection aux titulaires de droits d'auteur, ne donnant à aucun moment à l'utilisateur du contenu l'opportunité de défendre son cas. La loi japonaise adopte une approche plus mesurée, par le biais de la procédure "Notice-Notice-Take-Down" (notification-notification et retrait), qui accorde à l'utilisateur du contenu le droit de contester la demande de retrait.

Le rôle des FAI en matière de politique du contenu

"Ne tirez pas sur le facteur!" telle est la réponse des fournisseurs d'accès face aux pressions officielles croissantes pour les obliger à appliquer une politique de réglementation du contenu. A contrecoeur, les fournisseurs d'accès s'impliquent progressivement dans le contrôle du contenu. Deux options s'offrent à eux. La première est de faire appliquer la réglementation du gouvernement. Avec la seconde, basée sur un principe d'autorégulation, il appartient au fournisseur d'accès de décider de ce qu'il considère comme un contenu approprié. On court ainsi le risque de voir se privatiser la police du contenu, les fournisseurs d'accès assumant alors les responsabilités du gouvernement.

Bon nombre de pays ont adopté une législation aux termes de laquelle les fournisseurs d'accès doivent assumer des responsabilités supplémentaires ayant trait au contrôle du contenu; aussi bien du point de vue de ce qui est disponible sur les sites Web hébergés par leurs soins qu'au plan de ce qui est accessible par les clients qu'ils desservent. Cette approche pourrait déboucher sur des dépenses supplémentaires pour les fournisseurs d'accès et, à terme, sur une hausse des coûts de l'accès à l'Internet pour les utilisateurs.

FOURNISSEURS DE BANDE PASSANTE SUR L'INTERNET (IBP)

L'architecture d'accès à l'Internet est tri-étagée. Les fournisseurs d'accès qui connectent les utilisateurs constituent le 3ème niveau. Les niveaux 1 et 2 se composent de fournisseurs de bande passante sur l'Internet. Le niveau 1 (les dorsales de l'Internet) est le plus souvent géré par de grosses sociétés comme MCI, AT&T, Cable Wireless et France Telecom. Dans le domaine des dorsales de l'Internet, les sociétés de télécommunications traditionnelles ont étendu leur présence sur le marché mondial aux dorsales de l'Internet. Les fournisseurs du 2ème niveau fonctionnent généralement au niveau national ou régional.

LES ENJEUX

Les infrastructures de l'Internet devraient-elles être assimilées à un service public?

Les données Internet peuvent transiter par le biais de n'importe quel support de télécommunications. Dans la pratique, des installations comme les dorsales de 1er niveau sont devenues essentielles pour le fonctionnement de l'Internet. Leur position pivot au sein du réseau Internet confère à leurs propriétaires un pouvoir de marché suffisant pour imposer leurs prix et leurs conditions de fourniture de services. Il a été fait mention de deux affaires associées dans un récent rapport de l'OSCE (l'Organisation pour la sécurité et la coopération en Europe).

Dans la première affaire, une action a été intentée à l'encontre d'une page Web hébergée par Flashback en Suède qui présentait un contenu nazi litigieux. Les tribunaux ont décidé que la page ne violaient pas la législation suédoise anti-nazi. Cependant, un militant anti-nazi très engagé a monté une vive campagne contre Flashback, faisant ainsi pression sur le fournisseur d'accès de Flashback, Air2Net, et sur le principal opérateur de dorsale MCI/WorldCom. Devant les pressions de la campagne, MCI/WorldCom a décidé de déconnecter Flashback, et ce malgré l'absence de toute décision judiciaire dans ce sens. Les tentatives de Flashback pour trouver un autre fournisseur d'accès ont été vaines, car la plupart d'entre eux étaient aussi connectés par le biais de la dorsale gérée par MCI/WorldCom.

La deuxième affaire est intervenue aux Pays-Bas lorsqu'un petit fournisseur d'accès néerlandais, Xtended Internet, a été déconnecté par son fournisseur américain en amont sous les pressions exercées par le mouvement de Scientologie. Finalement, le fonctionnement de l'Internet pourrait dépendre des décisions prises par les propriétaires des dorsales centrales. La communauté mondiale de l'Internet a-t-elle le droit d'exiger des opérateurs de télécommunications des assurances du fonctionnement fiable des infrastructures vitales de l'Internet? Ces compagnies gèrent-elles une fonction publique?

La libéralisation des télécommunications et le rôle des fournisseurs d'accès

Il existe des points de vue divergents quant à la question de savoir dans quelle mesure les fournisseurs d'accès à l'Internet devraient être soumis à la réglementation existante de l'OMC. Les pays industrialisés soutiennent que les règles libéralisées octroyées par l'OMC aux opérateurs de télécommunications peuvent aussi s'appliquer aux fournisseurs d'accès. Une interprétation restrictive souligne le fait que le régime des télécommunications de l'OMC s'applique uniquement au marché des télécommunications. La réglementation du marché des fournisseurs d'accès exige de nouvelles règles de l'OMC.

MODELE ECONOMIQUE POUR LA CONNECTIVITE INTERNET

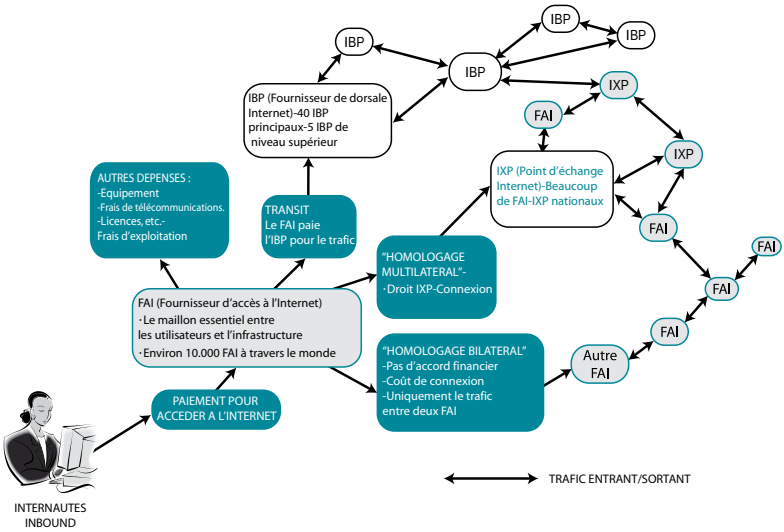
LA SITUATION ACTUELLE

Bien souvent, tout débat sur des questions liées à la gouvernance débouche sur une analyse de la distribution de l'argent et des sources de revenu. Quels sont les flux de financement sur l'Internet? Qui paie pour l'Internet?

Il existe d'innombrables transactions financières entre les nombreuses parties impliquées dans l'Internet.

- Les particuliers ou les sociétés abonnés paient leur fournisseur d'accès.
- Les fournisseurs d'accès paient les services des opérateurs de télécommunications et la bande passante Internet.

- Les fournisseurs d'accès paient les constructeurs pour le matériel, le logiciel et l'entretien (y compris les outils de diagnostic ainsi que le soutien technique pour le personnel qui gère leurs structures, les bureaux d'assistance et les services administratifs).
- Les parties qui enregistrent un nom de domaine auprès d'un prestataire d'enregistrement paient non seulement ce prestataire mais encore les services de l'IANA.
- Les fournisseurs d'accès paient les RIR pour les adresses IP.
- Les RIR paient l'ICANN.
- Les opérateurs de télécommunications paient les fabricants de câbles et satellites et les prestataires de services de télécommunications pour qu'ils leur fournissent les liaisons nécessaires. Comme ces opérateurs sont souvent dans le rouge, ils versent à leur tour des intérêts aux banques et consortiums bancaires.



La liste est longue et, à dire vrai, "tout se paie". En fin de compte, les coûts de cette chaîne sont couverts par les utilisateurs de l'Internet, qu'il s'agisse de particuliers ou d'institutions.

LES ENJEUX

Qui devrait couvrir le coût des liaisons entre les pays en développement et les pays industrialisés?

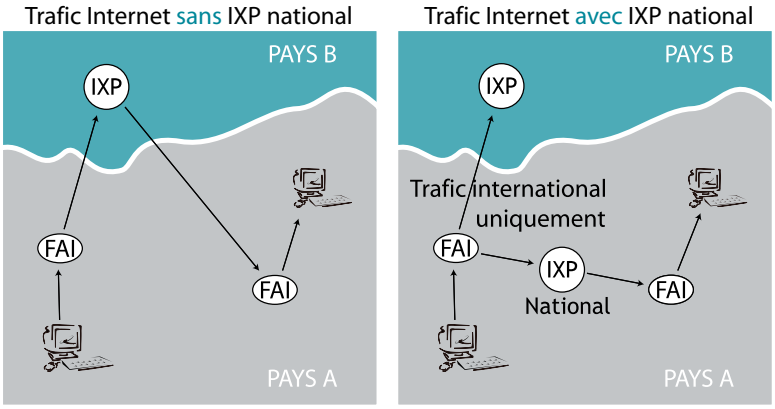
Actuellement, le coût est principalement supporté par les pays en développement. A la différence du système de téléphonie traditionnel, avec lequel le prix de chaque appel international est partagé entre les deux pays, le modèle Internet place la totalité du coût d'un seul côté, les pays en développement, qui doivent se connecter aux dorsales, situées pour la plupart dans les pays industrialisés. Aussi paradoxal que cela puisse paraître, on pourrait arguer que ce sont les petits pays pauvres qui subventionnent le système Internet dans les pays industrialisés.

Le problème des règlements financiers est extrêmement pertinent pour les pays les plus pauvres qui dépendent du revenu généré par les communications internationales en guise de source budgétaire importante. La situation s'est encore compliquée avec l'introduction de la téléphonie sur Internet, Voice over IP (VoIP), qui déplace le trafic téléphonique des opérateurs nationaux de télécommunications vers l'Internet.

L'UIT a amorcé des discussions sur les améliorations qui pourraient être apportées au système actuel pour le règlement des dépenses associées à l'Internet avec pour objectif primordial d'aboutir à une répartition mieux équilibrée des coûts d'accès à l'Internet. En raison de l'opposition des pays industrialisés, la résolution D.50 adoptée par l'UIT est quasiment sans effet.

Réduction des coûts d'accès par le biais de l'utilisation des points d'échange Internet (IXP)

Les IXP sont des installations techniques par le biais desquelles les différents fournisseurs d'accès échangent le trafic Internet. Les IXP sont habituellement établis afin de maintenir le trafic Internet à l'intérieur d'une communauté restreinte (par ex. une ville, une région ou un pays) et d'éviter ainsi le routage superflu par des emplacements géographiques reculés.



Les IXP jouent aussi un rôle important dans la réduction de la fracture numérique. Ainsi par exemple, dans le cas d'un pays sans IXP nationaux, une portion notable du trafic entre les clients à l'intérieur du pays doit être acheminée par le biais d'un autre pays. Ceci augmente le trafic de données internationales sur longues distances et le coût de fourniture du service Internet.

NORMES DU WEB

A la fin des années quatre-vingt, la bataille concernant les normes du réseau était achevée. TCP/IP s'était progressivement imposé comme le principal protocole du réseau, distançant toutes les autres normes, telles que X-25 soutenue par l'UIT (comme élément de l'architecture OSI - Open Systems Interconnection) et bon nombre d'autres normes de grandes marques, comme la norme SNA d'IBM. Si l'Internet facilitait les communications ordinaires entre une variété de réseaux grâce à TCP/IP, il manquait toujours au système des normes applicatives communes.

Une solution a été élaborée par Tim Berners-Lee et ses collègues du CERN de Genève. Il s'agissait d'une nouvelle norme pour échanger des informations sur l'Internet, appelée HTML (HyperText Mark-up Language, qui n'était autre qu'une version simplifiée d'une norme ISO existante appelée SGML). Le contenu affiché sur l'Internet devait d'abord être organisé en fonction des critères HTML. HTML comme base du

World Wide Web allait ouvrir la voie à la croissance exponentielle de l'Internet.

Depuis sa première version, HTML a été constamment amélioré et doté de nouvelles fonctionnalités. La pertinence croissante de l'Internet a mis en exergue la question de la normalisation de HTML. Ce point s'est avéré particulièrement important durant la "guerre des navigateurs" entre Netscape et Microsoft, lorsque chaque société a tenté de consolider sa position sur le marché en influençant les critères HTML. Si le HTML de base gérait uniquement le texte et les photos, les nouvelles applications Internet exigeaient des technologies plus sophistiquées capables de gérer des bases de données, des vidéos et des animations. Une telle variété d'applications a nécessité des efforts gigantesques en termes de normalisation pour veiller à ce que le contenu de l'Internet puisse être visualisé correctement par la majorité des navigateurs Internet.

La normalisation des applications est entrée dans une nouvelle ère avec l'émergence de XML (eXtended Mark-up Language) qui a conféré une plus grande souplesse à la définition de normes pour le contenu de l'Internet. De nouvelles séries de normes XML ont également été introduites. Ainsi, la norme pour la distribution du contenu sans fil s'appelle WML (Wireless Mark-up Language).

La normalisation des applications s'effectue principalement dans le cadre du World Wide Web Consortium (W3C), sous la gouverne de Tim Berners-Lee. Il est intéressant de constater que malgré sa pertinence très poussée pour l'Internet, jusqu'à présent, W3C n'a guère attiré d'attention dans le débat sur la gouvernance de l'Internet.

OPEN SOURCE

Un logiciel Open Source est mis à la disposition des utilisateurs à titre gracieux et il peut être modifié par ses utilisateurs. Les applications Open source sont développées par des programmeurs du monde entier qui travaillent sur le même code.

Au moment de son introduction, Open Source promettait de devenir une alternative intéressante face aux coûteux logiciels propriétaires. Linux est sans doute l'initiative Open Source la plus connue. La prolifération de logiciels Open Source a été plus lente que prévu, principalement du fait

d'un manque de soutien technique fiable. La toute dernière décision par certains acteurs majeurs, comme IBM et Intel, de se servir de Linux, la principale plate-forme Open Source, pourrait déboucher sur un développement réussi de cette approche.

De surcroît, il existe un regain d'intérêt envers Open Source sous un nouveau nom et selon un concept légèrement différent, portant le nom de Free/Libre Open Source Software (FLOSS). La principale différence entre Open Source et FLOSS réside dans le fait que FLOSS permet le libre accès au code sans aucun enregistrement préalable.

Open Source est souvent présenté comme la solution au développement des capacités TIC des pays en développement. Lors du SMSI, une tentative déployée par la société civile et quelques pays en développement en vue d'introduire Open Source et FLOSS dans le document final en guise de solution permettant de surmonter la fracture numérique a été édulcorée dans une référence générale aux "différents modèles de logiciel, y compris les logiciels propriétaires, les logiciels à code ouvert ou les logiciels dits libres".

CONVERGENCE: INTERNET-TELECOMMUNICATION-MULTIMEDIA

L'usage généralisé et dominant des protocoles Internet a déclenché un processus de convergence des télécommunication, du multimédia et des systèmes de divertissement. De nos jours, il est possible de passer un coup de téléphone, d'écouter la radio, de regarder la télé et de partager de la musique par le biais de l'Internet. Dans le domaine des télécommunications classiques, le principal point de convergence est la norme VoIP (voix sur IP). Sa popularité croissante est fondée sur des prix plus bas, la possibilité d'intégrer des lignes de communications voix et données, ainsi que l'usage d'outils informatiques avancés. Le protocole TCP/IP s'impose aussi en maître dans le domaine du multimédia et des divertissements. Si une convergence technique est indéniable et se produit à vive allure, ses conséquences économiques et juridiques nécessiteront toutefois davantage de temps pour évoluer.

LES ENJEUX

Les implications économiques de la convergence

Au niveau économique, la convergence a commencé à transformer radicalement les marchés traditionnels en plaçant en concurrence directe des sociétés qui fonctionnaient jusque-là dans des domaines distincts. Il reste à savoir qui va savoir tirer son épingle du jeu dans ce marché de plus en plus convergent: des grands groupes de télécommunications comme MCI ou des compagnies TIC comme IBM.

La même chose vaut aussi pour le marché du multimédia, même si dans ce domaine une poignée de compagnies ont réagi au défi posé par la convergence en développant à la fois des produits relevant du domaine informatique et du domaine des médias et des divertissements ou en formant des partenariats. Sony est un exemple de société qui a étoffé ses capacités à la fois dans le domaine des TIC et dans les médias/divertissements. La fusion d'America Online avec Time Warner visait à associer les télécommunications aux médias/divertissements. A présent, AOL/Time Warner a rassemblé sous une seule et même grande organisation des fournisseurs d'accès à l'Internet, des groupes de télévision, de musique et des éditeurs de logiciel.

Le besoin d'un cadre juridique

Le système juridique est le plus lent à s'ajuster aux changements provoqués par la convergence technologique et économique. Chacun de ces segments - télécommunications, médias/divertissement et TIC - a un cadre réglementaire qui lui est propre.

Cette convergence soulève donc plusieurs questions en terme de réglementation et de gouvernance. Que se passera-t-il dans les régimes nationaux et internationaux existants dans des domaines comme la téléphonie et la diffusion? Quels seront les nouveaux régimes développés qui seront principalement axés sur l'Internet? La réglementation de cette convergence devrait-elle être la responsabilité des pouvoirs publics (Etats et organisations internationales) ou devrait-elle se faire par le biais d'une autorégulation?

Certains pays, comme la Malaisie et la Suisse, ainsi que l'Union européenne, ont commencé à fournir des réponses à ces questions. La Malaisie a adopté la Loi sur les communications et les multimédias en 1998, qui établit un cadre général pour la réglementation de la convergence. Les nouvelles directives-cadres de l'UE, désormais transposées en lois

nationales, constituent aussi un pas dans cette direction, tout comme les lois et règlements suisses sur les télécommunications.

Le risque de convergence entre câblodistributeurs et fournisseurs d'accès

Dans bon nombre de pays, l'Internet à haut débit a été introduit par des réseaux câblés. Ceci vaut tout particulièrement pour les Etats-Unis, où l'Internet par câble est beaucoup plus répandu que l'ADSL, l'autre grande option de haut débit pour Internet. Quels sont les risques associés à cette convergence?

Certains observateurs soutiennent que l'intervention des câblodistributeurs entre les utilisateurs et l'Internet pourrait remettre en question le principe même du réseau de bout en bout.

La principale différence entre l'accès par ligne commutée classique et l'accès par câble tient au fait que l'univers du câble n'est pas réglementé par les règles qui s'appliquent aux entreprises de télécommunications. Ces règles, applicables au système de téléphonie, stipulent que l'accès doit être non discriminatoire. Les câblodistributeurs ne sont pas soumis à ces règles, ce qui leur donne un contrôle total sur l'accès de leurs abonnés à l'Internet. Ils peuvent bloquer l'utilisation de certaines applications et contrôler l'accès à certains contenus. Les possibilités de surveillance et, par là même, les risques de violation de la vie privée, sont beaucoup plus grands avec l'Internet par câble puisque l'accès est contrôlé par le biais d'un système semblable à celui des réseaux locaux, qui fournit un niveau élevé de contrôle direct aux usagers.

Dans un article sur cette question, le Syndicat américain pour les libertés civiles a donné un exemple des risques que représentent les monopoles des câblodistributeurs: C'est comme si on permettait à une compagnie des téléphones de gérer sa propre chaîne de restaurants et d'assurer un service fiable et des signaux de qualité aux entreprises qui appellent Domino et un signal occupé, en dérangement ou autre problème de fonctionnement à ceux qui appellent Pizza Hut."

Ce problème de convergence ne sera résolu qu'une fois qu'une décision sera prise sur la question de savoir si l'Internet par câble est un "service d'informations" ou un "service de télécommunications". Dans le deuxième cas, il devra être réglementé par le biais des règles qui s'appliquent aux entreprises de télécommunications.

SECURITE DE L'INTERNET

LA SITUATION ACTUELLE

La sécurité de l'Internet a suscité davantage d'intérêt au fil de l'essor rapide de la base des usagers de l'Internet. L'Internet a prouvé ce que beaucoup soupçonnaient depuis longtemps déjà: la technologie peut être à la fois habilitante et menaçante. Ce qui peut servir l'intérêt général d'une société peut aussi être utilisé à ses dépens.

Les effets négatifs de l'intégration rapide de l'Internet dans presque toutes les facettes des activités humaines augmentent la vulnérabilité de la société moderne. Les infrastructures essentielles, y compris les réseaux électriques, les systèmes de transport et les services de santé font tous partie d'un réseau mondial susceptible d'être la proie d'une attaque cybernétique. Sachant que les attaques de ces systèmes sont réputées engendrer des perturbations majeures et avoir des répercussions financières potentiellement très élevées, les infrastructures vitales sont des cibles fréquentes.

La sécurité de l'information est abordée plus en détail dans trois autres livrets de cette série, à savoir:
- Good Hygiene for Data and Personal Computers
- Information Security and Organisations
- Hacktivism, Cyber-terrorism and Cyber-war

Les questions liées à la sécurité de l'Internet peuvent être classées selon trois critères: le type d'action, le type d'auteur et le type de cible.

Une classification fondée sur le type d'action comprendrait: l'interception des données, l'interférence sur les données, l'accès illégal, les logiciels espions et le vol d'identité. Parmi les auteurs possibles, on peut citer les hackers, les cyberdélinquants, cyberguerriers ou encore les cyberterroristes.

Les cibles potentielles sont innombrables, qu'il s'agisse de particuliers, de sociétés privées ou d'institutions publiques en passant par des infrastructures vitales, des gouvernements ou encore des actifs militaires.

INITIATIVES POLITIQUES DANS LE DOMAINE DE LA SECURITE DE L'INTERNET

Il existe de nombreuses initiatives nationales, régionales et mondiales axées sur la sécurité de l'Internet.

Au niveau national il existe un volume croissant de législation et de jurisprudence qui traite de la sécurité de l'Internet. Les mesures les plus en vue sont les initiatives américaines associées à une autorité plus vaste de l'Etat dans sa lutte contre le terrorisme. Le ministère de la Sécurité du Territoire national est la principale institution qui traite des questions liées à la sécurité de l'Internet. Il est difficile de trouver un pays, tout au moins dans les pays industrialisés, qui n'ait pas une initiative quelconque axée sur la sécurité de l'Internet.

Au niveau international, les organisations les plus dynamiques ont été l'OCDE, qui a produit ses Lignes directrices sur la sécurité de l'information et l'UIT, qui a produit un grand nombre de cadres de sécurité, d'architectures et de normes, y compris la X.509, qui fournit la base de l'infrastructure à clé publique que l'on retrouve, par exemple, dans la version sécurisée de HTTP (HTTPS).

Le G8 a également proposé quelques initiatives dans le domaine de la sécurité de l'Internet, par exemple l'amélioration de la coopération entre les organismes chargés de faire appliquer la loi. Le G8 a également créé un sous-groupe sur la criminalité de haute technologie pour examiner la création d'un réseau de communication 24 heures sur 24 et 7 jours sur 7 entre les centres de sécurité cybernétique des Etats membres, la formation du personnel et l'amélioration des systèmes juridiques des Etats nations afin de combattre la cybercriminalité et de promouvoir la coopération entre la filière des TIC et les organismes chargés de l'application de la loi.

L'Assemblée générale des Nations Unies a adopté plusieurs résolutions sur une base annuelle sur les "Développements dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale", plus précisément les résolutions 53/70 en 1998, 54/49 en 1999, 55/28 en 2000, 56/19 en 2001, 57/239 en 2002 et 58/199 en 2003. A partir de 1998, toutes les résolutions ont eu une teneur semblable sans amélioration notable. Elles ne tiennent pas compte des profonds changements qui sont intervenus dans le domaine de la sécurité de l'Internet depuis 1998.

Un instrument juridique international de premier plan pour la sécurité de l'Internet est la Convention du Conseil de l'Europe sur la cybercriminalité, qui est entrée en vigueur le 1er juillet 2004.

Certains pays ont établi des arrangements bilatéraux. Les Etats-Unis ont des accords bilatéraux de coopération judiciaire dans les affaires criminelles avec plus de 20 autres pays. Ces accords sont également utilisé dans les affaires de cyberdélinquance.

Les milieux universitaires et les acteurs privés ont tenté de rédiger un accord international sous le nom de projet de Convention de Stanford sur la protection contre la cybercriminalité et le terrorisme. Ce projet préconise la création d'un organe international, appelé Agence pour la protection des infrastructures de l'information (AIIP).

LES ENJEUX

L'architecture de l'Internet et la sécurité

La nature même de l'organisation de l'Internet affecte sa sécurité. Devrions-nous persister dans notre approche courante qui consiste à intégrer des dispositifs de sécurité dans un système préexistant non sécurisé ou bien changer certains éléments dans le fondement même de l'infrastructure de l'Internet? Comment un tel changement affecterait-il les autres caractéristiques de l'Internet, notamment son caractère ouvert accessible à tous et sa transparence? Dans le passé, la plupart des développements en matière de normes Internet visaient à améliorer les performances ou à introduire de nouvelles applications. Jusqu'ici, la sécurité n'était pas une priorité.

Il est difficile de savoir si l'IETF sera en mesure de changer les normes de courrier électronique afin d'assurer l'authentification des auteurs pour, finalement, réduire l'usage abusif de l'Internet (par ex. le pollupostage, la cybercriminalité). Compte tenu de la controverse qui accompagne tout changement apporté aux normes élémentaires de l'Internet, il est fort probable que les améliorations du protocole Internet de base en matière de sécurité soient lentes et progressives. Le monde des affaires et autres parties intéressées par l'identification de solutions plus rapides pourraient commencer à développer de nouvelles couches Internet, "l'Internet intelligent", qui permettraient, entre autres, des communications sur l'Internet plus sécurisées.

Le commerce électronique et la sécurité de l'Internet

La sécurité est très souvent citée comme l'une des conditions préalables à une accélération de la croissance du commerce électronique. Sans un Internet fiable et sécurisé, les clients continueront de se montrer réticents à fournir des renseignements confidentiels en ligne, tels que leur numéro de carte de crédit. Il en va de même pour les services bancaires en ligne et la monnaie électronique.

Le respect de la vie privée et la sécurité de l'Internet

Une autre question débattue concerne le lien entre la sécurité et les droits de l'homme. Le renforcement de la sécurité de l'Internet implique-t-il une érosion du respect des droits à la vie privée? Comment l'usage de logiciel de cryptage devrait-il être réglementé, pour pouvoir à la fois renforcer la protection légitime du caractère confidentiel des communications et lutter contre les communications illégales des terroristes et des criminels? Cet équilibre entre la sécurité de l'Internet et les droits de l'homme ne cesse d'osciller.

Au lendemain du 11 septembre 2001, la sécurité est devenue la priorité absolue des Etats-Unis et cela a donné lieu à l'adoption de diverses lois nationales, qui stipulaient, entre autres, des niveaux plus élevés de surveillance de l'Internet. La réaction de la société civile s'est axée sur les dangers pour le respect de la vie privée et la liberté d'expression.

La question de l'équilibre entre la sécurité informatique et le respect de la vie privée a été mise en exergue dans les discussions concernant la possibilité d'élargir au niveau mondial la Convention du Conseil de l'Europe sur la cybercriminalité. La principale objection soulevée par les militants des droits de l'homme tient au fait que la Convention se penche sur des questions liées à la sécurité de l'Internet au détriment de la protection de la vie privée et autres droits fondamentaux.

CRYPTAGE

L'un des points qui figurent au coeur des débats sur la sécurité de l'Internet concerne la question du cryptage, qui a trait aux outils qui peuvent être utilisés pour protéger les échanges de données.

Un logiciel de cryptage brouille les communications électroniques (courriel, images) pour en faire un texte illisible en se servant d'algorithmes mathématiques. L'équilibre entre le besoin de protéger le caractère confidentiel de certaines informations et le besoin qu'ont les gouvernements et les services d'intelligence de surveiller le trafic potentiel des réseaux criminels et terroristes reste un défi majeur.

Les aspects internationaux de la politique en matière de cryptage sont pertinents pour le débat sur la gouvernance de l'Internet, compte tenu du fait que la réglementation du chiffrement devrait être mondiale ou, tout au moins, impliquer les pays capables de produire des outils de cryptage.

Ainsi par exemple, la politique des Etats-Unis concernant le contrôle des exportations de logiciel de cryptage n'était guère performante car elle ne pouvait pas contrôler la distribution internationale de logiciel de chiffrement. Les éditeurs de logiciel américains ont monté une gigantesque campagne de pression en arguant que les contrôles à l'exportation ne renforçaient en rien la sécurité nationale mais servaient simplement à miner les intérêts commerciaux américains.

REGIMES INTERNATIONAUX CONCERNANT LES LOGICIELS DE CRYPTAGE

Le cryptage a été abordé dans deux enceintes: l'Entente de Wassenaar et l'OCDE. L'Entente de Wassenaar est un régime international adopté par 33 pays industrialisés pour restreindre l'exportation d'armes conventionnelles et les technologies à "double usage" vers les pays en guerre ou jugés être des "Etats parias". L'accord établit un Secrétariat à Vienne. Par le truchement du Groupe Wassenaar, les Etats-Unis faisaient pression pour élargir "l'Approche Clipper" à l'échelle internationale en contrôlant les logiciels de cryptage au moyen d'un système à tiers de confiance. Cette approche a été rejetée par de nombreux pays, tout particulièrement le Japon et les pays scandinaves.

Un compromis a été atteint en 1998 par le biais de l'introduction de lignes directrices en matière de cryptographie, lesquelles renfermaient une liste de contrôle des produits cryptographiques matériels et logiciels à double usage à clé d'une longueur supérieure à 56 bits. Ce compromis comprenait des outils Internet tels que les navigateurs Web et le courrier électronique. Il est intéressant de noter que cet arrangement 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 à l'intérieur même des Etats-Unis. 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 a été une autre enceinte de coopération internationale dans le domaine de la cryptographie. Bien que l'OCDE ne produise pas de documents légalement contraignants, ses lignes directrices sur diverses questions sont largement respectées. Elles sont le résultat de consultations d'experts et d'un processus de prise de décision consensuel. La plupart de ses lignes directrices sont finalement incorporées dans la législation nationale. La question du chiffrement était un sujet très controversé au sein des travaux de l'OCDE. Le débat a été amorcé 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 l'Entente de Wassenaar, les négociations sur la proposition américaine firent l'objet d'une vive opposition de la part du Japon et des pays scandinaves. Les pourparlers débouchèrent sur un compromis de spécification concernant les principaux éléments d'une politique de cryptographie.

Bref, les diverses tentatives en vue de développer un régime international de chiffrement, principalement dans le contexte de l'Entente de Wassenaar, n'ont pas débouché sur l'élaboration d'un régime international efficace. Il est encore possible de se procurer de puissants logiciels de chiffrement sur l'Internet.

POLLUPOSTAGE

LA SITUATION ACTUELLE

Le pollupostage, ou spam en anglais, est habituellement défini comme du courrier électronique non sollicité qui est envoyé à un grand nombre

d'internautes. Le pollupostage est principalement utilisé à des fins publicitaires. Parmi ses autres usages, on peut citer: l'activisme social, les efforts de campagne politique et la distribution de matériel pornographique. Le pollupostage est inclus dans la corbeille des infrastructures car il entrave le fonctionnement normal de l'Internet du fait de son impact sur l'une de ses applications premières: le courrier électronique. Il constitue l'une des questions de gouvernance de l'Internet qui touche presque toutes les personnes qui sont connectées à l'Internet. Selon les statistiques les plus récentes, sur 13 messages électroniques, 10 peuvent être classés comme pollupostage. Outre le fait qu'il constitue un phénomène agaçant, le pollupostage engendre aussi des pertes économiques considérables, à la fois en termes de bande passante utilisée et en termes de temps passé à vérifier et à supprimer les messages indésirables. Une récente étude mandatée par l'UE sur le pollupostage a rapporté que les pertes annuelles, ne serait-ce qu'en termes de capacité de bande passante, sont de l'ordre de 10 milliards d'euros.

Il est possible de lutter contre le pollupostage sur deux fronts: le front technique et le front juridique. Du point de vue technique, il existe désormais nombre d'applications pour le filtrage des messages et la détection de pollupostage. Le principal problème associé aux systèmes de filtrage tient au fait qu'il leur arrive aussi d'effacer les messages légitimes. L'industrie de lutte contre le pollupostage est un secteur croissant qui offre des applications de plus en plus sophistiquées capables de faire la distinction entre le pollupostage et les messages légitimes. Les méthodes techniques n'ont toutefois qu'un impact limité et doivent être complétées par des mesures juridiques spécifiques.

Au plan juridique, nombre d'Etats nations ont réagi par l'introduction de nouvelles lois contre le pollupostage. Aux Etats-Unis la Loi dites "Can-Spam" tente de trouver un équilibre délicat entre l'admission du courrier électronique à des fins publicitaires et la prévention du pollupostage. Bien que la loi prescrive de lourdes peines pour la distribution de pollupostage, y compris des peines pouvant aller jusqu'à cinq ans de prison, d'après les critiques, certaines de ses dispositions tolèrent, ou risquent même d'encourager, le pollupostage. Le point de départ "par défaut" énoncé dans la loi est que le pollupostage est permis jusqu'au moment où

le destinataire du message y met un terme (par le jeu d'une clause d'exclusion). Depuis l'adoption de la loi en décembre 2003, les statistiques relatives au pollupostage ne font ressortir aucune diminution du nombre de messages indésirables.

En juillet 2003, l'Union européenne a introduit sa propre législation anti-spam dans le cadre de sa directive sur le respect de la vie privée et les communications électroniques. Malgré l'obligation que l'UE imposait aux Etats membres de faire appliquer cette loi anti-spam d'ici la fin de 2003, neuf Etats membres n'ont pas respecté ce délai. La législation de l'UE encourage l'autorégulation et les initiatives par le secteur privé qui déboucheraient sur une réduction du pollupostage.

LA REPONSE INTERNATIONALE

La législation anti-spam adoptée tant par les Etats-Unis que par l'UE présente une faiblesse inhérente: un manque de dispositions pour empêcher le pollupostage transfrontière. Cette question est particulièrement pertinente pour certains pays comme le Canada, lequel, d'après les statistiques les plus récentes, reçoit 19 sur 20 messages indésirables en provenance de l'étranger. Le ministre canadien de l'Industrie, Lucienne Robillard, a récemment déclaré que le problème ne pouvait pas être résolu "pays par pays". La récente étude sur la législation anti-spam de l'UE réalisée par l'Institut du droit de l'information de l'Université d'Amsterdam débouche sur une conclusion analogue: "Le simple fait que la plupart des messages indésirables proviennent de l'extérieur de l'UE limite sensiblement l'efficacité de la Directive de l'Union européenne.". Il faut mettre en place une solution mondiale, déployée par le biais d'un traité international ou d'un mécanisme semblable.

Pollupostage et développement

Le pollupostage entraîne de graves difficultés qui restent toutefois gérables dans les pays industrialisés mais il paralyse les infrastructures Internet de nombreux pays en développement. Compte tenu du bas débit et du sous-développement des infrastructures Internet, le pollupostage menace l'accès élémentaire à l'Internet pour bon nombre d'utilisateurs des pays en développement. Ces pays ne disposent généralement pas des ressources techniques et du savoir-faire requis pour lutter contre le spam. Par conséquent, le pollupostage creuse encore la fracture numérique entre pays industrialisés et pays en développement.

Un Mémorandum d'accord signé par l'Australie, la Corée et le Royaume-Uni est l'un des premiers exemples de coopération internationale dans la lutte contre le pollupostage.

L'OCDE a créé un groupe d'action sur le pollupostage et il a préparé une boîte à outils anti-spam. L'UIT s'est aussi montrée dynamique en organisant une Réunion thématique sur la lutte contre le spam (du 7 au 9 juillet 2004) et elle examine diverses options pour mettre sur pied un Mémorandum d'accord mondial de lutte contre le pollupostage. Au niveau régional, l'UE a créé le Réseau des agences de répression du pollupostage et l'APEC a préparé un ensemble de lignes directrices à l'intention des consommateurs.

Une autre approche possible en matière de lutte contre le pollupostage a été adoptée par les grandes groupes Internet qui hébergent des comptes de courrier électronique: America Online, British Telecomm, Comcast, EarthLink, Microsoft et Yahoo!. Ils ont fondé l'ASTA (Anti-Spam Technical Alliance), dont la tâche primordiale est de coordonner les activités techniques et politiques de lutte contre le pollupostage.

LES ENJEUX

Les différentes définitions du pollupostage

Le fait que le pollupostage ait différentes acceptions tend à nuire à la cohésion de la campagne anti-spam. Aux Etats-Unis, une préoccupation d'ordre général concernant la protection de la liberté d'expression et du Premier Amendement nuit aussi aux efforts de la campagne de lutte contre le pollupostage. Les législateurs américains estiment que le spam est uniquement du "courrier électronique commercial non sollicité" et laissent de côté toutes les autres formes de pollupostage, y compris l'activisme politique et la pornographie. Dans la plupart des autres pays, le spam est considéré être "tout message électronique envoyé en masse et non sollicité" quel que soit son contenu. Sachant que la majeure partie des messages indésirables sont générés aux Etats-Unis, cette différence dans les acceptions du terme risque de gravement entraver toute possibilité d'introduction d'un mécanisme international efficace de lutte contre le spam.

Le pollupostage et l'authentification des messages

L'un des facteurs structurels générateurs de spam réside dans la possibilité d'envoyer des messages électroniques sous une fausse adresse. Il existe une solution technique à ce problème mais celle-ci nécessiterait toutefois d'apporter des modifications aux normes existantes du courrier électronique sur l'Internet. L'IETF s'attache à introduire des change-

ments dans le protocole de courrier électronique qui permettraient de garantir l'authentification des courriers électroniques. C'est là un exemple de la manière dont les questions d'ordre technique (en l'espèce, les normes) peuvent influencer la politique. L'authentification des messages électroniques se solderait par un compromis possible, en ce sens qu'elle réduirait l'anonymat de l'Internet.

Le besoin d'une action mondiale

Comme nous l'avons déclaré plus haut, la majeure partie des messages indésirables proviennent de l'étranger. C'est un problème mondial qui exige une solution mondiale. Il existe différentes initiatives qui pourraient déboucher sur une meilleure coopération mondiale. Il a déjà été fait mention de certaines d'entre elles, par exemple les Mémorandums d'accord bilatéraux. D'autres comprennent des actions comme le renforcement des capacités et l'échange d'informations. Une solution plus intégrée nécessiterait un mécanisme mondial de lutte contre le spam. Lors de la toute dernière réunion de l'UIT, certains délégués ont proposé l'adoption d'un Mémorandum d'accord multilatéral ou encore l'adoption d'un instrument dans le contexte du SMSI. Jusqu'ici, les pays industrialisés donnent la préférence au renforcement de la législation nationale en association avec des campagnes bilatérales ou régionales de lutte contre le spam. Compte tenu du fait qu'ils sont dans la position non enviable de recevoir ce "mal public universel" qui provient le plus souvent des pays industrialisés, la plupart des pays en développement cherchent à mettre au point une réponse mondiale au problème du pollupostage.

SECTION 3

La corbeille juridique

LA CORBEILLE JURIDIQUE

Presque tous les aspects de la gouvernance de l'Internet comporte une dimension juridique, pourtant la formulation d'une réponse juridique aux développements rapides de l'Internet en est encore à ses balbutiements. Les deux approches dominantes concernant les aspects juridiques de l'Internet sont les suivantes:

a) Une approche de "droit réel", suivant laquelle l'Internet est en fait traité exactement comme les technologies des télécommunications antérieures, depuis les signaux de fumée jusqu'au téléphone. Bien qu'il soit plus rapide et plus détaillé, le principe de l'Internet est le même: il permet la communication entre plusieurs individus sur une certaine distance. Par conséquent, les règles juridiques existantes peuvent s'appliquer à l'Internet.

b) Une approche de "droit cybernétique" qui part du principe que l'Internet introduit de nouveaux types de liens sociaux dans le cyberespace. Par conséquent, il devient nécessaire de formuler de nouvelles "lois cybernétiques" spécialement façonnées pour le cyberespace. Un argument en faveur de cette approche est lié au fait que, de par la vitesse et le volume des communications transfrontières facilitées par l'Internet, l'application des règles juridiques existantes se trouve entravée

Bien que chacune de ces approches présente des arguments valides, l'approche du droit réel finit par avoir gain de cause tant du point de vue de l'analyse théorique qu'en termes de politique. L'opinion générale est qu'une forte proportion de la législation existante peut s'appliquer à l'Internet. Dans certains cas toutefois, comme par exemple la protection des marques déposées, les règles du droit réel devront être adaptées pour pouvoir s'appliquer au monde cybernétique. D'autres cas, par exemple le pollupostage, doivent être réglementés par des règles nouvellement conçues. En effet, le phénomène très proche du spam dans le monde réel, celui du courrier publicitaire, n'a rien d'illégal.

Cette discussion sur les considérations juridiques de l'Internet se divise en deux parties: les mécanismes juridiques et les questions juridiques.

MECANISMES JURIDIQUES

Les mécanismes juridiques suivants ont déjà été appliqués à la gouvernance de l'Internet ou bien ils pourraient l'être:

- Législation;
- Normes sociales (coutumes);
- Autorégulation;
- Réglementation par le biais d'un code (solution logicielle) (voir p. 22);
- Jurisprudence (décisions du tribunal);
- Droit international.

Législation

Chaque instrument législatif est constitué de règles et de sanctions. Les règles stipulent certains comportements acceptés (ne pas commettre de délit, payer ses impôts) et les sanctions stipulent les punitions en cas de manquement à ces règles (par ex. amendes, emprisonnement, peine de mort).

Les travaux législatifs se sont progressivement intensifiés dans le domaine de l'Internet. Ceci vaut tout particulièrement pour les pays de l'OCDE où les TIC se sont généralisées et ont un niveau d'impact élevé sur les relations économiques et sociales. A ce jour, les domaines prioritaires pour la réglementation législative ont été le respect de la vie privée, la protection des données, la propriété intellectuelle, la fiscalité et la cybercriminalité.

Indépendamment de la question de savoir si c'est l'approche du "droit réel" ou du "droit cybernétique" qui est la plus appropriée, un principe général demeure: la loi ne rend pas les comportements interdits impossibles, elle les rend simplement punissables. Le fait que la fraude soit interdite aussi bien dans le monde "réel" que dans le monde "cybernétique" ne veut pas dire pour autant que la fraude pourra être éradiquée. Cette distinction est pertinente car l'un des arguments fréquemment invoqués en faveur d'une réglementation cybernétique distincte repose sur le fait que le comportement interdit (fraude, crime, etc.) est déjà répandu dans le cyberespace et que le droit "réel" ne peut pas être utilisé avec efficacité.

Pourtant, les relations sociales sont trop complexes pour être uniquement réglementées par les législateurs. La société est dynamique et la législation est toujours à la traîne par rapport au changement. Cela se fait tout particulièrement sentir à notre époque où les progrès technologiques transforment la réalité sociale beaucoup plus rapidement que ne peuvent réagir les législateurs. Parfois, les règles deviennent caduques avant même de pouvoir être adoptées. Le risque d'obsolescence ju-

ridique est donc un facteur important lorsque l'on considère la réglementation de l'Internet.

Gouvernance de la société del'information

La loi est toujours à la traîne de la technologie

Normes sociales (Coutumes)

Tout comme la législation, les normes sociales prescrivent certains comportements. A la différence de la législation, aucun pouvoir national n'est chargé de faire appliquer ces normes. Elles sont appliquées par la communauté par le jeu de pressions exercées par l'entourage. A ses débuts, l'Internet était régi par un ensemble de normes sociales qui s'appelait "nétiquette", selon lequel les pressions de l'entourage et les risques d'exclusion étaient les principales sanctions. A cette période, l'Internet était avant tout utilisé par des communautés principalement universitaires et relativement restreintes, de sorte que les règles sociales étaient généralement respectées. La croissance de l'Internet a rendu ces règles inefficaces. Ce type de réglementation peut toujours être utilisé mais seulement au sein de groupes restreints ayant des liens communautaires très forts.

Autorégulation

Le livre blanc du gouvernement américain sur la gouvernance de l'Internet (1998) donne la préférence à l'autorégulation comme mécanisme de réglementation de l'Internet. L'autorégulation présente des similitudes avec les normes sociales décrites précédemment. Le principal écart tient au fait qu'à la différence des normes sociales, qui impliquent généralement un système réglementaire plutôt diffus, l'autorégulation est fondée sur une approche délibérée et bien structurée. Les règles de ce système sont généralement codifiées par le biais de codes de pratique ou de bonne conduite.

Le mouvement en faveur de l'autorégulation est tout particulièrement suivi au sein des fournisseurs d'accès à l'Internet (FAI). Dans bon nombre de pays, les FAI font de plus en plus l'objet de pressions de la part

des pouvoirs publics pour faire appliquer des règles ayant trait à la politique du contenu. Les FAI ont donc de plus en plus recours à l'autorégulation comme méthode pour imposer certaines normes de comportement et, finalement, pour empêcher l'ingérence du gouvernement dans leurs activités.

Si l'autorégulation peut certes être une technique réglementaire utile, il subsiste certains risques associés à son utilisation pour la réglementation des domaines d'intérêt public de premier plan, comme la politique du contenu. Il reste à voir dans quelle mesure les FAI seront capables de réglementer le contenu hébergé sur leurs sites Web. Peuvent-ils prendre des décisions en lieu et place des autorités légales? Peuvent-ils décider de ce qui constitue ou non un contenu acceptable? D'autres questions doivent aussi être examinées de plus près: la liberté d'expression et le respect de la vie privée.

Jurisprudence

La jurisprudence (les décisions des tribunaux) constitue un élément important du système juridique américain, le premier à se pencher sur les enjeux juridiques de l'Internet. Dans ce système, les précédents créent la loi, surtout dans les affaires ayant trait à la réglementation de nouvelles questions, telles que l'Internet. Les juges doivent trancher dans des affaires même s'ils n'ont pas tous les outils nécessaires pour le faire - à savoir les règles juridiques à appliquer.

Le premier outil juridique dont se servent les juges est l'analogie juridique, qui leur permet de comparer un nouveau concept à quelque chose qui leur est familier. La plupart des affaires concernant l'Internet ont été résolues par le biais d'analogies. Le lecteur trouvera une liste d'analogies aux pages 23 à 26.

La réglementation internationale

Un avis souvent exprimé à propos de la gouvernance de l'Internet tient au fait que l'Internet, de part son caractère global, exige une réglementation à l'échelle mondiale. La nécessité d'une approche universelle est fréquemment démontrée par le manque d'efficacité des mesures nationales contre le pollupostage ou la cyberdélinquance et autres activités indésirables. Le régime de l'aviation civile est souvent donné comme exemple d'un régime universel couronné de succès pour combattre la criminalité. "Depuis l'adoption des traités de l'aviation civile, le sabotage et les actes d'immix-

tion illégitimes ont progressivement reculé." L'une des principales raisons tient au fait que, grâce à la portée juridique universelle de l'aviation civile, les criminels ne peuvent plus trouver de "refuge" aussi facilement. Néanmoins, l'importance d'une approche mondiale ne signifie pas pour autant que certaines questions ne peuvent ou ne doivent pas être réglementées à l'échelle nationale ou régionale.

La réglementation mondiale exigera un consensus universel, qui ne pourra être obtenu qu'au terme d'un processus de négociation de longue haleine, pour autant qu'il puisse l'être. Divers mécanismes juridiques internationaux pourraient servir au développement d'un régime de gouvernance de l'Internet. D'après le Statut de la Cour internationale de Justice, les ressources juridiques internationales sont divisées en conventions, en coutumes et en principes généraux. En plus de cela, on trouve le "droit mou", en anglais "soft law", qui constitue une ressource de plus en plus importante du droit international.

Le droit des traités. Actuellement, la seule Convention qui soit axée directement sur des questions ayant trait à l'Internet est la Convention du Conseil de l'Europe sur la cybercriminalité. D'autres conventions et traités sont seulement en partie applicables à l'Internet. A titre d'exemple, prenons l'ensemble des conventions sur les droits de l'homme. La liberté d'expression est protégée par l'article 19 du Pacte international sur les droits civils et politiques. D'autres droits associés à l'Internet, tels que le respect de la vie privée et le droit à l'information sont réglementés par des instruments régionaux ou mondiaux sur les droits de l'homme. Dans le domaine du règlement des différends, l'un des principaux instruments est la Convention de New York pour la reconnaissance et l'exécution de sentences arbitrales étrangères.

Finalement, l'approche qui prévaudra en matière de gouvernance de l'Internet (national c. international, droit mou c. droit dur) influencera le type et la forme de toute convention éventuelle sur la gouvernance de l'Internet. D'aucuns soutiennent que l'Internet exigera un instrument juridique exhaustif, tel que la Convention sur le droit de la mer. Toutefois, cette analogie n'est pas opportune, car la négociation de la Convention du droit de la mer a nécessité la codification du droit coutumier existant et l'intégration de quatre conventions existantes.

Dans le cas de l'Internet, il n'existe pas de droit coutumier. Il est constamment façonné. D'innombrables approches et des expériences par tâtonnements sont tentées. Au lieu de déboucher sur un traité exhaustif sur

l'Internet, il est fort probable que l'on adoptera plusieurs instruments séparés.

Droit coutumier. L'élaboration du droit coutumier se fait le plus souvent sur une période plus longue pour permettre la cristallisation de certaines pratiques légalement contraignantes. Cela était certes possible dans le passé. Toutefois, les progrès technologiques depuis la Seconde Guerre mondiale ont nécessité l'élaboration rapide de cadres réglementaires internationaux, du fait des profondes conséquences économiques et politiques que ces changements engendrent en un laps de temps très court. L'Internet est un bon exemple de cette tendance. Il n'est guère probable que le droit coutumier jouera un rôle prépondérant dans le régime de gouvernance de l'Internet à naître.

"Droit mou". Le droit mou est habituellement associé à divers documents politiques, tels que des déclarations, des lignes directrices ou des lois types. Le critère linguistique pour identifier une loi molle n'est autre que l'emploi fréquent du mot "devrait" au lieu du mot "doit", qui est souvent associé à une approche légalement contraignante codifiée dans le droit "dur" (traités et conventions).

Bon nombre d'exemples d'accords de droit mou ont été respectés par les Etats parties. Certains d'entre eux revêtent une importance considérable, comme c'est le cas de l'Acte final d'Helsinki de 1975, qui établit le cadre des relations est-ouest. Le droit mou est utilisé par les Etats pour diverses raisons, telles que le renforcement de la confiance mutuelle, la dynamisation des progrès en cours et l'introduction de nouveaux mécanismes juridiques et gouvernementaux. Le droit mou pourrait être une technique juridique applicable à la gouvernance de l'Internet.

JURIDICTION

INTRODUCTION

La juridiction est la question de gouvernance de l'Internet qu'il est le plus urgent de traiter. Le nombre de différends liés à l'Internet ne cesse d'augmenter. La confusion qui règne en termes de juridiction pourrait avoir deux conséquences immédiates:

- rendre l'Etat incapable d'exercer son pouvoir légal en tant qu'entité responsable de la réglementation des relations sociales sur son propre territoire;
- rendre les particuliers et les entités juridiques incapables d'exercer leur droit à la justice (déni de justice).

D'autres conséquences potentielles d'une juridiction ambiguë pourraient être:

- la création d'un climat d'insécurité juridique sur l'Internet;
- le freinage du développement du commerce électronique;
- le cloisonnement de l'Internet en zones juridiques sûres.

Quel est le lien entre la juridiction et l'Internet?

La juridiction est essentiellement fondée sur la division géographique du globe en territoires nationaux. Chaque Etat a le droit souverain d'exercer sa propre juridiction sur son territoire. Toutefois, l'Internet facilite considérablement les échanges transfrontières, qui deviennent difficiles (mais non impossibles) à contrôler par le biais des mécanismes gouvernementaux traditionnels. La question de la juridiction sur l'Internet met en lumière l'un des principaux dilemmes associés à la gouvernance de l'Internet: comment peut-on "ancrer" l'Internet au sein de la géographie politique et juridique existante?

Juridiction - Techniques de base

La juridiction présente trois aspects principaux:

- Quel tribunal ou quel pouvoir de l'Etat dispose de l'autorité adéquate? (juridiction procédurale);
- Quelles règles devraient être appliquées ? (juridiction de fond);
- Comment les décisions du tribunal devraient-elles être appliquées? (juridiction d'application).

Les principaux critères suivants servent à déterminer la juridiction dans des circonstances particulières:

- Le lien territorial - le droit d'un Etat de statuer sur des personnes ou des biens à l'intérieur de son territoire;
- Le lien personnel - le droit d'un Etat de gouverner ses citoyens où qu'ils puissent se trouver;
- Le lien d'effets - le droit d'un Etat de gouverner sur les effets économiques et juridiques d'un territoire particulier, découlant d'activités réalisées ailleurs.

Un autre principe important du droit international moderne est le principe de la juridiction universelle dans les dossiers concernant des violations des normes juridiques internationales fondamentales (ius cogens), telles que le génocide et la piraterie.

LA SITUATION ACTUELLE

Des problèmes de juridiction surviennent lorsque des différends portent sur un élément extraterritorial (concernant par ex. des individus de plusieurs Etats différents ou des transactions internationales). Lorsqu'un contenu est affiché sur le Web, il est difficile de savoir quel droit national risque d'être violé, le cas échéant. Tout le contenu de l'Internet est accessible depuis n'importe quel point du globe. Dans ce contexte, presque toute activité sur l'Internet comporte un aspect international qui pourrait déboucher sur des juridictions multiples ou déclencher une réaction en chaîne.

Les deux affaires les plus parlantes et les plus fréquemment citées pour illustrer le problème de la juridiction sont l'affaire CompuServe de 1996 en Allemagne et l'affaire Yahoo! de 2001 en France.

Dans l'affaire CompuServe, un tribunal allemand a demandé à CompuServe d'interdire l'accès à du matériel pornographique. Pour faire observer la loi allemande, CompuServe se vit obligé de retirer le matériel de son serveur central aux Etats-Unis. De ce fait, il empêchait l'accès non seulement aux personnes habitant en Allemagne mais aussi aux citoyens vivant dans des pays (par ex. les Etats-Unis) où l'accès au matériel pornographique n'était pas interdit par la loi. CompuServe se vit dans l'obligation d'accepter la législation la plus restrictive dans ce domaine. Cette affaire déclencha la crainte de voir la totalité de l'Internet être soumis à la législation la plus restrictive (le principe du dénominateur le moins commun).

Quelques affaires récentes, y compris l'affaire Yahoo! jugée devant les tribunaux français, ont encore souligné la pertinence du problème des juridictions multiples. L'affaire Yahoo! fut déclenchée par une violation de la législation française concernant la distribution de propagande nazie. Ces lois empêchaient quiconque résidait en France d'accéder à un site Web hébergé par Yahoo! affichant des souvenirs à la gloire des Nazis, alors même que le site Web était hébergé aux Etats-Unis, où l'affichage de ce genre de matériel était, et reste encore, légal.

L'approche du droit réel soutient qu'aucun élément nouveau ne ressort d'affaires comme celle de CompuServe, puisque de nombreux exemples de réaction en chaîne se produisent en dehors du cyberespace. Un exemple célèbre concerne l'imposition par la Commission de l'UE de conditions strictes pour la fusion entre Boeing et McDonnell Douglas qui avait pourtant été approuvée par les autorités américaines. Bien qu'aucune des deux sociétés n'ait eu d'usines de production en Europe, elles durent tout de même observer la loi communautaire sur la concurrence pour pouvoir vendre des appareils à l'UE.

Si le raisonnement du "droit réel" est tout à fait sain en théorie, il présente toutefois de graves lacunes dans la pratique, susceptibles de brider l'applicabilité de la loi existante à l'Internet. Le principal problème concerne le volume gigantesque d'affaires potentielles liées à l'Internet, presque tout service ou tout site Web se trouvant exposé à une action légale potentielle en un point du globe. Par conséquent, il se peut que cet aspect quantitatif (le nombre de procès) remette en question le principe juridique et invite à trouver de nouvelles solutions.

SOLUTIONS POTENTIELLES

Des solutions potentielles au problème de juridictions multiples dans le contexte de l'Internet pourront peut-être venir:

- de la modernisation du droit privé international;
- de l'harmonisation des lois nationales, ce qui rendrait la question de la juridiction moins pertinente;
- du recours à l'arbitrage;
- de l'usage de solutions techniques pour identifier l'origine des utilisateurs (en premier lieu par le biais de logiciels de géolocalisation) (voir p. 125).

La modernisation du droit privé international

Dans les procédures judiciaires classiques, les tribunaux nationaux décident s'ils peuvent juger une affaire donnée et quelles règles devraient s'appliquer à la décision judiciaire. Les décisions qui concernent la juridiction procédurale et la juridiction de fond sont fondées sur le droit privé international ("conflit des lois" dans les systèmes juridiques anglo-saxons). Ces règles stipulent les critères permettant de déterminer la juridiction, tels que le lien entre le particulier et la juridiction nationale (par ex. nationalité, domicile) ou le lien entre une transaction particulière et la juridiction nationale (par ex. le lieu où le contrat a été passé, le

lieu où s'est déroulé l'échange). L'Internet rend l'application de ces critères plus complexe que dans les affaires classiques, mais pas impossible pour autant.

L'approche classique est rarement utilisée pour régler des différends ayant trait à l'Internet en raison de sa complexité, de sa lenteur et de son coût élevé. Elle ne cadre pas avec le modus operandi de l'Internet, qui est rapide, simple et pragmatique. Les principaux mécanismes du droit privé international ont été développés à une époque où l'interaction transfrontière était moins fréquente et moins intense. Proportionnellement parlant, il y avait moins d'affaires qui portaient sur des particuliers ou des entités émanant de juridictions différentes. Avec l'avènement de l'Internet, l'interaction transfrontière devient une affaire banale. Les communications, les échanges et les différends entre des institutions et des particuliers de différents pays sont beaucoup plus fréquents et beaucoup plus intenses qu'auparavant.

Une solution possible pourrait être la modernisation du droit privé international afin d'avoir un processus rapide et à faible coût pour l'attribution de juridiction nationale dans des affaires Internet. Des améliorations possibles pourraient comprendre des procédures simplifiées pour recenser les juridictions appropriées, l'option de délibérations en ligne et des arrangements souples de conseil juridique.

Au plan régional, l'Union européenne a adopté la Convention de Bruxelles qui simplifie le processus visant à aboutir à une décision concernant la juridiction et plaide en faveur de la protection des clients dans le cas du commerce électronique.

Au niveau mondial, le principal forum pour le remaniement du droit privé international est la Conférence de la Haye. Les négociations actuelles ont été dominées par les Etats-Unis. En 1992, les Etats-Unis ont amorcé des négociations sur la juridiction avec pour objectif premier le renforcement de la protection des droits de propriété intellectuelle par le biais d'une application universelle des décisions des tribunaux américains. Depuis 1992, la croissance de l'Internet et du commerce électronique a radicalement transformé la scène des négociations. Il devient de plus en plus hasardeux pour des compagnies Internet américaines d'agir dans un environnement à juridictions multiples. Les procès intentés contre CompuServe (Allemagne) et Yahoo! (France) ont démontré en quoi le contenu hébergé aux Etats-Unis pouvait déclencher des actions en justice dans des pays tiers.

Si la proposition initiale de la Convention de La Haye venait à être adoptée, cela poserait un défi considérable au système judiciaire américain. Les tribunaux américains seraient obligés de faire appliquer les décisions judiciaires étrangères qui porteraient sur du contenu hébergé sur des sites Web américains et finalement de remettre en question le principe même de liberté d'expression garanti par le Premier Amendement de la Constitution américaine. L'initiative a eu pour conséquence inattendue de provoquer un changement dans la position américaine, qui a tempéré ses ambitions de réformer le système de droit privé international. Le manque de progrès dans la modernisation du droit privé international au niveau mondial pourrait venir renforcer les autres options avancées afin de résoudre les conflits en matière de juridiction.

Les "pavillons de complaisance" de l'Internet

Une autre conséquence possible du manque d'harmonisation sera la migration des "données" et du contenu du Web vers des pays ayant un degré inférieur de contrôle du contenu. Si l'on reprend l'analogie du droit de la mer, certains pays pourraient devenir les "pavillons de complaisance" ou les centres "offshore" du cyberespace.

L'harmonisation des lois nationales

L'harmonisation des lois nationales devrait se traduire par l'élaboration d'une série de règles équivalentes au niveau mondial. Avec des règles identiques en place, la question de la juridiction devient moins pertinente. Il est possible d'arriver à une certaine harmonisation dans les domaines où il existe déjà un degré élevé de consensus mondial, par exemple, en ce qui concerne la pornographie juvénile, la piraterie, l'esclavage, le terrorisme et la cybercriminalité. Les opinions se rejoignent aussi sur d'autres questions, comme le pollupostage et la sécurité de l'Internet. Toutefois, dans certains domaines, y compris la politique du contenu, il semble bien improbable de pouvoir arriver à un consensus mondial sur les règles fondamentales.

Une autre option pour tenter de résoudre le problème de juridiction concerne l'arbitrage, que nous abordons ci-dessous.

ARBITRAGE

L'arbitrage est un autre mécanisme possible de règlement des différends. Il peut servir en guise d'alternative à des procédures judiciaires généralement longues et complexes. Dans l'arbitrage, les décisions sont prises par au moins un individu indépendant mais désigné par les parties en litige. L'arbitrage international au sein du secteur des affaires jouit d'une tradition qui remonte à loin. Un mécanisme d'arbitrage est habituellement énoncé dans un contrat privé et les parties au contrat conviennent de régler tout différend à venir par le biais d'une procédure arbitrale. Il existe une grande variété de contrats d'arbitrage, qui stipulent des questions comme le lieu d'arbitrage, les procédures et le tribunal compétent.

Les arbitrages en ligne sont également utilisés pour résoudre non seulement des différends Internet mais aussi des litiges commerciaux ordinaires. L'arbitrage en ligne se déroule intégralement sur l'Internet, y compris la présentation des preuves et les décisions.

L'un des principaux avantages de l'arbitrage tient au fait qu'il surmonte le problème de la sélection d'une juridiction procédurale et substantielle. Les deux sont sélectionnées à l'avance par les parties au contrat.

L'arbitrage présente des avantages particuliers vis-à-vis de l'une des tâches les plus délicates des affaires judiciaires liées à l'Internet, à savoir l'application des décisions (sentences). L'application des sentences arbitrales est réglementée par la Convention de New York pour la reconnaissance et l'exécution des sentences arbitrales étrangères, signée par la majorité des pays. D'après cette Convention, les tribunaux nationaux sont obligés de faire appliquer les sentences arbitrales. Il est ainsi plus simple de faire appliquer les sentences arbitrales que les décisions de tribunaux étrangers.

L'arbitrage a été utilisé à maintes reprises afin de combler la lacune créée par l'inaptitude du droit privé international existant à traiter des affaires liées à l'Internet. Un exemple parlant d'utilisation de la procédure d'arbitrage pour la résolution d'affaires Internet est l'UDRP (Uniform Domain-Name Dispute-Resolution Policy). L'UDRP a été mise au point par l'OMPI et mise en œuvre par l'ICANN en tant que procédu-

re primordiale de résolution des litiges. L'UDRP est désignée à l'avance comme mécanisme de règlement des différends dans tous les contrats impliquant l'enregistrement de gTLD (.com, .edu, .org, .net). L'aspect unique réside dans le fait que les sentences arbitrales sont appliquées directement par le biais de changements dans le système de noms de domaine sans avoir recours à une exécution forcée par le biais des tribunaux nationaux.

Globalement, l'arbitrage offre une solution plus rapide, plus simple et meilleur marché pour résoudre les litiges. Cependant, l'utilisation de l'arbitrage comme principal mécanisme de règlement des différends sur l'Internet présente quelques graves limitations.

Tout d'abord, compte tenu du fait que l'arbitrage est généralement convenu au préalable, il ne couvre pas la multitude de cas où il s'avère impossible d'aboutir à un accord préalable entre les parties (diffamation, différents types de responsabilité, cyberdélinquance).

Deuxièmement, nombreux sont ceux qui considèrent que la pratique actuelle qui consiste à annexer une clause d'arbitrage aux contrats ordinaires porte préjudice à la partie contractante la plus faible (en principe, il s'agit de l'utilisateur de l'Internet ou du client dans le cas d'une transaction en ligne).

Troisièmement, certains craignent que l'arbitrage n'étende le droit basé sur les précédents à l'échelle mondiale pour supprimer progressivement les autres systèmes juridiques nationaux. Dans le cas du droit commercial, ceci pourrait s'avérer plus acceptable, compte tenu du niveau déjà élevé d'harmonisation au niveau des règles de fond. Toutefois, cela deviendrait une tâche beaucoup plus délicate en ce qui concerne le contenu et les aspects socioculturels, où le système juridique national reflète une teneur culturelle spécifique.

Quatrièmement, la jurisprudence existante concernant l'Internet suggère que les procédures arbitrales, telles que celles fondées sur l'UDRP, ont été plus à l'écoute des intérêts du monde des affaires que de ceux des particuliers. Ci-après figure un exemple qui a trait à deux cas très semblables. Tout d'abord, un tribunal ordinaire français s'est prononcé contre la société française "Danone" et en faveur d'un employé vexé qui avait décidé de faire enregistrer le domaine "jeboycottedanone.com". Pourtant, dans le cadre d'une deuxième affaire, la sentence arbitrale de l'OMPI (fondée sur la procédure UDRP) a accepté la requête de Vivendi Universal de retirer le site Web "vivendiuniversalsucks.com" [Vivendi Univer-

sal c'est nul]. Dans les deux cas, les noms de domaine ont été utilisés comme moyen de protester et de critiquer. Un tribunal ordinaire en France a accepté ce type de protestation alors que la procédure arbitrale de l'OMPI l'a rejeté.

DROITS DE PROPRIETE INTELLECTUELLE

Le savoir et les idées sont les ressources clés de l'économie mondiale. Leur protection, par le biais des droits de propriété intellectuelle (DPI), s'impose de plus en plus comme l'un des enjeux les plus importants de l'Internet, avec des conséquences juridiques et politiques considérables. Les enjeux liés aux DPI englobent différents aspects qui touchent à la gouvernance de l'Internet. Sachant que le savoir et les idées sont un élément crucial de notre patrimoine culturel et de notre interaction sociale, ils conservent une valeur toute particulière pour bon nombre de sociétés. Les DPI sont aussi au cœur du débat sur le développement. Les DPI liés à l'Internet comprennent les marques déposées, les droits d'auteur et les brevets.

MARQUES DEPOSEES

La pertinence des marques déposées dans le contexte de l'Internet est liée à l'enregistrement des noms de domaine. Dans les débuts du développement de l'Internet, l'enregistrement des noms de domaine se faisait selon le principe du "premier arrivé, premier servi". Ceci a donné lieu au cybersquattage, pratique qui consiste à faire enregistrer des noms de sociétés commerciales pour les revendre par la suite à un prix plus élevé. Du fait de l'importance croissante de l'Internet, ce phénomène est devenu un problème majeur, car les sociétés devenaient susceptibles d'être représentées de façon erronée sur l'Internet. Les recours juridiques par l'intermédiaire des tribunaux ordinaires n'étaient guère pratiques car ces affaires prenaient trop de temps à résoudre.

Cette situation a obligé le monde des affaires à porter la question de la protection des marques au cœur même de la réforme de la gouvernance de l'Internet, ce qui a débouché sur la création de l'ICANN en 1998. Dans son livre blanc sur l'ICANN, le gouvernement américain demande à l'ICANN d'élaborer et de mettre en œuvre un mécanisme pour la protection des marques vis-à-vis des noms de domaine. Peu de temps après sa création, l'ICANN a introduit la procédure UDRP (Uniform Domain-Name Dispute-Resolution Policy) mise au point par l'OMPI.

Le recours à l'UDRP en guise de mécanisme de règlement des différends était une clause devant obligatoirement figurer dans tous les contrats d'enregistrement de domaine pour les domaines de niveau supérieur comme .com, .org et .net. Les titulaires de marques ont promu l'élargissement de l'application de la procédure UDRP aux domaines nationaux.

Les marques sont abordées dans d'autres sections du présent livret:

- le système des noms de domaine (DNS) (p. 41);
- la procédure UDRP (Uniform Domain-Name Dispute-Resolution Policy) (p. 79).

DROITS D'AUTEUR

Le concept traditionnel de droits d'auteur a été remis en cause de multiples façons par les développements liés à l'Internet, qu'il s'agisse simplement des opérations de "couper-coller" à partir du Web ou d'activités plus complexes, comme la distribution de fichiers audio ou vidéo par le biais du Net. Les fichiers peuvent être copiés et distribués dans le monde entier par le truchement de l'Internet sans coûts notables.

Ces développements compromettent l'équilibre délicat entre les intérêts des auteurs de matériel protégé et les intérêts du public associés à une plus

Les droits d'auteur protègent uniquement l'expression d'une idée matérialisée sous diverses formes, qu'il s'agisse d'un livre, d'un cédérom, d'un fichier informatique, ou autre. L'idée elle-même n'est pas protégée par les droits d'auteur.

grande créativité, un plus grand savoir et son bien-être général. La prévention de la copie illimitée du matériel et, dans le même temps, la sauvegarde de l'accès à ce matériel sur Internet, est l'un des dilemmes que doit résoudre la gouvernance de l'Internet. Jusqu'ici, les détenteurs de droits d'auteur, représentés par les grosses maisons de disque et les gros groupes multimédias, se sont montrés plus dynamiques dans la protection de leurs intérêts. L'intérêt du public n'est perçu que très vaguement et n'est pas suffisamment protégé.

L'un des développements ayant fait date dans le domaine des droits d'auteur, qui a déclenché une réponse massive et immédiate des détenteurs, a été l'échange de fichiers de musique par le biais de réseaux poste à poste. Il est estimé que Napster, l'exemple par excellence, a engendré des pertes à hauteur de 4,3 milliards de dollars pour l'industrie du disque. La réaction de l'industrie a mis en exergue les innombrables pièges, les analogies erronées et les lacunes du système juridique actuel. La situation a aussi illustré où en était la protection des droits d'auteur sur l'Internet en touchant du doigt les nombreuses questions qui restent à résoudre.

LA SITUATION ACTUELLE

Une protection plus stricte des droits d'auteur au niveau national et international

Les industries de l'enregistrement et du divertissement ont exercé de très vives campagnes de pression au niveau national et international pour renforcer la protection des droits d'auteur. Aux Etats-Unis, une protection plus stricte des droits d'auteur a été introduite par le biais de la Loi américaine de 1998 sur les droits d'auteur pour le millénaire numérique (DMCA). Au niveau international, la protection des articles numériques a été introduite dans le Traité de l'OMPI sur le droit d'auteur (1996). Ce traité prévoit également des dispositions pour le durcissement du régime de protection des droits d'auteur, par exemple avec l'introduction de clauses plus strictes de limitations des droits exclusifs des auteurs, l'interdiction de contourner les dispositifs technologiques de protection des droits d'auteur et autres mesures semblables.

Le nombre croissant de procès

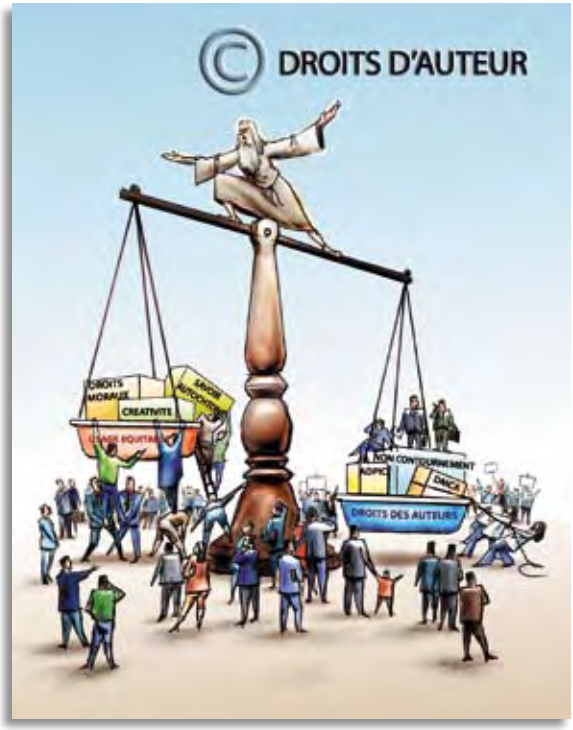
Ne serait-ce qu'en 2003, environ 1000 assignations liées à la DMCA ont été délivrées à l'encontre de fournisseurs d'accès, pour les adjoindre de met-

tre un terme aux activités de partage de fichiers de leurs abonnés et plus de 500 procès ont été intentés contre des particuliers.

Une affaire tout particulièrement pertinente pour l'avenir des droits d'auteur sur l'Internet concerne le procès intenté contre Grokster et StreamCast, deux sociétés qui produisent des logiciels de partage de fichier P2P. Suite aux dispositions de la DMCA, l'Association américaine des enregistrements sonores a prié ces sociétés de renoncer au développement de la technologie de partage des fichiers qui contribue à la violation des droits d'auteur. Au départ, sous réserve de circonstances raisonnables, les tribunaux américains ont préféré ne pas tenir des éditeurs de logiciel comme Grokster et StreamCast responsables des violations éventuelles de droits d'auteur. Toutefois, en juin 2005, la Cour suprême des Etats-Unis a statué que les éditeurs de logiciel étaient responsables de tout usage abusif éventuel de leurs programmes.

Logiciel contre les violations de droits d'auteur

Les outils qui peuvent être utilisés par les contrevenants peuvent aussi être employés par les défenseurs des droits d'auteur. De par tradition, les pouvoirs publics et les sociétés ont honoré leurs responsabilités par le biais de mécanismes juridiques. Toutefois, l'usage d'outils logiciels "alternatifs" par le monde des affaires contre les bafoueurs de droits d'auteur se vulgarise.



Un article paru dans le International Herald Tribune recensait les stratagèmes logiciels suivants,

utilisés par l'industrie de l'enregistrement et du divertissement pour protéger ses droits d'auteur:

- un cheval de Troie, qui redirige les usagers vers les sites Web où ils peuvent faire l'achat légitime de la chanson qu'il tente de télécharger;
- un logiciel de "blocage" qui bloque l'ordinateur pendant un laps de temps et affiche une mise en garde contre le téléchargement de musique piratée;
- "silence", une technique par le biais de laquelle le disque dur est lu pour tenter de retirer tout fichier piraté susceptible de s'y trouver;
- "interdiction", une technique qui bloque l'accès à Internet de quiconque tente de télécharger de la musique piratée.

Le professeur Lawrence Lessig, de l'Université de droit de Stanford aux Etats-Unis, prévient que de telles mesures pourraient bien être elles-mêmes illégales. Il souligne que parmi les mesures ratifiées pour contrer la violation des droits d'auteur ne figurent aucune de celles mentionnées plus haut. Les sociétés amenées à prendre de telles mesures d'autoprotection seraient-elles jugées enfreindre la loi?

Technologies permettant la gestion des droits numériques

Comme approche à long terme plus structurelle, le monde des affaires a introduit différentes technologies pour la gestion de l'accès aux matériels protégés par droits d'auteur. Microsoft a introduit un logiciel de gestion des droits numériques pour gérer le téléchargement des fichiers audio, vidéo et autres matériels protégés par droits d'auteur. Des systèmes analogues ont été mis au point par Xerox (ContentGuard), Philips et Sony (InterTrust).

L'utilisation d'outils technologiques pour la protection des droits d'auteur a été reconnue tant au niveau international (Traité sur le droit d'auteur de l'OMPI) qu'au niveau de la loi américaine sur les droits d'auteur pour le millénaire numérique. Cette dernière va encore plus loin en ce sens qu'elle criminalise toute activité visant à contourner les dispositifs de protection du matériel protégé par droits d'auteur.

LES ENJEUX

Modifier les mécanismes de droits d'auteur existants ou en développer de nouveaux?

Comment faudrait-il ajuster les mécanismes de protection des droits d'auteur pour refléter les profonds changements intervenus suite aux progrès réalisés dans le domaine des TIC et de l'Internet? Une option suggérée par le livre blanc du gouvernement américain sur La propriété intellectuelle et les infrastructures nationales d'informations soutient que seules des modifications minimes sont requises, essentiellement afin de "dématérialiser" les concepts de "fixation", "distribution", "transmission" et "publication" associés aux droits d'auteur. Cette approche a été suivie dans les principaux traités internationaux sur les droits d'auteur, y compris les ADPIC et les Conventions sur les droits d'auteur de l'OMPI.

Toutefois, il existe un point de vue contraire qui soutient que les changements apportés au système juridique doivent être radicaux, puisque le concept de droit d'auteur dans le monde numérique ne réfère plus simplement au "droit d'empêcher la copie" mais aussi au "droit d'empêcher l'accès". Finalement, du fait des possibilités techniques toujours plus vastes qui permettent de restreindre l'accès au matériel numérique, on peut se demander si la protection des droits d'auteur a bien une raison d'être. Il reste à savoir comment l'intérêt du grand public, le deuxième élément de cette équation des droits d'auteur, sera finalement protégé.

Protection de l'intérêt public - Un "usage équitable" du matériel protégé par droits d'auteur

Les droits d'auteur ont d'abord été conçus pour stimuler la créativité et l'invention. C'est la raison pour laquelle ils conjuguent deux éléments: la protection des droits d'auteur et la protection des intérêts du public. Le principal défi consiste à stipuler comment le grand public pourrait consulter du matériel protégé par droits d'auteur pour améliorer sa créativité, son savoir et son bien-être général. D'un point de vue opérationnel, l'intérêt du public est protégé par le biais du concept "d'usage équitable" du matériel protégé. L'usage équitable est généralement défini comme une utilisation à des fins de recherche universitaire ou autres fins non commerciales.

Droits d'auteur et développement

Toute restriction de l'usage équitable pourrait affaiblir la position des pays en développement. L'Internet dote les chercheurs, les étudiants et les autres habitants des pays en développement d'un outil puissant pour participer aux échanges scientifiques et universitaires mondiaux. Un régime restrictif des droits d'auteur pourrait avoir des répercussions adverses sur le renforcement des capacités dans les pays en développement.

Un autre aspect concerne la numérisation accrue des arts culturels et artistiques des pays en développement. Il est paradoxal de constater que les pays en développement devront peut-être finir par payer pour le privilège d'accéder à leur patrimoine artistique et culturel lorsqu'il deviendra numérisé, reconditionné et protégé par des grands groupes étrangers de l'industrie du divertissement et des médias.

OMPI et ADPIC

Il existe deux régimes internationaux principaux pour la protection des droits d'auteur. L'Organisation mondiale de la propriété intellectuelle (OMPI) gère le régime classique des droits de propriété intellectuelle, sur la base des Conventions de Berne et de Paris. Un autre régime qui commence à s'imposer est celui géré par l'OMC et fondé sur les ADPIC. La transition de la coordination internationale des DPI de l'OMPI vers l'OMC est intervenue afin de renforcer la protection des DPI, tout particulièrement au plan de la mise en application. Ce développement fut l'un des principaux acquis des pays industrialisés durant le cycle d'Uruguay des négociations de l'OMC.

Bon nombre de pays en développement sont perturbés par cet état de fait. 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 droits de propriété intellectuelle 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'auteur

Les mécanismes internationaux de mise en application dans le domaine de la propriété intellectuelle ont encore été renforcés en rendant les FAI

responsables s'ils viennent à héberger du matériel qui viole des droits d'auteur, si le matériel n'est pas retiré sur notification de la violation. Cette mesure a donné au régime des DPI, qui jusque-là était vague, une force exécutoire immédiate dans le domaine de l'Internet.

BREVETS

En principe, un brevet protège un nouveau processus ou un nouveau produit d'une nature essentiellement technique ou manufacturière. Ce n'est que récemment que des brevets ont commencé à être accordés pour les logiciels. L'augmentation des dépôts de brevet donne lieu à un accroissement des procès chez les éditeurs de logiciel américains, portant sur des sommes d'argent colossales.

Du point de vue de la gouvernance de l'Internet, le principal développement a porté sur l'octroi très souple d'une protection par brevet des procédés commerciaux sur l'Internet, tels que la procédure "1-Clic" employée par Amazon.com. La principale critique de cette décision tient au fait qu'Amazon a seulement protégé l'idée (l'utilisation d'un seul clic), et non un processus commercial particulier.

Suite au dépôt réussi du brevet "1-Clic", on a assisté à une déferlante de dépôts de brevet, y compris des propositions totalement ridicules, par exemple une demande de brevet pour le téléchargement sur Internet. Un autre cas très controversé concerne la demande par British Telecom d'un droit de licence pour le brevet de liens hypertexte, qu'elle avait déposé dans les années quatre-vingt. Si British Telecom obtient gain de cause, les utilisateurs de l'Internet devront payer un droit pour chaque lien hypertexte qu'ils souhaiteront créer ou utiliser. Sinon, il fera date dans l'histoire à l'instar d'autres affaires célèbres comme la tentative de faire breveter la roue.

Il est important de souligner que la pratique qui consiste à faire breveter les logiciels ou les procédures associées à l'Internet n'est pas adoptée en Europe ni dans la majorité des autres pays.

CYBERCRIMINALITE

La technologie est mise au point pour pouvoir être utilisée mais il est aussi très fréquent qu'elle soit mal employée voire employée abusivement. En général, la cybercriminalité porte sur l'usage illicite des technologies de l'information et des communications. Si la composante "criminalité" du terme a été clairement définie (par ex. vol, pornographie juvénile), les avis quant à la signification de l'élément "cyber" sont multiples.

Dans le débat sur la cybercriminalité, il existe une dichotomie entre droit "réel" et droit "cybernétique". L'approche du droit réel affirme que la cybercriminalité est simplement un crime ordinaire, commis avec un ordinateur. Le délit est le même, seul l'outil est différent. Aux yeux du droit cybernétique, certains éléments uniques de la cybercriminalité font qu'elle justifie un traitement spécial, tout particulièrement en termes de répression et de prévention.

Les rédacteurs de la Convention sur la cybercriminalité du Conseil de l'Europe se sont voulus plus proches de l'opinion du droit réel, estimant que le seul aspect spécifique de la cybercriminalité est l'utilisation des TIC comme moyen de commettre un délit. La Convention, qui est entrée en vigueur le 1er juillet 2004, constitue le principal instrument international dans ce domaine.

La Convention réglemente la fraude informatique, les violations de droits d'auteur, la pornographie juvénile et la sécurité des réseaux. Le protocole récemment ajouté à la Convention porte aussi la distribution de contenu à caractère raciste ou xénophobe aux rangs des délits réglementés par la Convention.

La Convention stipule différents mécanismes procéduraux concernant les activités de répression criminelle des Etats, telles que l'échange de données associées à la cybercriminalité, y compris les journaux du trafic Internet. Des responsabilités particulières incombent aux fournisseurs d'accès à l'Internet dans ce régime de lutte contre la cyberdélinquance, y compris l'obligation de préserver les journaux Internet de leurs abonnés et de faciliter l'interception légale aux fins de recueillir des preuves. Res-

te à savoir si la Convention sera ratifiée par le Congrès des Etats-Unis; cette ratification serait un pas important en faveur d'une portée mondiale de la Convention.

Outre le Conseil de l'Europe, le G-8 a adopté un Plan d'action qui stipule une action concertée sur les crimes suivants associés à l'Internet: pédophilie et exploitation sexuelle, trafic de stupéfiants, blanchiment de capitaux, fraude électronique ainsi que l'espionnage industriel et national.

En 2003, l'OCDE a produit des lignes directrices afin d'aider les gouvernements à lutter contre la fraude sur l'Internet. L'Union européenne a entamé le processus d'adoption de la Décision cadre sur la cybercriminalité, pour renforcer les mesures pratiques et la coopération dans le domaine de la cyberdélinquance.

LES ENJEUX

Définition de la cybercriminalité

La définition de la cybercriminalité est l'un des enjeux primordiaux ayant un impact juridique pratique. Il existe des différences multiples et graves dans l'interprétation de la cyberdélinquance et ceci pourrait avoir des répercussions directes sur l'efficacité du régime international de lutte contre la cybercriminalité.

Ainsi par exemple, si la définition de la cybercriminalité met l'accent sur la méthode - par exemple l'accès non autorisé à des systèmes informatiques sécurisés - on court le risque de confondre la cybercriminalité avec l'hacktivisme (désobéissance civile numérique).

Cybercriminalité et droits de l'homme

La Convention sur la cybercriminalité a renforcé le débat sur le juste milieu entre la sécurité et les droits de l'homme. La société civile notamment s'est maintes fois déclarée soucieuse de voir que la Convention confère aux pouvoirs publics un pouvoir trop large, y compris le droit de contrôler les ordinateurs des hackers, la surveillance des communications, et plus encore. Ces vastes pouvoirs pourraient compromettre les droits de l'homme, notamment le droit au respect de la vie privée et à la liberté d'expression.

Collecte et sauvegarde des preuves

L'un des principaux défis que représente la lutte contre la cybercriminalité concerne la collecte de preuves destinées aux procès. De nos jours, la rapidité des communications exige une réaction fulgurante de la part des organismes chargés de faire appliquer la loi. Une possibilité pour la sauvegarde de la preuve se trouve dans les journaux du réseau qui fournissent des informations sur les personnes ayant accédé à telle ou telle ressource de l'Internet et à quel moment elles l'ont fait. La Convention sur la Cybercriminalité renferme un certain nombre de dispositions qui ont trait à cette question.

SIGNATURES NUMERIQUES

Globalement parlant, les signatures numériques sont liées à l'authentification des individus sur l'Internet, de sorte qu'elles ont des implications sur de nombreux aspects de l'Internet, y compris la juridiction, la cyberdélinquance et le commerce électronique. L'utilisation des signatures numériques devrait contribuer à renforcer la confiance accordée à l'Internet.

L'authentification numérique en général fait partie du cadre du commerce électronique. Elle devrait faciliter les transactions électroniques par la conclusion de marchés en ligne. Ainsi par exemple, un accord est-il valide et a-t-il force de loi s'il est réalisé par courrier électronique ou par le biais d'un site Web? Dans de nombreux pays, la loi exige que les contrats soient "écrits" ou "signés". Qu'est-ce que cela implique du point de vue de l'Internet?

Confrontés à de tels dilemmes et face aux pressions exercées pour les contraindre à créer un environnement propice au commerce électronique, nombre de gouvernements ont commencé par adopter une législation régissant les signatures

numériques. Le principal défi est lié au fait que les gouvernements ne cherchaient pas à réglementer un problème existant, comme la cybercriminalité ou les violations de droits d'auteur, mais ils s'efforçaient plutôt de créer un nouvel environnement dans lequel ils n'avaient aucune expérience pratique. Ceci a donné lieu à toute une kyrielle de solutions et à un manque de précision dans les dispositions ayant trait aux signatures numériques.

Les principales approches que l'on peut recenser concernant la réglementation des signatures numériques sont au nombre de trois. La première est une approche "minimaliste", qui stipule que les signatures électroniques ne peuvent pas être rejetées au seul motif qu'elles sont dans un format électronique. Cette approche énumère des applications très vastes et a été adoptée dans les pays de droit commun: Etats-Unis, Canada, Australie et Nouvelle-Zélande.

La deuxième approche est "maximaliste" et stipule un cadre et des procédures d'application pour les signatures numériques, y compris le cryptage et l'utilisation d'identifiants à clé publique. Cette approche stipule généralement l'établissement d'organismes de certification agréés qui peuvent certifier les futurs usagers d'une signature numérique. Cette approche prévaut dans la législation des pays européens, comme l'Allemagne et l'Italie.

La troisième approche, adoptée dans la directive de l'UE sur les signatures numériques, conjugue les deux approches qui précèdent. Elle comporte une disposition minimaliste pour la reconnaissance des signatures fournies par le biais d'un support électronique. L'approche maximaliste est aussi reconnue par le fait qu'il est admis que des "signatures électroniques avancées" auront un effet juridique plus puissant dans le système judiciaire (c.à.d. qu'il sera plus facile de prouver ces signatures en cas de procès).

La réglementation de l'UE concernant les signatures numériques a été l'une des réponses élaborées au niveau multilatéral. Si elle a certes été adoptée par tous les Etats membres de l'UE, il subsiste une différence dans le statut juridique des signatures numériques. Seuls huit pays ont mis en œuvre les conditions requises par la directive aux termes desquelles une signature numérique doit être traitée de la même façon qu'une signature ordinaire.

Au niveau mondial, en 2001, la CNUDCI (Commission des Nations Unies pour le droit commercial international) a adopté la loi type sur les signa-

tures électroniques. La loi type accorde le même statut aux signatures numériques qu'aux signatures manuscrites, sous réserve du respect de certaines conditions techniques.

La Chambre de commerce internationale (CCI) a publié un guide intitulé "General Usage in International Digitally Ensured Commerce" (GUIDEC), qui présente un tour d'horizon des meilleures pratiques ainsi que des problèmes ayant trait à la réglementation et à la certification dans ce domaine.

En corrélation directe avec le problème des signatures numériques figurent les initiatives d'infrastructure à clé publique (ICP). Deux organisations, l'UIT et l'IETF, travaillent dans le domaine de la normalisation des ICP.

LES ENJEUX

Besoin de normes d'application détaillées

Bien que de nombreux pays industrialisés aient adopté une vaste législation en matière de signature numérique, cette législation manque souvent de normes et procédures détaillées pour permettre sa mise en œuvre. Compte tenu de la modernité de ces problèmes, nombreux sont les pays qui attendent de voir dans quelle direction les normes vont effectivement se développer. Les initiatives de normalisation interviennent à différents niveaux, que ce soit à l'échelle des organisations internationales (l'UIT) ou des associations professionnelles (l'IETF).

Risque d'incompatibilité

La grande diversité des approches et des normes dans le domaine des signatures numériques pourrait déboucher sur l'incompatibilité des différents systèmes nationaux. Des solutions décousues pourraient finir par brider le développement du commerce électronique à l'échelle mondiale. Il serait bon que l'harmonisation qui s'impose soit assurée par le biais d'organisations régionales et mondiales.

DROIT DU TRAVAIL

Il est fréquemment déclaré que l'Internet change "notre façon de travailler". Si ce phénomène exige d'être approfondi, les aspects suivants ont une pertinence directe pour la gouvernance de l'Internet:

- L'Internet a engendré un niveau élevé de travailleurs temporaires et à contrat à durée déterminée. Le néologisme "temporaire permanent" a été inventé pour décrire des employés qui sont gardés pour de longues périodes sur la base de contrats à court terme constamment renouvelés. Cette notion introduit un échelon inférieur de protection sociale dans la main-d'œuvre.
- Le télétravail devient de plus en plus pertinent grâce aux progrès dans le domaine des télécommunications, notamment l'accès à l'Internet à haut débit.
- La sous-traitance à des pays tiers dans le secteur des services TIC, comme les centrales d'appels et les unités de traitement des données, ne cesse d'augmenter. Une proportion considérable de ces activités ont déjà été transférées vers des pays à faibles coûts, principalement l'Asie et l'Amérique latine.

Les TIC ont gommé la routine classique Travail, Loisirs, Repos (8+8+8 heures). Il est de plus en plus difficile de distinguer où commence le travail et où il s'arrête. Cette évolution des conditions de travail pourrait exiger une nouvelle législation du travail, pour traiter de questions comme 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 au travail constitue un enjeu majeur. Un employeur est-il en droit de surveiller l'utilisation de l'Internet par ses employés (par ex. le contenu de leurs messages électroniques ou leur accès aux sites Web)? La jurisprudence finit par s'étoffer progressivement dans ce domaine et de nouvelles solutions deviennent disponibles.

En France, au Portugal et en Grande-Bretagne, les consignes juridiques et un certain nombre d'affaires ont finalement eu pour conséquence de limiter la surveillance du courrier électronique des employés. L'employeur doit donner une mise en garde préalable de toute surveillance éventuelle. Au Danemark, les tribunaux ont jugé une affaire portant sur le licenciement d'un employé ayant envoyé des courriers électroniques privés et ayant accédé à un site de chat à orientation sexuelle. Le tribunal a statué que le renvoi n'était pas légal car l'employeur n'avait pas mis en place de politique d'utilisation de l'Internet qui interdisait tout usage non autorisé de l'Internet. Une autre logique appliquée par le tribunal danois tenait au fait que l'utilisation de l'Internet par l'employé n'affectait pas ses performances de travail.

De par tradition, le droit du travail se veut être une question nationale. Or, la mondialisation en général et l'Internet en particulier ont entraîné une internationalisation des questions prud'homales. Devant le nombre croissant de personnes travaillant pour des sociétés étrangères et en interaction avec des équipes de travail à l'échelle mondiale, le besoin d'établir des mécanismes réglementaires internationaux adéquats se fait de plus en plus sentir. Cet aspect a été reconnu dans la déclaration du SMSI, laquelle, au paragraphe 47, appelle au respect de toutes les normes internationales pertinentes dans le domaine du marché du travail des TIC.

RESPECT DE LA VIE PRIVEE ET PROTECTION DES DONNEES

Le respect de la vie privée et la protection des données sont étroitement liés aux enjeux de la gouvernance de l'Internet. La protection des données est un mécanisme juridique qui garantit le respect de la vie privée.

Qu'est-ce que le respect de la vie privée? La définition du respect de la vie privée dépend du point de vue de chacun. Certaines personnes n'ont pas d'objection à dévoiler certaines informations de nature privée, tandis que d'autres gardent leur vie privée plus jalousement. Le respect de la vie privée est également déterminé par les cultures nationales. Si la question du respect de la vie privée est importante dans les sociétés occidentales, elle peut revêtir une importance moindre dans d'autres cultures.

Néanmoins, même en tenant compte de ces réserves, il convient de définir la notion de respect de la vie privée pour pouvoir l'invoquer comme concept juridique. Les définitions varient beaucoup. Une définition classique décrit le respect de la vie privée comme "le droit d'être laissé tranquille". Les définitions modernes du respect de la vie privée se concentrent sur le caractère privé des communications (pas de surveillance des communications) et de l'information (par de manipulation des informations ayant trait aux particuliers). De par tradition, le respect de la vie privée se rapportait, le plus souvent, aux relations entre les citoyens (particuliers) et l'Etat. Toutefois, de nos jours, le cadre du respect de la vie privée s'est élargi et il englobe aussi désormais le secteur des affaires comme l'illustre le dessin à la page suivante.

Respect de la vie privée: entre les particuliers et l'Etat

Les informations ont toujours été une marchandise essentielle pour permettre aux pouvoirs publics de surveiller leur territoire et leur population. On peut s'en rendre compte dans les manuscrits les plus anciens, lesquels pour la plupart ont trait à des fonctions publiques. Les technologies de l'information ont énormément renforcé les capacités de l'Etat à collecter et analyser l'information. Ceci comprend à la fois les informations gérées par les services gouvernementaux (registres fiscaux, sociaux, de santé, immobiliers, pénaux) ainsi que les compagnies franchi-

sées par des gouvernements pour assurer des services critiques (électricité, eau, télécommunications).

Toutes ces informations sont recueillies avec l'accord tacite mais involontaire des citoyens car il leur est impossible de se soustraire à ces régimes, à moins d'émigrer vers un autre pays, où ils seraient, de toute façon, confrontés au même problème.

Les technologies, telles que l'entreposage des données, servent à cumuler et apparier les données d'un grand nombre de systèmes individuels (par exemple fiscalité, registres immobiliers, propriété de véhicule) afin de réaliser des analyses sophistiquées, de rechercher des modèles de comportement, des incohérences, des changements d'habitude et autres révélations de ce type. Elles pourraient avoir un impact spectaculaire sur la société et, dans la plupart des cas, elles demeurent dans le cadre de la Déclaration universelle des droits de l'homme.

Le terrorisme, l'espionnage et autres activités contre un Etat ont engendré une surveillance accrue des suspects (qu'ils soient ressortissants de l'Etat ou non). Les militants pour le respect des libertés civiles mettent en garde contre l'érosion progressive du respect de la vie privée des individus du fait de l'introduction de mesures de sécurité nationale de plus en plus strictes.

Il y a quelques années, une proposition visant à équiper chaque ordinateur personnel d'un processeur qui lui donnerait une identité unique (la puce "Clipper"), mais qui aurait aussi pu, par pure coïncidence (ou peut-être pas), servir à assurer une surveillance déguisée par l'Etat, a suscité un véritable tollé du grand public. A l'époque, la bataille de la puce Clipper a été remportée par les libertaires, mais aujourd'hui la balance penche de nouveau du côté du renforcement de la sécurité nationale.

Suite aux attentats du 11 septembre, la Loi américaine "Patriot Act" et des législations comparables dans d'autres pays ont introduit un cadre pour un contrôle plus strict des communications électroniques, y compris une clause prévoyant l'interception légitime. Le concept d'interception légitime pour appuyer la collecte de preuves est aussi inclus dans la Convention de 2001 sur la cybercriminalité du Conseil de l'Europe (Articles 20 et 21).

Des outils de surveillance plus puissants verront le jour au fil des progrès technologiques et ils pourraient venir encore renforcer le rôle de l'Etat tout en réduisant davantage le respect de la vie privée des particuliers.

Respect de la vie privée: entre les particuliers et les sociétés

Dans ce triangle du respect de la vie privée, la deuxième relation, qui revêt une importance croissante, est celle qui existe entre un particulier et le monde des affaires. Dans une économie informatisée, l'information sur les consommateurs, y compris leurs préférences et leurs profils d'achat, devient un produit de marché très prisé. La vente de données concernant les clients est devenue un commerce très rémunérateur sur l'Internet.

Il existe une autre sorte de "surveillance" entre les particuliers et le monde des affaires, en particulier, dans le cas du commerce électronique.

Ici, des millions d'individus révèlent, en toute connaissance de cause, un volume considérable d'informations à des organisations commerciales: numéros de carte de crédit, adresse et autres renseignements lesquels, s'ils sont utilisés à mauvais escient, peuvent déboucher sur de graves conséquences, telles que la fraude ou le vol d'identité.

Le succès et la pérennité du commerce électronique, aussi bien entre les sociétés et leurs clients qu'entre plusieurs sociétés, dépendent de l'instauration d'un climat de confiance totale envers les politiques de respect de la vie privée appliquées par les sociétés et envers les mesures de sécurité mises en place par les entreprises pour protéger les renseignements confidentiels de leurs clients contre le vol ou contre une utilisation abusive.

Les organisations commerciales exploitent aussi les technologies d'entreposage de données pour acquérir un meilleur contrôle des habitudes et des préférences de leurs clients. Les supermarchés utilisent des cartes de fidélité pour dépister les habitudes d'achats de leurs clients, quel jour de la semaine et à quelle heure de la journée ils préfèrent faire leurs achats, combien ils dépensent, quels produits ils achètent (puisque l'entrepôt de données est aussi relié au matériel de caisse).

Les résultats de ces analyses sont ensuite utilisés pour monter des initiatives de marketing personnalisées ciblées au niveau des foyers individuels. En l'absence de législation sur la protection des données, les informations concernant les particuliers recueillies par les entreprises peuvent être vendues et utilisées dans d'autres contextes.

Respect de la vie privée: entre l'Etat et les sociétés

Ce troisième côté du triangle est celui qui fait le moins de bruit mais c'est peut-être le plus pertinent. Les deux camps, aussi bien l'Etat que le monde des affaires, collectent des volumes considérables de données concernant les particuliers. Il a été signalé que certaines de ces données étaient échangées dans le contexte des mesures anti-terroristes. Toutefois, dans certaines situations, par exemple dans le cas de la Directive européenne sur la protection des données, l'Etat supervise et protège des données sur des particuliers détenues par des sociétés commerciales.

Respect de la vie privée: entre particuliers

Le dernier aspect du respect de la vie privée, qui n'est pas représenté dans le symbolisme du triangle, concerne le risque potentiel pour la vie privée émanant des particuliers eux-mêmes. De nos jours, la technologie met entre les mains des particuliers de puissants outils de surveillance. Même un simple téléphone portable doté d'un appareil photo peut devenir un outil de surveillance. De nos jours, on peut se procurer des appareils photos et des microphones miniatures ultra sophistiqués à un prix raisonnable. Pour reprendre les propos parus dans The Economist, la technologie a "démocratisé la surveillance". De nombreux exemples d'intrusions dans la vie privée ont été documentés, qu'il s'agisse simplement d'actes de voyeurisme ou de l'utilisation plus élaborée d'appareils photos pour enregistrer les codes secrets des cartes bancaires ou encore à des fins d'espionnage électronique.

Le principal problème tient au fait que l'essentiel de la législation est axé sur les risques posés au respect de la vie privée qui découlent de l'Etat. Confrontés à cette nouvelle réalité, quelques gouvernements ont pris des mesures initiales. Le Congrès américain a adopté une Loi pour la prévention du voyeurisme par vidéo, la "Video Voyeurism Prevention Act", qui empêche la prise de photos de personnes dévêtues sans leur accord. Des lois analogues pour le respect de la vie privée, qui empêchent la surveillance de particuliers, ont aussi été adoptées en Allemagne et dans quelques autres pays.

La réglementation internationale en matière de respect de la vie privée et de protection des données

Le principal document international concernant le respect de la vie privée et la protection des données est celui publié par l'OCDE en 1980

et intitulé "Lignes directrices sur la protection de la vie privée et les flux transfrontières de données de caractère personnel". Ces lignes directrices et les travaux ultérieurs de l'OCDE ont inspiré bon nombre de règlements internationaux et régionaux dans ce domaine. Les principes proposés dans les lignes directrices de l'OCDE ont été largement acceptés. Les principales différences résident dans la mise en œuvre de ces principes.

Une approche, adoptée aux Etats-Unis, est fondée sur l'autorégulation. Des politiques en matière de respect de la vie privée sont définies par les sociétés commerciales. Il appartient aux entreprises et aux particuliers de décider de ces politiques. La principale critique soulevée à l'encontre de cette approche tient au fait qu'elle place les particuliers dans une position relativement plus vulnérable.

D'après la seconde approche, favorisée par l'Union européenne, la protection de la vie privée devrait être assurée par les pouvoirs publics. Cette approche du respect de la vie privée, promue dans la Directive européenne de 1995 sur la protection des données (95/46/CE), couvre la protection des particuliers vis-à-vis du traitement des données à caractère personnel et la libre circulation de ces données. Outre la Directive européenne, qui constitue le principal mécanisme, l'approche européenne en matière de respect de la vie privée et de protection des données est également façonnée par d'autres instruments régionaux, tels que la Convention du Conseil de l'Europe sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (1981).

Ces deux approches - Etats-Unis et Union européenne - en matière de respect de la vie privée commencent à présenter un caractère contradictoire. Le principal problème découle de l'utilisation des données à caractère personnel par les sociétés commerciales. Comment l'UE peut-elle imposer sa réglementation à, disons, un éditeur de logiciel basé aux Etats-Unis? Comment l'UE peut-elle veiller à ce que les données sur ses citoyens soient protégées en fonction des règles spécifiées dans sa Directive sur la protection des données? D'après quelles règles (celles de l'UE ou celles des Etats-Unis?) les données transférées du réseau d'une société européenne vers une société américaine sont-elles manipulées? L'UE a menacé de bloquer le transfert de données vers les pays qui se montreraient incapables de garantir le même niveau de protection de la vie privée que celui énoncé dans sa directive. Immanquablement, cette requête a débouché sur un conflit avec l'approche d'autorégulation prônée par les Etats-Unis en matière de protection de la vie privée.

Cette profonde divergence a rendu tout accord éventuel plus difficile à atteindre. De toute façon, il aurait été impossible d'ajuster la législation américaine pour l'aligner sur la Directive de l'UE car cela aurait nécessité de modifier des principes fondamentaux du système juridique américain. L'impasse a finalement pu être débloquée lorsque l'ambassadeur Aaron des Etats-Unis a proposé une formule dite "refuge" ("Safe Harbour"). Cette approche recentrait tout le problème et offrait un moyen de sortir de l'impasse dans laquelle se trouvaient les négociations.

Il a été possible de trouver une solution aux termes de laquelle la réglementation de l'UE pouvait s'appliquer aux sociétés américaines dans les limites d'un "refuge" juridique. Les sociétés américaines qui manipulent des données sur les citoyens européens peuvent choisir de signer un engagement à respecter les dispositions de l'UE en matière de protection de la vie privée. Une fois qu'elles ont signé, les sociétés doivent observer les mécanismes officiels d'exécution convenus entre l'UE et les Etats-Unis.

Les avis contradictoires en matière de protection des données électroniques à caractère personnel entre l'UE et les Etats-Unis ont confirmé que l'interdépendance croissante créée par le commerce électronique peut remettre en question certains principes fondamentaux ancrés dans leur passé culturel et social respectif. Du fait de la mondialisation, il ne fait aucun doute que ce problème se présentera de nouveau au fil de la participation d'autres sociétés. "L'accord refuge" devrait être perçu comme un précédent utile et un outil précieux pour formuler des accords semblables entre l'UE et d'autres pays, y compris le Canada et l'Australie.

SECTION 4

La corbeille économique

LA CORBEILLE ECONOMIQUE

L'importance de l'aspect économique de la gouvernance de l'Internet est illustrée par le titre du document qui a amorcé la réforme de la gouvernance de l'Internet et qui est à l'origine de l'ICANN: "Programme-Cadre pour un commerce électronique mondial" (1997). Le Cadre stipule que "le secteur privé devra piloter" le processus de gouvernance de l'Internet et que la principale fonction de cette gouvernance sera de "faire appliquer un environnement juridique prévisible, minimaliste, cohérent et simple pour le commerce électronique". Ces principes sont le fondement même du régime de l'Internet fondé sur l'ICANN.

Différents mécanismes politiques et réglementaires très pertinents pour le commerce électronique sont classés dans d'autres corbeilles.

LA CORBEILLE INFRASTRUCTURE ET NORMALISATION :

- L'introduction de l'accès à haut *débit* et du concept de *qualité* de service est une condition préalable à la croissance accélérée du commerce électronique dans le domaine du multimédia (par ex. la distribution de films et de chansons).
- La *sécurité de l'Internet* doit consolider la fiabilité et la robustesse de l'environnement propice au commerce électronique. Elle doit aussi permettre de renforcer la confiance des consommateurs envers le commerce électronique.
- Le *cryptage* est un élément crucial pour la protection des communications, notamment en ce qui concerne les transactions financières

LA CORBEILLE JURIDIQUE

- La *juridiction* est importante pour la fiabilité juridique du commerce électronique, notamment en ce qui concerne la protection des consommateurs.
- L'importance des *droits de propriété intellectuelle* pour le commerce électronique est liée au volume croissant de transactions en ligne portant sur des produits incorporels.
- La *signature numérique* facilite les transactions en ligne et résout le problème de l'authentification.

- Davantage d'informations concernant les individus étant recueillies dans le cadre des transactions en ligne, la *protection des données* assure une protection indispensable du respect de la vie privée des particuliers.

COMMERCE ELECTRONIQUE

Le choix d'une définition du commerce électronique comporte d'innombrables implications tant pratiques que juridiques. Suivant la classification dont relève une transaction en ligne donnée, des règles précises s'appliquent, par exemple celles qui réglementent la fiscalité ou les douanes.

Pour le gouvernement des Etats-Unis, l'élément crucial qui permet de faire la distinction entre commerce classique et commerce électronique est "l'engagement en ligne de vendre des biens ou des services". Cela signifie que toute affaire commerciale conclue en ligne devrait être considérée comme une transaction électronique, même si la réalisation du marché nécessite une livraison physique. Ainsi par exemple, l'achat d'un livre par le biais du site Amazon.com est considéré comme une transaction de commerce électronique bien que l'ouvrage soit en principe livré par le biais des services postaux. L'OMC définit le commerce électronique de façon plus précise comme "la production, la distribution, la commercialisation, la vente ou la livraison de biens et de services par un moyen électronique".

Le commerce électronique peut prendre de nombreuses formes:

- de l'entreprise au consommateur (acronyme anglais B2C) - le type de commerce électronique le plus répandu (par ex. Amazon.com);
- de l'entreprise à l'entreprise (B2B) - le plus intensif d'un point de vue économique. En 2001, le volume de transactions B2B aux Etats-Unis portait sur une valeur de US$995 milliards, ce qui représentait 93,3 % de toutes les transactions en ligne;
- de l'entreprise à l'Etat (B2G) - secteur extrêmement important dans le domaine des marchés publics;
- du consommateur au consommateur (C2C) - par exemple, les ventes aux enchères sur e-Bay

Bon nombre de pays ont élaboré un cadre réglementaire pour le commerce électronique. Des lois ont été adoptées dans le domaine des signatures numériques, du règlement des différends, de la cybercriminalité, de la protection des clients et de la fiscalité. Au niveau international, un nombre croissant d'initiatives et de régimes ont trait au commerce électronique.

L'OMC ET LE COMMERCE ELECTRONIQUE

L'acteur politique prépondérant dans le secteur des échanges mondiaux modernes est l'Organisation mondiale du commerce (OMC); elle réglemente bon nombre de questions ayant trait au commerce électronique, y compris la libéralisation des télécommunications, les droits de propriété intellectuelle et certains aspects des progrès en matière de TIC. L'OMC traite directement du commerce électronique par le biais des initiatives suivantes:

- Un moratoire temporaire sur les droits de douane imposés sur les transactions en ligne qui a été introduit en 1998. Il a rendu toutes les transactions électroniques exemptes de droits de douane à l'échelle mondiale.
- L a création du Programme de travail de l'OMC pour le commerce électronique, qui promeut le débat sur le commerce en ligne

Bien que le commerce électronique ait été au second plan de l'ordre du jour diplomatique de l'OMC, diverses initiatives ont vu le jour et un certain nombre d'enjeux primordiaux ont été identifiés. Deux questions sont traitées ici.

Les transactions électroniques devraient-elles être considérées comme des services (et donc être réglementées par l'AGCS) ou comme des marchandises (et être réglementées par le GATT)?

Le classement de la musique comme marchandise ou comme service change-t-il selon que la musique est fournie sur un cédérom (bien corporel) ou par le biais de l'Internet (bien incorporel)? Finalement, la même chanson pourrait avoir un statut commercial différent (et faire l'objet de différentes réglementations douanières et fiscales) en fonction de la méthode de livraison. Comme on peut le voir, le problème de la catégorisation présente des implications considérables du fait des mécanismes réglementaires différents qui s'appliquent aux marchandises et aux services.

Quel devrait être le lien entre les ADPIC et la protection des DPI sur l'Internet?

Sachant que les ADPIC confèrent des mécanismes d'application beaucoup plus stricts pour les DPI, les pays industrialisés ont tenté d'élargir la portée des ADPIC au commerce électronique et à l'Internet au moyen de deux approches. Tout d'abord, en invoquant le principe de la "neutralité technologique", ils soutiennent que les ADPIC, tout comme d'autres règles de l'OMC, devraient englober tous les supports de télécommunications, y compris l'Internet. Deuxièmement, certains pays industrialisés ont demandé une intégration plus étroite des "traités numériques" de l'OMPI dans le régime des ADPIC. Les ADPIC confèrent des mécanismes d'application plus stricts que les conventions de l'OMPI. Ces deux questions restent en suspens et elles vont prendre de l'importance dans les négociations futures de l'OMC.

Au cours de l'étape actuelle des négociations commerciales, il est peu probable que le commerce électronique soulève beaucoup d'attention au sein de l'ordre du jour de l'OMC. Le manque de dispositifs mondiaux en matière de commerce électronique sera en partie couvert par des initiatives particulières (concernant, par exemple, les contrats et les signatures) et par différents accords régionaux, principalement au sein de l'UE et dans le bassin de l'Asie Pacifique.

AUTRES INITIATIVES INTERNATIONALES EN MATIERE DE COMMERCE ELECTRONIQUE

L'une des initiatives les plus réussies et les mieux reçues à l'échelle internationale dans le domaine du commerce électronique est la Loi type de la CNUDCI sur le commerce électronique. La loi type met l'accent sur les mécanismes pour l'incorporation du commerce électronique dans le droit commercial traditionnel (par ex. reconnaître la validité des documents électroniques). La Loi type a été utilisée comme point de départ de la réglementation du commerce électronique dans de nombreux pays.

Une autre initiative conçue pour développer le commerce en ligne est l'introduction d'ebXML (Electronic Business XML) par le Centre des Nations Unies pour la facilitation des échanges et le commerce électronique (UN/CEFAT). De fait, le standard ebXML pourrait bientôt devenir la principale norme pour l'échange de documents commerciaux par voie électronique, remplaçant ainsi la norme EDI actuelle (Electronic Data Interchange - Echange de données informatisées).

Les travaux de l'OCDE abordent divers aspects ayant trait au commerce électronique, y compris la protection des consommateurs et les signatures numériques. L'OCDE met l'accent sur la promotion et la recherche en matière de commerce électronique par le biais de ses recommandations et de ses lignes directrices. D'autres organisations internationales, comme la Conférence des Nations Unies sur le Commerce et le Développement (CNUCED) et le Groupe de travail de l'ONU sur les TIC mènent aussi différents travaux de recherche et de renforcement des capacités dans le domaine du commerce électronique.

Dans le monde des affaires, les organisations internationales les plus dynamiques sont la Chambre de commerce internationale, qui publie tout un éventail de recommandations et d'analyses à propos du commerce électronique et le Dialogue mondial des entreprises, qui promeut le commerce électronique dans un contexte tant international que national.

INITIATIVES REGIONALES

L'UE a élaboré une stratégie de commerce électronique lors du prétendu "Sommet des Dot Com" des chefs de l'UE à Lisbonne (en mars 2000). Bien qu'elle ait adopté une approche privée et centrée sur le marché en matière de commerce électronique, l'UE a aussi introduit quelques mesures de correction pour tenter de protéger les intérêts publics et sociaux (la promotion de l'accès universel, une politique de concurrence qui tient compte de l'intérêt public et des restrictions dans la distribution de contenu nuisible). L'UE a adopté la "Directive sur le commerce électronique" ainsi qu'une série d'autres directives ayant trait aux signatures électroniques, à la protection des données et aux transactions financières électroniques.

Dans la région Asie Pacifique, le point focal de la coopération sur le commerce électronique est la Coopération économique Asie Pacifique (APEC). L'APEC a créé le Groupe directeur sur le commerce électronique qui se penche sur diverses questions ayant trait au commerce électronique, notamment la protection des consommateurs, la protection des données, le pollupostage et la sécurité du cyberespace. L'initiative la plus récente et la plus en vue de l'APEC est son Plan d'action individuel pour des échanges sans papier, qui entend instituer des échanges de marchandises sans papier dans la région Asie-Pacifique d'ici 2010.

PROTECTION DES CONSOMMATEURS

La confiance des consommateurs est l'une des principales conditions préalables au succès du commerce électronique. Le commerce électronique est encore relativement nouveau et les consommateurs ne lui font pas autant confiance qu'aux achats qu'ils peuvent réaliser dans le monde "réel". La protection des consommateurs est une méthode légale importante pour renforcer la confiance envers le commerce électronique.

La réglementation du commerce électronique devrait protéger les consommateurs dans un certain nombre de domaines: la manipulation en ligne des informations sur les cartes de paiement, la publicité mensongère et la fourniture de produits défectueux. Une autre particularité du commerce électronique réside dans l'internationalisation de la protection des consommateurs, problème qui ne revêt guère d'importance dans le commerce classique. Dans le passé, les consommateurs avaient rarement besoin d'invoquer un mécanisme international de protection. Avec le commerce électronique, un nombre croissant de transactions interviennent par-delà les frontières nationales.

La juridiction est une question importante qui gravite autour de la protection des consommateurs. La juridiction implique deux approches principales. La première avantage le vendeur (le plus souvent une compagnie d'affaires électroniques) et il s'agit d'une approche fondée sur le pays d'origine/prescrite par le vendeur. Dans ce scénario, les sociétés de commerce électronique ont l'avantage de se reposer sur un environnement juridique connu et prévisible. L'autre approche, qui favorise le client, est une approche fondée sur le 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 de ce dilemme serait une harmonisation plus systématique des règles de protection des consommateurs, ce qui rendrait la question de la juridiction moins pertinente.

Tout comme pour d'autres enjeux du commerce électronique, l'OCDE a pris la tête du processus en adoptant les Lignes directrices pour la protection du consommateur dans le contexte du commerce électronique (2000) et les Lignes directrices pour la protection des consommateurs

contre les pratiques commerciales frauduleuses et trompeuses au-delà des frontières (2003). L'OCDE a établi les principes majeurs, désormais adoptés par quelques associations commerciales, y compris la Chambre de commerce internationale et le Council of Better Business Bureaus (Conseil des bureaux d'éthique commerciale).

L'UE offre un degré élevé de protection des consommateurs dans le contexte du commerce électronique. Ainsi par exemple, le problème de la juridiction a été résolu par le biais de la Convention de Bruxelles, qui stipule que les consommateurs auront toujours droit de recours auprès de la protection juridique locale.

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

Le développement à venir du commerce électronique exigera soit l'harmonisation des législations nationales soit l'élaboration d'un nouveau régime international pour la protection des consommateurs dans le contexte du commerce électronique.

FISCALITE

Le dilemme de la gouvernance de l'Internet quant à savoir si les questions liées au cyberespace devraient être traitées différemment des questions du monde réel est clairement illustré dans le domaine de la fiscalité. Dès les premiers balbutiements de l'Internet, les Etats-Unis ont tenté de faire de l'Internet une zone en franchise. En 1998, le Congrès américain a adopté la Loi sur la liberté fiscale. L'OCDE et l'UE quant à elles appuient l'opinion contraire, à savoir que l'Internet ne devrait pas bénéficier d'un traitement fiscal privilégié. Les Principes d'Ottawa de l'OCDE stipulent qu'il n'existe aucune différence entre la fiscalité classique et la fiscalité électronique qui soit susceptible de nécessiter une réglementation particulière. De nombreux états des Etats-Unis ont plaidé dans ce sens, demandant que les transactions sur l'Internet soient assujetties à l'impôt.

Une autre question liée à la fiscalité du commerce électronique qui reste en suspens entre l'UE et les Etats-Unis est la définition du lieu d'imposition. Les Principes d'Ottawa introduisaient la notion de "destination" au lieu du principe "d'origine" de la fiscalité. Le gouvernement des Etats-Unis a fortement intérêt à ce que l'imposition reste au point d'origine des transactions, puisque la plupart des transactions en ligne sont basées aux Etats-Unis. En revanche, l'intérêt de l'UE en faveur d'une "imposition au point de destination" est largement guidé par le fait que l'UE compte davantage de consommateurs que de vendeurs ayant recours au commerce électronique.

DOUANES

Les services douaniers sont directement touchés par le commerce électronique. La transaction de marchandises numériques par-delà les frontières internationales ne peut pas être contrôlée de la même façon que la transaction de biens matériels. Il est difficile, pour ne pas dire impossible, d'identifier les colis Internet renfermant des produits sur lesquels des droits de douane devraient être acquittés. Ceci soulève de multiples questions ayant trait à l'applicabilité du concept existant de contrôles douaniers ainsi que l'introduction d'un certain nombre de procédures nouvelles.

Au niveau politique, la principale initiative est le moratoire de l'OMC sur l'imposition de droits de douane sur les transmissions de biens et services par voie électronique (1998). La dernière prolongation explicite du moratoire a eu lieu à Doha en 2001. En raison de l'échec des négociations de l'OMC à Cancun (2003), cette question n'a pas été officiellement abordée. Elle laissait la place à différentes interprétations quant à la question de savoir si un moratoire douanier mondial était ou non toujours en vigueur. D'un point de vue pratique, cela ne fait guère de différence, puisqu'il est quasiment impossible d'imposer un droit de douane sur des biens et services livrés par l'Internet en raison des difficultés techniques que poserait leur inspection.

LA MONETIQUE: MONNAIE ET TRANSACTIONS BANCAIRES ELECTRONIQUES

La monétique peut se définir comme la conclusion d'une transaction financière au sein d'un environnement en ligne par le biais de divers instruments de paiement en ligne. L'existence d'un système électronique de paiement est une condition préalable au développement réussi du commerce électronique. Le domaine des paiements électroniques nécessite de faire une distinction entre les transactions bancaires en ligne et l'argent électronique.

Le concept de banque virtuelle implique l'utilisation d'un ordinateur individuel et de l'Internet pour effectuer des opérations bancaires classiques telles que des paiements par carte ou des transferts de fonds. L'originalité réside uniquement dans le support de la transaction alors que le service bancaire reste essentiellement le même. La banque virtuelle offre des avantages à ses clients et réduit les coûts de transaction. En termes de gouvernance, elle ne pose pas de problèmes spécifiques, hormis ceux que nous avons déjà évoqués plus haut, tels que la protection des clients au niveau international.

En revanche, la notion "d'argent électronique" introduit une innovation majeure. Le Bureau américain de la Réserve Fédérale définit la monnaie électronique comme "de l'argent qui circule par voie électronique". L'argent électronique est généralement associé à ce qu'on appelle des "cartes intelligentes" émises par des sociétés comme Mondex, Visa Cash, et CyberCash. L'argent électronique présente toujours les caractéristiques suivantes:

- Il est stocké électroniquement, le plus souvent sur une carte à puce.
- Il est transféré électroniquement. Dans la plupart des cas, cela se produit entre consommateurs et commerçants. Parfois, il est possible de réaliser des transferts entre particuliers.
- Les transactions d'argent électronique mettent en œuvre un système complexe, faisant intervenir l'émetteur de la valeur de l'argent électronique, les opérateurs de réseau et le compensateur des transactions d'argent électronique.

A ce jour, l'argent électronique en est encore à un stade embryonnaire. Son utilisation n'est pas très répandue en raison d'une sécurité limitée et d'un manque de confidentialité. L'argent électronique pourrait évoluer dans deux sens:

D'une part, il pourrait connaître un développement évolutif qui engloberait des méthodes de transactions électroniques plus sophistiquées, y compris la mise au point de méthodes performantes de micro-paiement. A terme, toutes ces transactions seraient ancrées dans le système bancaire et monétaire existant.

D'autre part, on pourrait assister à un développement révolutionnaire qui porterait l'argent électronique hors du contrôle des banques centrales. La Banque des Règlements Internationaux (BRI) a d'ores et déjà identifié un contrôle moindre sur les flux financiers et la masse monétaire comme faisant partie des risques associés à l'argent électronique. D'un point de vue conceptuel, l'émission d'argent électronique serait comparable à l'impression de billets sans la sanction d'un organisme bancaire central. Une telle approche permettrait aux institutions privées d'émettre des fonds essentiellement destinés au commerce électronique. Comme l'observe un éminent banquier : "Les successeurs de Bill Gates auraient mis les successeurs d'Alan Greenspan en faillite". Un tel développement aurait des implications considérables pour l'avenir des relations gouvernementales et internationales; de fait, comme le constate le même banquier: "Les sociétés se sont débrouillées sans banque centrale dans le passé. Elles pourraient bien faire de même à l'avenir". A ce stade, d'autres possibilités concernant l'utilisation d'argent électronique revêtent encore un caractère spéculatif.

LES ENJEUX

1. L'usage plus répandu de services bancaires virtuels et d'argent électronique pourrait entraîner une transformation du système bancaire mondial, en offrant aux clients des options supplémentaires tout en réduisant les frais bancaires. Les banques physiques seront sérieusement remises en question par les banques virtuelles plus rentables.
2. Une enquête sur le commerce électronique donne le manque de méthodes de paiement (par ex. cartes) comme la troisième raison, derrière la sécurité et la confidentialité, pour ne pas avoir recours au commerce électronique. Actuellement, il est quasiment impossible

de réaliser des transactions en ligne sans carte de crédit. C'est là un obstacle majeur pour les pays en développement qui ne disposent pas d'un marché développé de cartes de crédit. Les gouvernements de ces pays devront promulguer les changements juridiques requis pour permettre une introduction plus rapide des paiements par carte.

3. Afin de dynamiser le développement du commerce électronique, les gouvernements du monde entier auront besoin d'encourager toutes les formes de règlements sans espèces, y compris les cartes de crédit et l'argent électronique. L'introduction accélérée de l'argent électronique nécessitera des mesures réglementaires supplémentaires par les pouvoirs publics. Après Hong Kong, le premier à avoir introduit une législation exhaustive régissant le domaine de la monnaie électronique, l'UE a adopté la Directive relative à l'argent électronique en 2000.

   Les gouvernements rechignent à introduire la monnaie électronique en raison des risques potentiels qu'elle présente pour l'autorité des banques centrales. A ce titre, certains donnent de sérieux avertissements, comme l'économiste David Saxton: "L'argent numérique est une menace pour tous les gouvernements de cette planète désireux de gérer leur propre monnaie". Les gouvernements craignent également de voir l'argent électronique servir au blanchiment de fonds.

4. Certains analystes estiment que le véritable essor du commerce électronique est lié à l'introduction de services performants et fiables pour les petites transactions. Ainsi par exemple, les internautes hésitent encore à utiliser leur carte de crédit pour régler de petits montants (de quelques euros ou de quelques dollars), qui sont généralement majorés d'un montant supplémentaire pour accéder à des articles ou autres services sur l'Internet. Un système de micro-paiement basé sur la monnaie électronique pourrait offrir la solution nécessaire. W3C, le principal organisme de normalisation de l'Internet, travaille à la création de normes pour différents systèmes de micro-paiement.

5. Du fait de la nature de l'Internet, il est probable que la monnaie électronique deviendra mondiale - donnant ainsi un excellent prétexte pour aborder cette question à l'échelon international. Un acteur potentiel dans le domaine des services bancaires virtuels est le Groupe des services bancaires virtuels du Comité de Bâle. Ce groupe a déjà commencé à se pencher sur la question de l'autorisation, les normes

de prudence, la transparence, la confidentialité, le blanchiment de fonds et la surveillance transfrontière, qui sont autant de questions cruciales pour l'introduction de la monnaie électronique.

6. Différentes formes de paiements électroniques ont été mises au point, principalement au sein des économies avancées. Les versements électroniques exigent un environnement juridique stable, sûr et fonctionnel. Toutefois, la plupart des pays en développement sont encore des économies à base d'argent comptant. Si l'usage de cartes devient autorisé, il est tributaire de l'usage de signatures. Cet écart immense affecte aussi le développement du commerce électronique et creuse encore la fracture numérique entre les riches du Nord et les pauvres du Sud. A la différence de mesures comme l'achat de matériel, l'introduction de modes de paiement électronique exige l'introduction progressive de nombreux dispositifs techniques et institutionnels. Un élément indispensable tant pour le commerce électronique que pour les paiements en ligne qui ne peut pas s'acquérir du jour au lendemain est la confiance des consommateurs.

7. La toute nouvelle requête du Procureur général de l'Etat de New York enjoignant Paypal et Citibank de ne pas effectuer de paiements aux casinos virtuels associe directement le règlement électronique et l'application de la loi. Ce que les pouvoirs publics chargés de l'application de la loi n'ont pas pu obtenir par le biais de mécanismes juridiques, ils pourraient bien l'obtenir par le biais du contrôle des versements électroniques.

SECTION 5

La corbeille développement

LA CORBEILLE DEVELOPPEMENT

La technologie n'est jamais neutre. L'histoire de la société humaine nous donne maints exemples de technologie qui autonomise certains individus, certains groupes ou certaines nations, tout en en marginalisant d'autres. L'Internet n'est pas différent à cet égard. Du particulier à l'échelle mondiale, un profond changement est intervenu dans la répartition de la richesse et du pouvoir. L'impact des TIC sur la distribution du pouvoir et sur le développement a soulevé de nombreuses questions:

- Comment les changements accélérés par les TIC affectent-ils la fracture déjà grande entre le Nord et le Sud? Les TIC vont-elles réduire ou creuser le fossé existant?
- Quand et comment les nations en développement seront-elles capables d'atteindre le niveau de TIC des pays plus industrialisés?

La réponse à ces questions et à d'autres exige une analyse de la pertinence du développement dans le contexte de la gouvernance de l'Internet. Presque toutes les questions ayant trait à la gouvernance de l'Internet ont une dimension qui touche le développement. Ainsi par exemple:

- l'existence d'une infrastructure des télécommunications, première condition requise pour surmonter la fracture numérique;
- le modèle économique actuel pour l'accès à l'Internet, qui impose un fardeau disproportionné sur les pays en développement, lesquels doivent financer l'accès aux dorsales situées dans les pays développés;
- le pollupostage, qui a des conséquences comparativement plus graves pour les pays en développement en raison de leur bande passante limitée et de leur manque de capacités à y remédier;
- la réglementation mondiale des DPI, qui affecte directement le développement, du fait des opportunités réduites des pays en développement en termes d'accès au savoir et aux informations en ligne

L'aspect développemental du Sommet mondial de la société de l'information (SMSI) a été souligné à maintes reprises, à commencer par la résolution de l'Assemblée générale des Nations Unies sur le SMSI, qui souligne que le SMSI devrait assurer "la promotion du développement, en particulier pour ce qui touche l'accès à la technologie et son transfert".

La Déclaration de Genève du SMSI et son Plan d'Action ont mis en exergue le développement comme priorité et l'ont lié à la résolution sur le millénaire et à sa promotion de "l'accès de tous les pays [.] aux techniques de l'information, de la transmission des connaissances et de la communication, aux fins du développement".

Le lien avec les objectifs du Millénaire pour le développement étant établi, le SMSI est fort bien placé dans le contexte du développement.

Ce chapitre se concentrera exclusivement sur les enjeux primordiaux du développement, tels que la fracture numérique et l'accès universel, enjeux fréquemment soulevés dans le débat sur le développement. Il sera suivi d'une analyse des principaux facteurs qui influencent l'Internet et le développement: infrastructure, appui financier, enjeux politiques et aspects socioculturels.

Comment les TIC affectent-elles le développement de la société?

The main dilemmas about ICT and development were summarised in a recent article in *The Economist* ("Falling through the Net?", 21 September 2000). The article proposes pro and con arguments for the thesis that ICT provides specific impetus for development.

Les TIC NE facilitent PAS le développement	Les TIC facilitent le développement
• Les "externalités de réseau" aident les premiers arrivés à établir une position de force. Ceci favorise les géants américains de sorte que les entreprises locales des économies émergentes se trouveraient en fait figées en dehors du commerce électronique. • Le recentrage du pouvoir du vendeur vers l'acheteur (avec l'Internet, inévitablement "un autre fournisseur n'est jamais plus loin qu'un clic de souris") lèsera les pays plus pauvres. Il nuira aux producteurs de marchandises, essentiellement en provenance des pays en développement. • Un intérêt supérieur envers les segments pointus des économies riches réduira l'intérêt des investisseurs potentiels envers les pays en développement.	• Les TIC abaissent les coûts de main-d'œuvre ; il revient moins cher d'investir dans les pays en développement. • On assiste à une diffusion très rapide des TIC au-delà des frontières, ce qui n'était pas le cas avec les technologies antérieures. Les technologies antérieures (voie ferrée et électricité) ont mis des décennies à gagner les pays en développement mais les TIC progressent à pas de géant. • La possibilité de sauter les technologies plus anciennes en brûlant les étapes intermédiaires telles que les fils de cuivre et les téléphones analogiques encourage le développement. • La tendance des TIC à réduire la taille optimale d'une entreprise dans la plupart des industries est beaucoup plus proche des besoins des pays en développement

LA FRACTURE NUMERIQUE

La fracture numérique se définit comme un fossé entre ceux qui, pour des raisons techniques, politiques, sociales ou économiques, disposent de l'accès et des capacités d'utilisation des TIC, et ceux qui n'en disposent pas. Différents points de vue ont été avancés concernant la taille et la pertinence de la fracture numérique.

Il peut exister une fracture numérique à différents niveaux: au sein d'un même pays et entre plusieurs pays, entre des communautés rurales et urbaines, entre les jeunes et les plus vieux, et même entre les hommes et les femmes. Les fractures numériques ne sont pas des phénomènes indépendants. Elles reflètent de profondes inégalités socioéconomiques en termes d'éducation, de soins de santé, de capitaux, de logement, d'emploi, d'eau potable et d'alimentation. Ce point a été clairement énoncé par la DOT Force du G8: "il n'existe pas de dichotomie entre la fracture numérique et les divisions sociales et économiques plus vastes que le processus de développement devrait aborder; la fracture numérique a besoin d'être comprise et résolue dans le contexte de ces divisions plus vastes".

La fracture numérique se creuse-t-elle?

Les progrès des TIC laissent le monde en développement à la traîne à une allure bien plus rapide que les avancées technologiques réalisées dans les autres domaines (par ex. les techniques agricoles ou médicales) et, comme le monde développé dispose des outils nécessaires pour utiliser avec brio ces progrès technologiques, la fracture numérique semble se creuser de façon continuelle et rapide. C'est là l'opinion fréquemment exprimée dans divers documents faisant autorité, tels que le Rapport sur le développement humain du PNUD et les Rapports sur l'emploi dans le monde de l'OIT.

Certains points de vue divergents soutiennent que les statistiques relatives à la fracture numérique sont souvent trompeuses et qu'en réalité la fracture numérique ne se creuse pas du tout. Selon cet avis, l'accent traditionnel mis sur le nombre d'ordinateurs, le nombre de sites Web ou la bande passante disponible devrait céder la place à un accent sur l'impact

plus vaste des TIC sur les sociétés dans les pays en développement. Fréquemment, les exemples cités concernent les réussites numériques de l'Inde et de la Chine.

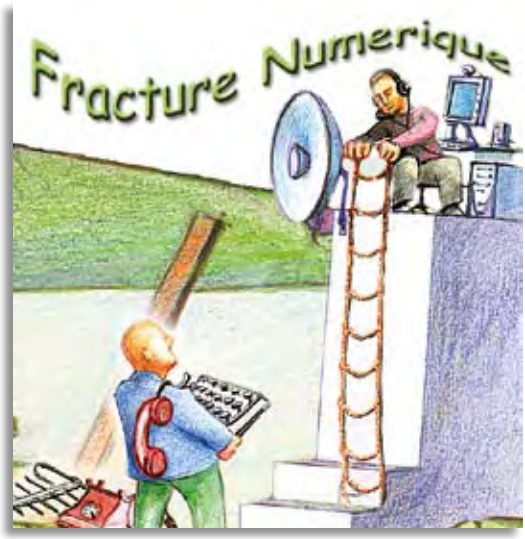
ACCES UNIVERSEL

Outre la fracture numérique, un autre concept dont il est fréquemment fait mention dans le débat sur le développement concerne l'accès universel, c'est-à-dire l'accès pour tous. S'il est vrai qu'il devrait être la pierre angulaire de toute politique de développement des TIC, il subsiste des perceptions et des conceptions divergentes quant à la nature et la portée de cette politique d'accès universel. Une référence fréquente à la notion d'accès universel dans les préambules des déclarations internationales et les résolutions sans mesure politique ou financière à l'appui en font un principe vague n'ayant guère de pertinence pratique. La question de l'accès universel au niveau mondial demeure dans une large mesure une question politique et dépend finalement de la volonté des pays développés à investir dans la réalisation de cet objectif.

A la différence de l'accès universel au niveau mondial, dans certains pays, l'accès universel est un concept économique et juridique fort bien développé. Fournir l'accès aux télécommunications pour tous les citoyens a été le fondement même de la politique des télécommunications adoptée par les Etats-Unis. Il s'ensuit un système très élaboré regroupant différents mécanismes politiques et financiers, dont le but est de subventionner les coûts d'accès dans les zones reculées et les régions ayant des coûts de connexion élevés. La subvention est financée par les régions ayant de faibles coûts de connexion, principalement les grandes villes. L'UE a elle aussi pris un certain nombre de mesures concrètes pour parvenir à un accès universel.

STRATEGIES POUR SURMONTER LA FRACTURE NUMERIQUE

La théorie du développement centré sur la technologie, qui a dominé les sphères politiques et universitaires depuis plus d'un demi-siècle, soutient que le développement est tributaire de la disponibilité des technologies. Plus la technologie est disponible, plus le développement fleurit. Toutefois, cette approche a failli à bon nombre de pays (surtout les anciens pays socialistes) où il est vite devenu évident que le développement de la société est un processus beaucoup plus complexe. La technologie est certes un élément nécessaire mais, à elle seule, elle ne suffit pas à engendrer le développement. Parmi les autres éléments requis, on peut citer un cadre réglementaire, un appui financier, des ressources humaines disponibles et d'autres conditions socioculturelles. Même si tous ces ingrédients sont réunis, le défi majeur reste la question de savoir quand et comment les utiliser, les marier et provoquer des interactions entre eux.



DEVELOPPEMENT DES INFRASTRUCTURES DE TELECOMMUNICATIONS ET DE L'INTERNET

La possibilité d'établir la connectivité est une condition préalable pour amener les particuliers et les institutions à l'Internet et finalement surmonter la fracture numérique. Il existe différentes possibilités pour fournir et renforcer cette connectivité.

L'essor rapide des communications sans fil offre une nouvelle chance à de nombreux pays en développement. Patrick Gelsinger de la société Intel a conseillé aux pays en développement de dire "non" à des infrastructures des télécommunications à base de fils de cuivre pour utiliser le

sans fil comme la solution des boucles locales et les fibres optiques pour les dorsales nationales. Les communications sans fil seront peut-être la solution au problème que pose le développement des infrastructures de communications terrestres (pose de câbles sur de très longues distances dans de nombreux pays d'Asie et d'Afrique). De cette façon, il devient réalisable de surmonter le problème du dernier kilomètre, ou boucle locale, l'un des obstacles majeurs à un développement plus rapide de l'Internet. De par tradition, l'aspect infrastructurel de la fracture numérique a été la préoccupation première de l'Union internationale des télécommunications.

APPUI FINANCIER

Les pays en développement reçoivent un appui financier par le biais de différents circuits, y compris les agences de développement bilatérales ou multilatérales telles que le PNUD ou la Banque mondiale, ainsi que les initiatives et les banques régionales de développement. Avec la libéralisation accrue du marché des télécommunications, on a constaté une vulgarisation du phénomène qui tend à développer les infrastructures des télécommunications à partir de l'investissement direct étranger. Bon nombre de pays en développement luttent continuellement pour attirer des capitaux privés.

A l'heure actuelle, la plupart des compagnies occidentales des télécommunications sont entrées dans une phase de consolidation, après avoir accumulé des dettes massives suite à des surinvestissements dans les années quatre-vingt-dix. Si elles hésitent encore à investir, on s'attend à ce qu'à moyen terme elles investissent dans les pays en développement car le marché des pays industrialisés est désormais sursaturé du fait des montées en puissance massives observées à la fin des années quatre-vingt-dix.

The importance of the financial aspect was clearly recognised during the L'importance de l'aspect financier a été clairement reconnue au cours de la phase de Genève du SMSI. Une suggestion avancée au SMSI concernait l'établissement d'un Fonds de solidarité numérique administré par l'ONU pour aider les pays désavantagés d'un point de vue technologique à construire des infrastructures de télécommunications. Le fonds dépendrait de contributions volontaires. Certains ont proposé la création d'un système de don, par exemple $1 par achat d'un ordinateur individuel, d'un progiciel ou d'un matériel de réseau. Toutefois, cette proposition n'a pas su séduire suffisamment les pays industrialisés, lesquels ont donné

la préférence à l'investissement direct plutôt qu'à la création d'un fonds de développement centralisé. Afin d'explorer d'autres possibilités de régimes de financement plus souples et plus appropriés, il a été convenu de créer un Groupe de travail sur le financement des TIC pour le développement qui rendra compte au SMSI de 2005 en Tunisie.

ASPECTS SOCIOCULTURELS

The socio-cultural aspect of digital divides encompasses a variety of isL'aspect socioculturel des fractures numériques englobe une foule de questions, y compris l'alphabétisation, les compétences en matière de TIC, la formation, l'éducation et la protection des atouts linguistiques.

Pour les pays en développement, l'un des principaux enjeux a été la "fuite des cerveaux" décrite comme le mouvement d'une main-d'œuvre hautement qualifiée des pays en développement vers les pays industrialisés. Du fait de ce phénomène, les pays en développement se montrent perdants sur de nombreux tableaux. La principale perte concerne la main-d'œuvre qualifiée. Les pays en développement perdent aussi l'investissement consacré à la formation et à l'éducation de la main-d'œuvre qualifiée migrante. Il est probable que la fuite de cerveaux se poursuivra, du fait des divers régimes d'emploi et d'immigration qui ont été introduits par les Etats-Unis, l'Allemagne et d'autres pays industrialisés dans le but d'attirer de la main-d'œuvre qualifiée, le plus souvent formée aux technologies de l'information et des télécommunications.

Un phénomène qui pourrait peut-être mettre un terme voire, dans certains cas, renverser la fuite des cerveaux, concerne la vulgarisation de la sous-traitance des tâches TIC aux pays en développement. Les exemples les plus réussis jusqu'ici ont été le développement de centres d'édition de logiciel en Inde, par exemple à Bangalore.

A l'échelle mondiale, les Nations Unies ont créé le Réseau des diasporas numériques afin de promouvoir le développement de l'Afrique, par le biais de la mobilisation du savoir-faire et des ressources technologiques, managériales et professionnelles des diasporas africaines dans le domaine des TIC.

Des initiatives de l'UNESCO s'avèrent particulièrement pertinentes pour l'aspect social de la fracture numérique. L'UNESCO a adopté une Convention sur la protection de la diversité culturelle et elle a lancé un certain nombre de projets destinés à promouvoir la diversité linguistique et culturelle sur l'Internet.

POLITIQUE ET REGLEMENTATION DES TELECOMMUNICATIONS

A bien des égards, les questions liées à la politique des télécommunications sont étroitement liées à l'élimination de la fracture numérique. Tout d'abord, les investisseurs privés d'une part, mais aussi, et de plus en plus souvent, les donateurs publics ne sont pas prêts à investir dans des pays sans bénéficier d'un environnement institutionnel et juridique propice au développement de l'Internet. Deuxièmement, le développement des secteurs nationaux des TIC dépend de la création des cadres réglementaires nécessaires. Troisièmement, l'existence de monopoles nationaux des télécommunications est souvent citée comme l'une des raisons à l'origine du coût plus élevé de l'accès à l'Internet.

La création d'un milieu habilitant est une tâche éprouvante, qui nécessite la démonopolisation progressive du marché des télécommunications, l'introduction de lois régissant l'Internet (couvrant les droits d'auteur, le respect de la vie privée, le commerce électronique, etc.), et l'octroi de l'accès à tous, sans aucune restriction politique, religieuse ou autre.

Le débat concernant l'impact de la libéralisation du marché des télécommunications sur le développement gravite autour de deux points de vue prépondérants. Le premier est que la libéralisation n'a pas profité aux pays en développement. Avec la perte des monopoles de télécommunications, les gouvernements des pays en développement ont perdu une source importante de revenu pour l'élaboration de leur budget. Les budgets plus faibles ont touché tous les autres secteurs de la vie économique et sociale. Selon ce point de vue, les perdants sont les gouvernements des pays en développement et les gagnants sont les compagnies de télécommunications du monde développé. Le second point de vue argue que l'ouverture des marchés des télécommunications a donné lieu à une concurrence accrue, ce qui apporte une qualité de service supérieure et des coûts moindres. A terme, cela débouchera sur un secteur des télécommunications performant et rentable, condition préalable au bon développement général de la société

SECTION 6

La corbeille socioculturelle

LA CORBEILLE SOCIOCULTURELLE

Les réseaux qui relient les ordinateurs existaient bien avant l'Internet. Ce qui fait l'originalité de l'Internet, c'est le fait qu'il facilite différentes formes de communication et de créativité de l'être humain. Les principaux progrès sont associés à la manière dont l'Internet est utilisé pour de nouveaux modes de communication (courrier électronique, Web, multimédia). Dans ce contexte, certains analystes soutiennent que l'Internet est plus un phénomène de société qu'un phénomène technologique. Il s'inscrit en complément des communications traditionnelles et offre de nouvelles formes de communication qui lui sont propres (par ex. les communautés cybernautes). Ces développements ont donné naissance à une dimension socioculturelle de l'Internet. La corbeille socioculturelle englobe certaines des questions les plus controversées de la problématique que constitue la gouvernance de l'Internet, à savoir la politique du contenu et le multilinguisme. Ce sont ces questions, en particulier, qui traduisent les différences nationales, religieuses et culturelles les plus présentes dans le monde d'aujourd'hui.

LA POLITIQUE DU CONTENU

L'une des principales questions socioculturelles concerne la politique du contenu, qui est souvent abordée sous différents points de vue: droits de l'homme (liberté d'expression et droit de communiquer), gouvernement (contrôle du contenu) et technologie (outils pour le contrôle du contenu), pour n'en nommer que quelques-uns.

Le débat sur le contenu se concentre généralement sur trois groupes de contenu. Le premier groupe concerne le contenu pour le contrôle duquel il existe déjà un consensus mondial. On retrouve ici la pornographie juvénile et diverses questions, telles que la justification du génocide et l'incitation ou l'organisation d'actes terroristes, interdites par le droit in-

ternational (ius cogens). S'il existe bien un consensus sur le besoin de retirer ce contenu de l'Internet, il subsiste néanmoins différentes interprétations. Ainsi par exemple, qu'est-ce qui constitue exactement un acte de soutien au terrorisme?

Le *second groupe* concerne le contenu qui est susceptible d'être choquant ou insultant pour des pays, des régions ou des groupes ethniques donnés en raison de leurs valeurs religieuses ou culturelles. Une communication mondialisée et plus intensive remet en cause les valeurs locales culturelles et religieuses. La plupart des procès liés à l'Internet ont trait à cette sorte de contenu. Dans l'affaire Yahoo!, un tribunal français a demandé à Yahoo.com (aux Etats-Unis) d'interdire aux citoyens français d'accéder à certaines parties d'un site Web qui vendait des souvenirs et articles de propagande nazie. L'Allemagne a une jurisprudence très étoffée, de nombreux procès ayant été intentés contre les propriétaires de sites Web hébergeant du matériel à caractère nazi. La majeure partie du contrôle du contenu au Moyen-Orient et dans les pays d'Asie est officiellement justifiée au nom de la protection de valeurs culturelles spécifiques. Cela comprend généralement le blocage de l'accès à des sites pornographiques ou à des sites de jeu d'argent.

Le *troisième groupe* concerne le contenu à caractère politiquement ou idéologiquement sensible. En bref, il s'agit de la censure de l'Internet. Transparency International a signalé un certain nombre de pratiques de ce type en Chine, en Birmanie et en Arabie saoudite.

COMMENT S'EFFECTUE LA POLITIQUE DU CONTENU?

Un menu *à la carte* en matière de politique du contenu renferme les options juridiques et techniques suivantes appliquées sous diverses déclinaisons.

Filtrage public (gouvernemental) du contenu

TL'élément commun d'un filtrage gouvernemental est un "Index Internet" de sites Web dont l'accès est interdit aux citoyens. Si un site Web figure dans "l'Index Internet", les internautes ne pourront pas y accéder. D'un point de vue technique, le filtrage applique généralement un blocage d'adresse IP à partir d'un routeur, des serveurs proxy et la redirection par le DNS. Le filtrage du contenu s'effectue dans de nombreux pays. Outre certains pays communément associés à ce genre de pratiques (Chine, Arabie saoudite et Singapour), d'autres pays le pratiquent de plus

en plus souvent. Ainsi par exemple, l'Australie a mis en place un système de filtrage pour certaines de ses pages nationales. En Allemagne, l'état de la Rhénanie du Nord-Westphalie a demandé aux FAI de filtrer l'accès à des sites principalement, mais pas exclusivement, à caractère néonazi.

Systèmes privés de classement et de filtrage

Confronté au risque potentiel de la désintégration de l'Internet du fait de la mise en place de diverses barrières nationales (systèmes de filtrage), W3C et d'autres institutions sur la même longueur d'onde ont suggéré la mise en œuvre de systèmes de classement et de filtrage contrôlés par les internautes eux-mêmes. D'un point de vue technique, les mécanismes de filtrage sont intégrés dans les navigateurs Internet. L'accessibilité du contenu spécifique est indiquée par un label qui correspond à un site Web donné. L'utilisation de ce type de filtrage a été particulièrement prisée en guise de système permettant de restreindre l'accès aux seuls sites "adaptés aux enfants".

Logiciel de géolocalisation

Une autre solution technique ayant trait au contenu concerne les logiciels de géolocalisation, qui filtrent l'accès au contenu d'un site particulier en fonction de l'origine nationale/la position géographique de l'utilisateur. L'affaire Yahoo! est importante à cet égard car le groupe d'experts impliqués dans l'affaire, y compris Vint Cerf, ont signalé que dans 90 % des cas Yahoo! serait en mesure de déterminer si des sections de l'un de ses sites hébergeant des souvenirs nazis étaient effectivement accédées depuis la France. Cette évaluation technologique a aidé le tribunal à prendre sa décision finale. Les éditeurs de logiciels de géolocalisation prétendent qu'ils peuvent identifier le pays d'origine sans commettre d'erreur et la ville dans environ 85 % des cas, notamment s'il s'agit d'une grande ville. Les logiciels de géolocalisation peuvent aider les fournisseurs de contenu de l'Internet à filtrer l'accès en fonction de l'emplacement géographique de l'internaute et ainsi éviter des procès devant des tribunaux étrangers.

Contrôle du contenu par le biais des moteurs de recherche

Il existe une différence notable entre la disponibilité et l'accessibilité du matériel qui se trouve sur l'Internet. Le fait qu'une page Web ou un contenu donné soit disponible sur l'Internet ne veut pas dire pour autant qu'il ou elle sera consulté(e) par de nombreux internautes. Ainsi par ex-

emple, si un site Web donné ne peut pas être trouvé sur Google, sa pertinence s'en trouve grandement réduite. La passerelle entre l'internaute et le contenu du Web est le plus souvent un moteur de recherche. Il a été largement médiatisé que l'un des premiers exemples de contrôle de contenu par le biais des moteurs de recherche avait été effectué par les autorités chinoises par le biais du moteur de recherche Google. Si des internautes tapaient un mot interdit dans la fonction de recherche de Google, ils perdaient leur connectivité à l'Internet pendant quelques minutes. Le service informatique des autorités chinoises a déclaré: "Avec certains sites Internet, il est tout à fait normal qu'à certains moments vous puissiez y accéder et que vous ne le puissiez pas à d'autres. Le ministère n'a reçu aucune information à propos d'un éventuel blocage de Google."

Pour s'aligner sur la législation locale, Google a décidé de restreindre le matériel figurant sur ses sites Web nationaux. Ainsi par exemple, sur les versions française et allemande de Google, il n'est pas possible de chercher et donc de trouver des sites Web contenant du matériel à caractère nazi. Cela révèle un certain niveau d'autocensure de la part de Google afin d'éviter d'éventuels procès.

Nécessité d'un cadre juridique approprié

Le vide juridique dans le domaine de la politique du contenu, qui caractérisait l'utilisation initiale de l'Internet, a permis aux gouvernements de bénéficier de pouvoirs discrétionnaires élevés en matière de contrôle du contenu. Sachant que la politique du contenu est une question très sensible dans toute les sociétés, il devient nécessaire d'adopter des instruments juridiques. La réglementation nationale dans le domaine de la politique du contenu fournira peut-être une meilleure protection des droits de l'homme et pourrait résoudre le rôle parfois ambigu des FAI, des organismes chargés de l'application de la loi et autres intervenants. Ces dernières années, nombre de pays ont introduit une législation sur la politique du contenu.

Initiatives internationales

Au niveau international, les principales initiatives sont liées aux pays d'Europe ayant une législation solide dans le domaine des discours incitant à la haine, y compris le racisme et l'antisémitisme. Les institutions régionales européennes ont tenté d'imposer ces lois sur le cyberespace. L'instrument juridique clé qui s'attaque à la question du contenu est le Protocole additionnel à la Convention sur la cybercriminalité du Conseil

de l'Europe. Le protocole dénonce différents types de discours incitant à la haine qui devraient être interdits sur l'Internet, y compris la propagande à caractère raciste et xénophobe, les propos justifiant le génocide et les crimes contre l'humanité.

L'Organisation pour la sécurité et la coopération en Europe (OSCE) est particulièrement dynamique dans ce domaine. En juin 2003, la réunion de l'OSCE sur la liberté des médias et l'Internet a adopté les Recommandations d'Amsterdam. Ces recommandations promeuvent la liberté d'expression et tentent de réduire la censure sur l'Internet. En juin 2004, l'OSCE a organisé la Conférence sur le lien entre la propagande raciste, xénophobe et antisémite sur l'Internet et les crimes de haine (à Paris, les 16 et 17 juin 2004). Le temps fort de cette manifestation concernait les usages abusifs potentiels de l'Internet et la liberté d'expression. Ces manifestations de l'OSCE ont fourni un large éventail de points de vue issus des milieux universitaires et politiques sur ces deux aspects de la surveillance du contenu.

L'UE a mené plusieurs initiatives dans le contexte du contrôle du contenu, en adoptant la Recommandation de la Commission européenne contre la diffusion de matériel raciste par l'Internet. D'un point de vue pratique, l'UE a introduit son Plan d'action pour un Internet plus sûr, qui renferme les grandes lignes suivantes:

- créer un réseau européen de lignes directes pour la notification de contenus illicites;
- promouvoir l'autorégulation;
- développer des systèmes de classement et de filtrage du contenu et d'étalonnage des logiciels et services de filtrage;
- sensibiliser le grand public à une utilisation plus sûre de l'Internet.

LES ENJEUX

Contrôle du contenu et liberté d'expression

Le revers de la médaille est que, très souvent, le contrôle du contenu implique une entrave à la liberté d'expression. Ce point est particulièrement important aux Etats-Unis, où le Premier Amendement garantit une très grande liberté d'expression, et même le droit de publier du matériel de propagande nazie et autre contenu analogue. Trouver un juste milieu entre contrôle du contenu et liberté d'expression est donc un défi considérable. L'essentiel du débat récent sur la gouvernance de l'Internet, y

compris les procès et la législation du Congrès, avait pour objectif de tenter de trouver ce juste milieu.

Le Congrès américain tend à pencher vers un contrôle du contenu plus strict, alors que la Cour Suprême cherche à protéger le Premier Amendement de la Constitution américaine (la liberté d'expression). L'exemple le plus notoire concerne la Loi du Congrès américain Communications Decency Act (Loi de 1996 sur la décence de la communication), déclarée inconstitutionnelle par la Cour Suprême qui a jugé qu'elle violait le Premier Amendement.

Dans une large mesure, c'est la liberté d'expression qui détermine la position des Etats-Unis dans le débat international sur la gouvernance de l'Internet. Ainsi par exemple, si les Etats-Unis ont effectivement ratifié la Convention sur la cybercriminalité, ils ne sont pas en mesure de signer le Protocole additionnel à cette Convention qui traite des discours incitant à la haine et au contrôle du contenu. La question de la liberté d'expression a également été soulevée dans le contexte de l'affaire Yahoo!. C'est la limite que les Etats-Unis refuseront de franchir dans les négociations internationales.

"Illicite hors ligne - Illicite en ligne"

Ce qui porte le débat sur le contenu au dilemme qui existe entre le monde "réel" et l'univers "cybernétique". Les règles existantes concernant le contenu peuvent s'appliquer à l'Internet. Ce point est souvent souligné dans le contexte européen. La Décision-cadre du Conseil de l'Europe sur la lutte contre le racisme et la xénophobie indique expressément que "ce qui est illicite hors ligne doit le rester sur les réseaux". L'un des arguments de l'approche cybernétique en matière de réglementation de l'Internet est que la quantité (volume de communications, nombre de messages) fait une différence qualitative. Sous cette optique, le problème des discours incitant à la haine n'est pas qu'aucune réglementation n'a été promulguée pour le proscrire, mais que le volume et la vulgarisation de l'Internet en font une différente sorte de problème juridique. Davantage de personnes s'y trouvent exposées et il est difficile de faire appliquer les règles existantes. Par conséquent, la différence intrinsèque de l'Internet est principalement liée aux problèmes ayant trait à l'application, et non aux règles elles mêmes.

Efficacité du contrôle du contenu

Dans les discussions sur la politique de l'Internet, l'un des principaux arguments a trait au caractère décentralisé de l'Internet qui peut contourner la censure. L'Internet comprend de nombreuses techniques et technologies qui peuvent permettre un contrôle efficace; cependant, d'un point de vue technique, il est tout aussi facile de contourner un mécanisme de contrôle. Dans les pays où le contrôle du contenu incombe au gouvernement, les internautes techniquement doués ont trouvé des moyens de contourner ces contrôles. Néanmoins, le contrôle du contenu ne s'adresse pas à ce petit groupe d'utilisateurs experts; il s'adresse plutôt à l'ensemble de la population. Lessing énonce clairement ce problème: "Il n'est pas nécessaire qu'une réglementation soit totalement efficace pour qu'elle soit suffisamment efficace".

Qui devrait être chargé de la politique du contenu?

Les principaux acteurs dans le domaine de la politique du contenu sont les pouvoirs publics. Les gouvernements prescrivent ce qu'il convient de contrôler et comment. Certains groupes de particuliers, par exemple des parents, souhaitent vivement introduire une politique de contrôle du contenu plus efficace pour protéger leurs enfants. Différentes initiatives de classement visent à aider les parents à filtrer le contenu adapté aux enfants. La politique du contenu est également assurée par des sociétés privées et des universités afin de restreindre l'accès à certains matériels. Dans certains cas, le contenu est contrôlé par le biais de progiciels; par exemple, le mouvement de Scientologie a distribué à ses membres un logiciel appelé Scienositter qui limite l'accès aux sites Web formulant des critiques à l'encontre du mouvement.

Au Royaume-Uni, la Internet Watch Foundation constitue une initiative inédite. Elle vise à lutter contre le mauvais traitement des enfants sur l'Internet. La Fondation est une initiative multipartite mise sur pied par le gouvernement, les fournisseurs d'accès à l'Internet et des représentants des internautes.

DROITS DE L'HOMME

L'Internet a introduit de nouvelles formes de communication et d'interaction dans la société et finalement été jusqu'à influencer les concepts traditionnels des droits de l'homme. Un ensemble fondamental de droits de l'homme liés à l'Internet comprend le respect de la vie privée, la liberté d'expression, le droit de recevoir des informations, différents droits qui protègent la diversité culturelle, linguistique et les minorités ainsi que le droit à l'éducation. Au cours de la première phase du SMSI, beaucoup de groupes de la société civile ont proposé l'introduction d'un droit de communiquer qui va au-delà des droits existants liés à l'Internet.

Les droits de l'homme existants qui n'ont pas été couverts dans d'autres sections de ce livret sont brièvement abordés ici.

La liberté d'expression et le droit de chercher, recevoir et répandre des informations

C'est l'un des droits humains fondamentaux, qui est normalement invoqué dans le cadre des discussions sur la politique du contenu et la censure. Dans la Déclaration universelle des droits de l'homme de l'ONU, la liberté d'expression est compensée par le droit de l'Etat à limiter la liberté d'expression pour des raisons de moralité, d'ordre public et de bien-être général (article 29). Ainsi, tant le débat que la mise en œuvre de l'article 19 doivent être replacés dans le contexte de l'établissement d'un équilibre judicieux entre deux besoins. Ce régime ambigu ouvre de nombreuses possibilités d'interprétation différente des normes et, à terme, différentes applications.

Droit à la vie privée

Le droit à la vie privée est abordé dans le chapitre qui traite de la corbeille juridique (p. 69).

Les droits de propriété intellectuelle

Les droits de propriété intellectuelle autorisent quiconque à jouir de la protection des intérêts moraux et matériels qui découlent d'une production scientifique, littéraire ou artistique. Ce droit est compensé par le droit de chacun de participer librement à la vie culturelle et de partager les progrès scientifiques. La création d'un juste équilibre entre ces deux prétentions est l'un des principaux défis auxquels doit répondre la gouvernance de l'Internet.

MULTILINGUISME ET DIVERSITE CULTURELLE

Dès sa naissance, l'Internet a été un média dominé par la langue anglaise. D'après certaines statistiques, environ 80 % du contenu du Web est en anglais. La situation a incité de nombreux pays à prendre des mesures concertées en vue de promouvoir le multilinguisme et la protection de la diversité culturelle. La promotion du multilinguisme n'est pas seulement un enjeu culturel; elle est aussi directement liée au besoin de développement supplémentaire de l'Internet. Pour que l'Internet soit utilisé par un plus grand nombre de membres de la société et pas seulement par des élites nationales, son contenu doit être accessible en plus de langues.

LES ENJEUX

Tout d'abord, la promotion du multilinguisme exige des normes techniques qui facilitent l'utilisation des alphabets autres que romains. L'une des premières initiatives en matière d'utilisation multilingue des ordinateurs était Unicode. Le Consortium Unicode est une institution à but non lucratif qui met au point des normes en vue de faciliter l'utilisation de jeux de caractères pour des langues différentes. Récemment, l'ICANN et l'IETF ont pris une décision importante en acceptant de promouvoir des noms de domaine internationaux écrits en chinois, en arabe et autres alphabets non latins.

Deuxièmement, de nombreux efforts ont été déployés pour tenter de perfectionner les logiciels de traduction automatique. Compte tenu de sa politique qui prône la traduction de tous les documents officiels dans la

langue de tous ses Etats membres, l'UE a appuyé différentes initiatives dans le domaine de la traduction automatique. Si des avancées significatives ont bien été réalisées, des contraintes subsistent.

Troisièmement, la promotion du multilinguisme exige des cadres de gouvernance appropriés. Le premier élément des régimes de gouvernance a été assuré par des organisations comme l'UNESCO. L'UNESCO a institué de nombreuses initiatives axées sur le multilinguisme, y compris l'adoption de documents importants, tels que la Déclaration universelle sur la diversité culturelle. Un autre acteur de premier plan en matière de multilinguisme est l'UE, puisqu'elle prêche le multilinguisme comme l'un de ses principes fondamentaux en termes de politique et de fonctionnement.

BIENS PUBLICS UNIVERSELS

Le concept de biens publics universels peut être lié à de nombreux aspects de la gouvernance de l'Internet. Les liens les plus directs concernent l'accès à l'infrastructure de l'Internet, la protection des connaissances développées par le biais de l'interaction avec l'Internet, la protection des normes techniques publiques et l'accès à l'enseignement en ligne.

Ce sont principalement des sociétés privées qui gèrent l'infrastructure de l'Internet. L'un des défis actuels concerne l'harmonisation de la propriété privée de l'infrastructure de l'Internet avec le statut de l'Internet comme bien public universel. Les législations nationales prévoient que la propriété privée peut être restreinte par certaines exigences publiques, y compris la fourniture de droits égaux à tous les usagers 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 des internautes à travers le monde, un nouveau savoir et de nouvelles informations voient le jour. Un savoir considérable a été généré par l'échange de listes de publipostage, les groupes de discussion et les blogues. Dans nombre de cas, il n'existe pas de mécanismes jurid-

iques internationaux qui protègent ce genre de savoir. Devant ce vide juridique, il devient possible pour les particuliers d'en faire une marchandise et de la commercialiser. Ce vivier commun de savoir, base importante de créativité, risque ainsi de s'amenuiser. Plus l'Internet est commercialisé, moins les échanges seront spontanés. Ceci pourrait déboucher sur une raréfaction de l'interaction créative. Le concept de biens publics universels pourrait fournir des solutions qui permettraient aussi de protéger le savoir mis en commun sur l'Internet pour les générations futures.

En ce qui concerne la normalisation, des efforts quasi-permanents sont faits pour remplacer les normes publiques par des normes privées et propriétaires. C'est ce qui se produit avec Microsoft (par le biais des navigateurs et d'ASP) et avec Sun Microsystems (par le biais de Java). Les normes Internet (essentiellement TCP/IP) sont considérées comme étant ouvertes et publiques. Le régime de gouvernance de l'Internet devrait veiller à protéger les principaux standards de l'Internet en tant que biens publics universels.

Protection de l'Internet comme bien public universel

Certaines solutions basées sur le concept de l'Internet comme bien public universel peuvent être élaborées à partir des concepts économiques et juridiques existants. Ainsi par exemple, la théorie économique propose un concept bien développé de "bien public" qui a été élargi au niveau international au concept de "bien public universel". Un bien public présente deux propriétés essentielles: consommation non concurrente et caractère non exclusif. La première suppose que la consommation par un individu n'empêche pas celle d'un autre; la seconde, qu'il est difficile, si ce n'est impossible, d'exclure une personne de la jouissance du bien en question. Au niveau mondial, le Programme des Nations Unies pour le développement (PNUD) a introduit le concept de bien public universel. Dans le droit international, une solution potentielle est le concept de res communis omnim (espace de patrimoine commun à toute l'humanité devant être réglementé et entretenu par toutes les nations).

Il sera important de considérer lequel de ces concepts pourra s'appliquer à l'Internet et avec quelles conséquences. Nombreux sont ceux qui reconnaissent que l'orientation de l'évolution future de l'Internet dépendra de l'établissement d'un juste milieu entre les intérêts publics et privés.

ENSEIGNEMENT

L'Internet a ouvert de nouvelles possibilités en termes d'enseignement. Différentes initiatives "d'apprentissage électronique", "d'apprentissage en ligne" ou "d'apprentissage à distance" ont été introduites, leur objectif premier étant d'utiliser l'Internet comme moyen de dispenser les cours. Si l'Internet ne saurait remplacer l'enseignement classique, l'éducation en ligne offre de nouvelles possibilités d'apprentissage, tout particulièrement lorsque des contraintes de temps et d'espace empêchent une personne de se rendre en classe. Certains pronostics avancent que le marché de l'apprentissage en ligne pourrait représenter environ US$10 milliards d'ici 2010.

L'apprentissage en ligne a également engendré un enseignement transfrontière plus intensif, avec des étudiants qui participent à des cours de formation en ligne dispensés par d'autres pays. Ce phénomène a introduit une dimension de gouvernance internationale dans le secteur éducatif.

De par tradition, l'enseignement a été gouverné par des institutions nationales. L'agrément des établissements d'enseignement, la reconnaissance des qualifications et l'assurance qualité sont autant d'éléments qui sont régis au niveau national. Toutefois, l'enseignement transfrontière nécessite l'établissement de nouveaux régimes de gouvernance. De nombreuses initiatives internationales visent à combler l'écart de gouvernance, notamment dans des domaines comme l'assurance qualité et la reconnaissance des diplômes universitaires.

L'OMC et l'enseignement

Une question très controversée dans les négociations de l'OMC concerne l'interprétation des articles 1 (3) (b) et (c) de l'Accord général sur le commerce de services, qui stipule des exceptions au régime de libre échange pour les services dispensés par le gouvernement. Certains, et c'est généralement l'avis des Etats-Unis et du Royaume-Uni, estiment que 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 protéger les intérêts des secteurs didactiques américain et britannique afin de se tailler la part du lion sur le marché mondial de l'enseignement et il a fait l'objet d'une vive opposition de la part de nombreux autres pays.

Le principal argument opposé à ce point de vue est que les universités offrent un service public et qu'elles ont un rôle social et culturel important à jouer dans chaque pays, au-delà du simple transfert de connaissances et d'informations. Selon ce point de vue, un marché mondial libre dans le secteur de l'enseignement pourrait léser les universités des petits pays et des pays en développement et déboucher sur une dominance didactique des établissements d'enseignement des Etats-Unis et du Royaume-Uni, réduisant ainsi considérablement la diversité culturelle et privant bon nombre de sociétés du rôle catalyseur des universités dans le développement de la culture nationale. Une autre critique du libre échange dans le secteur de l'enseignement réside dans son incompatibilité potentielle avec l'application du droit à l'éducation.

Le futur débat, qui verra probablement le jour dans le contexte de l'OMC et de certaines autres organisations internationales, sera axé sur le dilemme de l'enseignement en tant que marchandise ou en tant que bien public. Si l'enseignement est considéré comme une marchandise, les règles de libre échange de l'OMC deviendront aussi applicables dans ce domaine. En revanche, l'approche de bien public préserverait le modèle actuel en matière d'enseignement aux termes duquel les universités publiques bénéficient d'un statut spécial en guise d'institutions importantes pour la culture nationale. Le résultat de ce débat aura un impact considérable sur le développement de l'apprentissage en ligne.

Assurance qualité

La disponibilité de systèmes de délivrance d'apprentissage en ligne et une pénétration relativement aisée de ce marché ont mis en exergue la question de l'assurance qualité. En mettant trop l'accent sur la fourniture en ligne, on peut oublier l'importance de la qualité des supports et de la didactique. Une grande variété de difficultés possibles peut compromettre la qualité de l'enseignement. L'une concerne la montée en ligne relativement aisée de nouveaux établissements d'enseignement, le plus souvent à but lucratif, qui bien souvent n'ont que très peu des capacités didactiques et pédagogiques requises. Un autre problème en matière d'assurance qualité réside dans le fait que le simple transfert des supports pédagogiques classiques sur papier vers des supports en ligne

ne tire pas pleinement parti du potentiel qu'offre le nouveau média en termes d'enseignement.

Des discussions sur l'apprentissage transfrontière en général et l'apprentissage virtuel en particulier ont commencé au niveau international. L'une des tentatives les plus exhaustives afin de fournir une assurance qualité pour les programmes d'enseignement transnationaux est celle de l'UNESCO et du Conseil de l'Europe dans leur "Code de bonne pratique pour la fourniture d'un enseignement transnational".

La reconnaissance des diplômes universitaires et le transfert de crédits

La reconnaissance des diplômes est devenue une question particulièrement pertinente au sein de l'apprentissage virtuel, le principal défi étant la reconnaissance des diplômes au-delà du contexte régional, à une échelle principalement mondiale.

La tendance générale qui promeut la mobilité des étudiants dans l'enseignement supérieur fait qu'il est possible d'étudier dans un certain nombre d'universités. L'UE, en particulier, a fait des progrès remarquables dans ce domaine par le biais de diverses initiatives, telles que le programme Socrate. La mobilité des étudiants exige le transfert des crédits d'enseignement entre universités de différents pays. Les cadres réglementaires requis ont commencé à se développer au niveau régional. L'UE a elle-même commencé à élaborer un cadre réglementaire avec le Système européen de transfert de crédits (ECTS). La région Asie-Pacifique suit dans le sillage de l'Europe en introduisant son propre modèle régional pour les échanges d'étudiants et un système associé de crédits (UCTS).

La normalisation de l'apprentissage en ligne

La phase initiale du développement de l'apprentissage en ligne s'est caractérisée par un rapide essor et par une grande diversité des matériels, en termes de plates-formes, de contenus et de didactique. Toutefois, il est nécessaire de mettre au point des normes communes afin de faciliter l'échange de formations en ligne et d'introduire un certain étalon de référence en termes de qualité.

La première norme, AICC (Aviation Industry CBT Committee), a été élaborée par l'association des professionnels de l'aviation avec pour objectif premier d'assurer une certaine interopérabilité dans les program-

mes d'enseignement virtuel indépendamment des contenus et des plates-formes. L'autre développement majeur a été l'avènement de l'IMS (Instructional Management System), qui a introduit un certain nombre de normes dans le domaine de l'apprentissage virtuel, y compris les spécifications de métadonnées pouvant être partagées par des ressources de téléenseignement (description du contenu, intitulé de la formation, auteurs, coût, taxonomie de l'apprentissage, etc.). L'IMS est basé sur XML (eXtended Markup Language). En outre, le Learning Technology Standards Committee (LTSC) de l'Institut des ingénieurs électriciens et électroniciens (IEEE) a réalisé divers travaux dans le domaine de la normalisation.

Le Ministère américain de la Défense (DoD) a lancé le développement le plus récent en 1997. Confronté aux limites intrinsèques de toutes les normes existantes, le DoD a créé l'initiative ADL (Advanced Distributed Learning - Apprentissage distribué avancé), qui a donné naissance à une nouvelle norme appelée SCORM (Shareable Content Object Reference Model - Modèle de référence pour les objets de contenu d'apprentissage partageables). SCORM est la norme la plus sophistiquée et la plus répandue pour les ressources de téléformation. L'une des raisons du succès de SCORM réside dans le fait qu'elle est devenue la norme exigée pour les cours dispensés au DoD (un marché d'une valeur de quelque US$700 millions par an) et aux autres services gouvernementaux américains. De ce fait, SCORM acquiert une très haute visibilité à l'international et son usage devient de plus en plus répandu.

L'essentiel des initiatives de normalisation intervient aux Etats-Unis sous l'égide d'établissements privés et professionnels. Les autres initiatives, y compris à l'international, sont d'une portée bien moindre.

SECTION 7

Annexes

ANNEXE I

"LES AVEUGLES ET L'ELEPHANT"

Un jour six hommes de l'Hindoustan
Tous enclins à apprendre,
S'en vinrent voir un Eléphant
(Et pourtant tous étaient aveugles),
Pour tenter par observation
De satisfaire leur soif de savoir.

Le premier approcha l'Eléphant,
Et, perdant pied, alla buter
Contre son flanc large et robuste,
Et de suite de s'exclamer:
"A Dieu ne plaise! mais l'Eléphant
Ressemble beaucoup à un mur!"

Le second, palpant une défense,
s'écria: "Qu'avons-nous donc ici
Si rond, si lisse et si pointu?
A mon avis, rien n'est plus clair
Cet Eléphant extraordinaire
Ressemble beaucoup à une lance!"

Le troisième s'avança vers l'animal,
Et, ce faisant, il s'empara
De sa trompe qui se tortillait,
Sans hésiter, il déclara:
"Je vois fort bien que l'Eléphant
Ressemble beaucoup à un serpent!"

Le quatrième tendit allègrement la main
et se prit à toucher le genou de la bête.
"A quoi ressemble cet animal extraordinaire
Ne fait pas le moindre mystère,"
"Cet Eléphant, c'est l'évidence,
Ressemble beaucoup à un arbre!"

Le cinquième, qui par chance se saisit de l'oreille,
Déclara: "Même le plus aveugle des hommes
Peut dire à quoi il ressemble le plus;
Nul ne saurait le nier
Cette merveille que l'on nomme Eléphant
Ressemble beaucoup à un éventail!"

A peine le sixième avait-il commencé
A tâtonner la bête,
Que sa queue qui se balançait
Lui arriva entre les mains,
"Je vois," prononça-t-il, "l'Eléphant
Ressemble beaucoup à une corde!"

Ainsi ces hommes de l'Hindoustan
Se disputèrent longuement,
Chacun soutenant son avis
Avec force et obstination.
Si chacun avait en partie raison,
Pour l'ensemble, tous avaient tort!
Moralité: Trop souvent dans les guerres théologiques,
Les parties en conflit, je crois,
Se moquent dans la plus totale ignorance
De ce que veulent dire leurs opposants
Et palabrent à n'en plus finir sur un Eléphant
Qu'aucune d'entre elles n'a jamais vu!

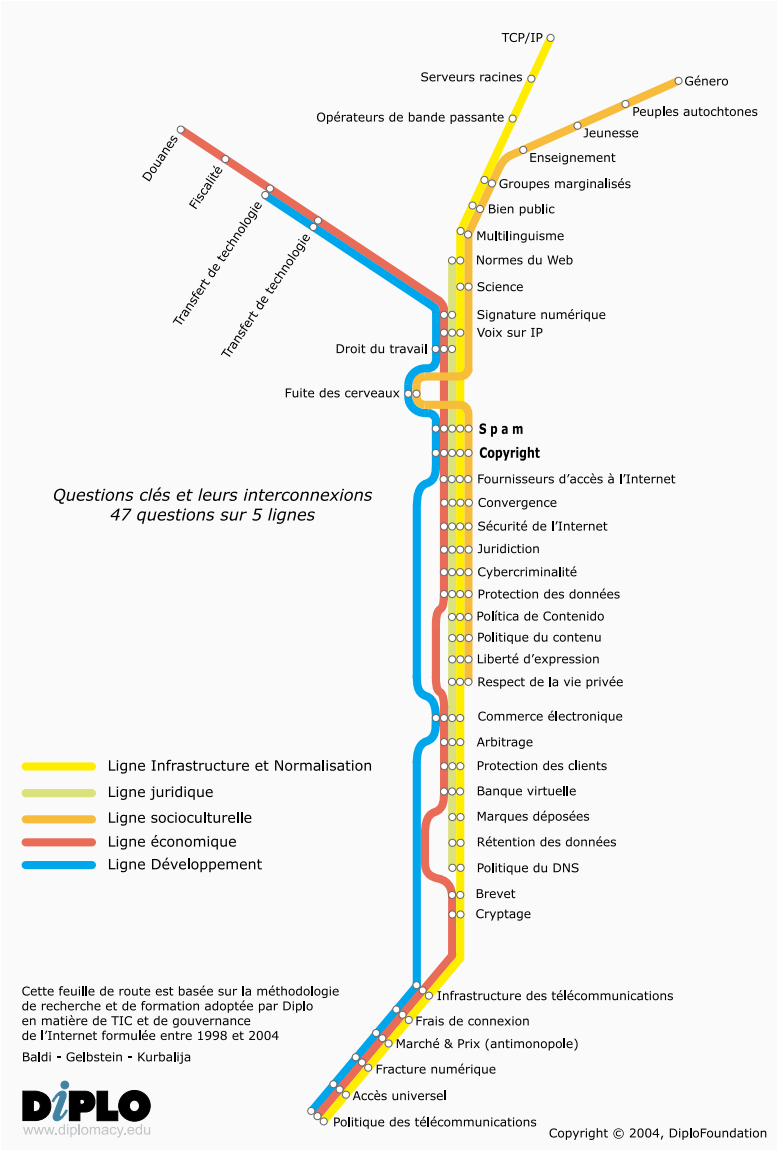
John Godfrey Saxe, poète américain (1816-1887)

ANNEXE II – SYNTHESE DE L'EVOLUTION DE LA GOUVERNANCE DE L'INTERNET

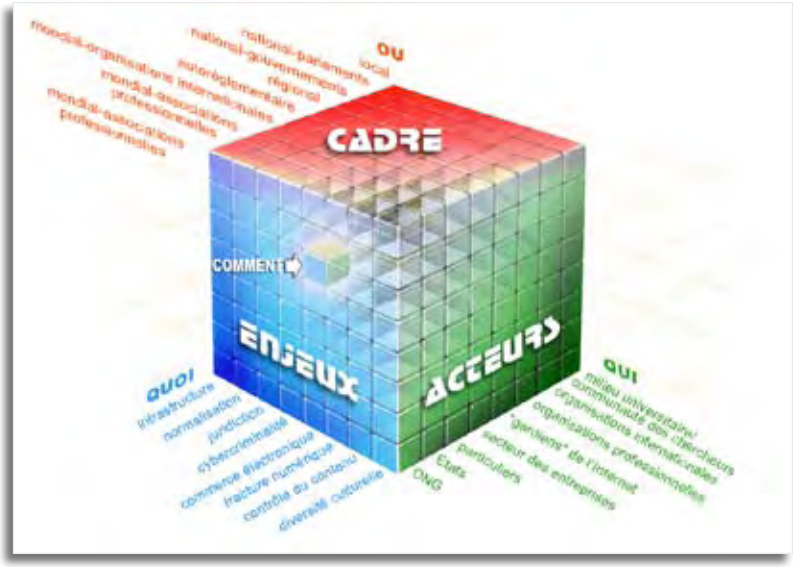
Acteur / Période	Etats-Unis	"Gardiens" de l'Internet	Organisations internationales	Secteur privé	Pays	Société civile
	Le Ministère de la Défense (DoD) gère le DNS					
1986	La National Science Foundation (NSF) prend le relais du DoD					
1994				NSI signe un contrat avec la NSF pour gérer le DNS de 1994 à 1998		
DEBUT DE LA "GUERRE DU DNS". DEBUT DE LA "GUERRE DU DNS". Lorsque la NSF a sous-traité la gestion du DNS à NSI (une société privée), la communauté Internet (principalement l'ISOC) a tenté pendant plusieurs années de ramener la gestion du DNS dans le domaine public. Elle y est parvenue au bout de 4 ans. Ci-après figure un tour d'horizon de ce processus, qui a eu recours à maintes techniques diplomatiques: négociations, formation de coalition, usage de pressions, formation de consensus, etc.						
Juin 1996		L'IANA/ISOC - entendent prendre le relais de NSI à expiration de son contrat; introduction de domaines supplémentaires; vive opposition du secteur des marques à la création de domaines de niveau supérieur; vive opposition de l'IUT également				
Printemps 1997		Proposition de l'IAHC (Comité ad hoc international). Composition de l'IAHC: 2 représentants des groupes d'intérêts des marques déposées, OMPI, UIT et NSF plus 5 représentants de l'IETF. Conclusion du Mémorandum d'Accord sur les gTLD décrivant le DNS comme une "ressource publique"; sept nouveaux domaines; solide protection des marques déposées. Création de CORE (Conseil des Registres - cérémonie d'inauguration en mars 1997 à l'UIT de Genève); CORE s'est immédiatement effondrée. Vive opposition du gouvernement des Etats-Unis, de NSI et de l'UE.				
1997	Le gouvernement des Etats-Unis transfère la gestion du DNS au Ministère du Commerce (DoC)					
Juin 1998	Un livre blanc du MdC invite les principaux acteurs à proposer leur propre solution	Des propositions sont reçues de l'IFDT (International Forum on White Paper), de l'ORSC (Open Root Server Confederation) et du BWG (Boston Working Group)				
		Au lieu de rédiger un nouveau document, l'ISOC se concentre sur: - la formation d'une vaste coalition regroupant des organisations internationales (ayant participé à l'initiative IAHC), le secteur privé (IBM) et des pays clés (l'UE, le Japon, l'Australie); - la création d'une nouvelle organisation				

Deuxième moitié de 1998		Septembre 1998 - Projet d'accord mixte entre l'ISOC et NSI Octobre 1998 - l'ISOC révoque l'accord et crée l'ICANN				
15 nov. 1998	Le DoC transfère l'autorité à l'ICANN	L'ICANN acquiert deux nouvelles fonctions vitales: - Pouvoir d'accréditation des registres pour les gTLD - Gestion du rôle de supervision (la dimension politique reste aux mains du DoC)				
Avril 1999		Signature d'un accord DoC - ICANN - NSI et introduction d'un "système de registres partagés"; NSI perd son monopole mais obtient un accord de transition à son avantage (gestion de quatre domaines, etc.) LA STRUCTURE ET LE FONCTIONNEMENT DE L'ICANN				
Juin 1998		Formation de PSO (Protocol Supporting Organisation) regroupant l'IETF, le W3C et d'autres pionniers de l'Internet	Initialisation du processus de noms de domaine Internet de l'OMPI	Création de l'ASO (Address Support Organisation) pour représenter l'association des registres de DNS (ARN, RIPE, NCC); création de la DNSO (Domain Name Supporting Organisation) pour protéger les marques et les intérêts commerciaux.	30 pays établissent un GAC (Comité consultatif gouvernemental) afin de gagner davantage d'influence dans la gestion des domaines nationaux. L'ICANN réagit en créant le sous-comité de la DNSO – ccTLD	
FIN DE "LA GUERRE DU DNS" La "guerre" s'est terminée sur un compromis. L'ISOC a réussi à obtenir davantage de contrôle public sur la gestion du DNS même si les intérêts commerciaux restaient très puissants. Ainsi, les intérêts du secteur privé et des "gardiens" de l'Internet se trouvaient convenablement protégés. Ce n'était pas le cas de ceux des Etats nations et de la communauté Internet dans son ensemble. Ce sont les deux aspects les plus vulnérables de la gouvernance de l'ICANN.						
2000-2003			Emergence d'une plus grande attention accordée à l'Internet au sein de l'UIT, de l'OMPI, de l'UNESCO, de l'OCDE, du Conseil de l'Europe et de la Banque mondiale	Fortes pressions de la part du secteur privé en faveur d'un Internet réglementé (lois sur les droits d'auteur, le commerce électronique, etc.)	Développement d'une législation sur l'Internet, procès, etc.	Participation des ONG à des questions telles que la fracture numérique, les droits de l'homme, la parité des sexes sur l'Internet, etc.
			Initiatives multisectorielles et mondiales axées sur l'essor de l'Internet, la gouvernance, etc.: la Dot Force du G8, le Forum économique mondial, le Groupe de travail des Nations Unies sur les TIC, le Sommet mondial sur la société de l'information, le Global Knowledge Partnership.			

ANNEXE III - FEUILLE DE ROUTE POUR UN VOYAGE A TRAVERS LA GOUVERNANCE DE L'INTERNET



ANNEXE IV - CUBE DIPLO DE LA GOUVERNANCE DE L'INTERNET



L'axe QUOI a trait aux ENJEUX que soulève la gouvernance de l'Internet (par ex. l'infrastructure, les droits d'auteur, le respect de la vie privée). Il traduit la dimension multidisciplinaire de cette approche. L'axe QUI du cube se concentre sur les principaux ACTEURS (Etats, organisations internationales, société civile, secteur privé). C'est le côté multipartite de l'approche. L'axe OU du cube traite du CADRE dans lequel il convient d'aborder les questions liées à l'Internet (autoréglementaire, local, national, régional ou mondial). Il s'agit d'une approche stratifiée de la gouvernance de l'Internet.	En déplaçant les pièces du cube, nous obtenons l'intersection - COMMENT. C'est la section du cube qui peut nous aider à voir comment certaines questions précises devraient être réglementées, en termes de techniques cognitives-juridiques (par ex. analogies) et en termes d'instruments (par ex. loi molle, traités et déclarations). Ainsi par exemple, une intersection spécifique peut nous aider à voir COMMENT les questions ayant trait au respect de la vie privée (le quoi) devraient être abordées par la société civile (le qui) au niveau national (le où). Distinct du cube de la gouvernance de l'Internet figure un cinquième élément - QUAND.

A PROPOS DES AUTEURS

Jovan Kurbalija

Jovan Kurbalija est le directeur fondateur de DiploFoundation. Ancien diplomate, il jouit d'une carrière professionnelle et universitaire distinguée en droit international, en relations internationales et en technologies de l'information. Depuis la fin des années quatre-vingt, il mène des recherches dans le domaine des TIC et du droit. En 1992, il a été chargé de créer le premier Pôle sur les Technologies de l'Information et la Diplomatie à l'Académie méditerranéenne des Etudes diplomatiques à Malte. Après plus d'une décennie d'initiatives couronnées de succès dans le domaine de la formation, de la recherche et de l'édition, en 2003 le Pôle est devenu la DiploFoundation.

Jovan Kurbalija dirige des téléformations dans le domaine des TIC et de la diplomatie et il donne des conférences auprès de divers établissements universitaires et didactiques en Suisse, aux Etats-Unis, en Autriche, au Royaume-Uni, aux Pays-Bas et à Malte. Il était également membre du Groupe de travail des Nations Unies sur la gouvernance de l'Internet.

Du point de vue de la recherche, ses principaux centres d'intérêt gravitent autour de la diplomatie et du développement d'un régime international pour l'Internet, l'utilisation de l'hypertexte dans les relations internationales, les négociations en ligne et le droit diplomatique.

jovank@diplomacy.edu

Ed Gelbstein

Eduardo Gelbstein est membre honoraire de l'Institut des Nations Unies pour la formation et la recherche (UNITAR); il est collaborateur du Groupe de travail des Nations Unies sur les technologies de l'information et des communications (TIC) et a participé aux travaux préparatoires du Sommet mondial sur la société de l'information. Ancien directeur du Centre international d'informatique des Nations Unies.

Outre sa collaboration avec les Nations Unies, ses prestations de conférencier et de maître de conférence reflètent 40 ans d'expérience en matière de gestion des technologies de l'information.

Il a travaillé en Argentine, aux Pays-Bas, au Royaume-Uni et en Australie avant de rejoindre le système onusien en 1993, à Genève d'abord puis à New York. Il a obtenu un diplôme d'ingénieur électronicien de l'Université de Buenos Aires en 1963 et détient une maîtrise obtenue aux Pays Bas et un doctorat décroché au Royaume-Uni.

gelbstein@diplomacy.edu

INFORMATION SOCIETY LIBRARY

Ce ne sont certes pas les ouvrages sur les technologies et la gestion de l'information qui font défaut. Ce livre vient s'ajouter à la kyrielle d'ouvrages sur ce thème mais il entend faire un certain nombre de choses:

- donner aux lecteurs non initiés un aperçu des quelques principes qui sont importants et relativement pérennes dans ce domaine;
- présenter le matériel dans un contexte qui soit pertinent pour les travaux de ceux qui sont impliqués dans les relations internationales;
- piquer suffisamment la curiosité des lecteurs pour qu'ils s'aventurent au-delà de cet ouvrage afin d'explorer ce domaine et de se livrer à des expériences pour renforcer leurs connaissances et prendre des mesures qui répondront à leurs besoins propres.

Le format de ces livrets et leur contenu s'inspirent des cours donnés par les auteurs durant les dernières années dans divers environnements et des réactions des participants. Les commentaires éventuels des lecteurs à propos de ces ouvrages seraient vivement appréciés par les auteurs pour leur permettre de peaufiner les éditions futures.

AUTRES TITRES PARUS DANS LA COLLECTION INFORMATION SOCIETY LIBRARY

Internet Basics • FAQs, Facts and FFPs (Frequently Found Problems)

Finding Information in Cyberspace • From irritation to inspiration

Good Hygiene for Data and Personal Computers • Why and how to protect Data and personal computers

Appropriate Use • Guidelines and best practices for e-mail and other Internet services

Information Security and Organisations • A non-technical guide to players, offences and effective defences

Hacktivism, Cyber-terrorism and Cyberwar • The activities of the uncivil society in cyberspace

Online Learning for Professionals in Full Time Work • A guide to what works and what does not

Yellow Pages for the Information Society Library • A directory of recommended URLs

SERIE KNOWLEDGE FOR DEVELOPMENT

Cette publication fait partie de la série "Knowledge for Development" publiée par le Global Knowledge Partnership, initiative mondiale visant à accroître la disponibilité de l'information et des connaissances sur diverses questions relevant du domaine des TIC au service du développement.

AUTRES TITRES PARUS DANS LA SERIE KNOWLEDGE FOR DEVELOPMENT

Media and the Information Society

Multi-Stakeholder Partnerships

ICT for Development Success Stories

ICT for Poverty Reduction in Asia

www.diplomacy.edu

Diplo *est une organisation à but non lucratif dont le but est d'aider tous les pays, et plus particulièrement ceux qui ont des ressources limitées, à participer pleinement aux relations internationales. Diplo promeut une approche multipartite, impliquant la participation d'organisations internationales, de la société civile et d'autres acteurs des affaires internationales. Aux rangs des activités de Diplo figurent des programmes d'enseignement et de formation, des recherches et le développement de technologies de l'information et des communications pour les milieux diplomatiques.*

www.globalknowledge.org

Le Global Knowledge Partnership(GKP) *est un réseau mondial qui s'attache à mettre le potentiel des technologies de l'information et des communications (TIC) au service d'un développement durable et équitable. La vision de GKP prône un monde où chacun a des chances égales et peut accéder au savoir et aux informations et s'en servir pour améliorer sa vie quotidienne. Le réseau promeut l'échange d'informations, d'expériences et de ressources pour contribuer à la réduction de la pauvreté et à l'autonomisation des peuples.*

DEZA
DDC
DSC
SDC
COSUDE

www.sdc.admin.ch

La Direction du développement et de la coopération (DDC) *est l'agence chargée de la coopération internationale au sein du Département fédéral des affaires étrangères (DFAE). La DDC est responsable de la coordination générale de la coopération au développement et de la coopération à l'Est avec d'autres offices de la Confédération ainsi que de l'aide humanitaire de la Suisse.*

ISBN 99932-53-14-6
9 789993 253143