ICANN ET LA GOUVERNANCE D'INTERNET

La coordination technique comme levier d'une politique publique mondiale

Hans Klein

Lavoisier | « Les Cahiers du numérique »

2002/2 Vol. 3 | pages 91 à 128

ISSN 1622-1494
ISBN 2746205106

Deuxième partie

Une souveraineté « introuvable » : organiser et nommer le monde numérique

ICANN et la gouvernance d'internet

La coordination technique comme levier d'une politique publique mondiale[1]

Hans Klein

La gouvernance d'internet

Internet est souvent salué comme un royaume d'anarchie bienveillante, où la communication libre est solidement établie. C'est une « hydre moderne » capable de contourner la réglementation (Froomkin, 1999, p. 129) et un « espace hors contrôle » (Lessig 1999, p. 24). Comme le dit John Perry Barlow, chantre de l'internet, « *Ô gouvernements du monde industriel ... vous n'avez point de souveraineté là où nous nous rassemblons.* » (cité *in* Lessig, 1999, p. 218).

Pour le dire de façon moins pittoresque, internet met à l'épreuve la *gouvernance*. J'entends par « gouvernance » l'existence d'une quelconque autorité capable de créer pour l'usage d'internet des règles globalement

1. Une première version de l'article est parue in *The Information Society*, vol. 18, n° 3, 2002 (Tailor and Francis ed.). Les recherches contribuant à cette étude ont été effectuées lors d'une résidence au Centre de sociologie de l'innovation de l'Ecole des Mines de Paris, avec le soutien d'une bourse Chateaubriand de l'Ambassade de France aux Etats-Unis. Traduction de Rosemary PeterCricks et Françoise Massit-Folléa.

LCN, volume 3, n° 2-2002, pages 93 à 128

applicables et renforcées par des sanctions. La gouvernance d'internet existe sous des formes diverses et partielles (salons de *chat* sur AOL, ou réglementation gouvernementale des ordinateurs à l'intérieur du territoire national), mais, dans l'ensemble, internet ne possède pas de système cohérent et efficace pour établir et imposer autoritairement des règles. Cela s'explique tant par les caractéristiques de la technologie (qui rendent difficile tout contrôle) que par l'expansion mondiale des communications *via* internet (qui crée un conflit de juridiction entre les régulateurs gouvernementaux).

Cette dimension « ingouvernable » d'internet, pourtant, est en train de changer. Dans son livre *Code* (1999), Lawrence Lessig analyse diverses stratégies visant à éliminer l'anonymat des internautes et à faciliter l'application de lois contraignantes. Exemple récent : à la suite d'un procès concernant la vente aux enchères sur internet de souvenirs nazis, interdite en France, la société *Yahoo!* fut condamnée à détecter l'origine géographique des utilisateurs pour leur appliquer la législation sur les contenus en vigueur dans leur pays (AFP, 2000). Comme avec d'autres technologies antérieures, plus internet se répand dans la société, plus on tâche de l'intégrer dans les structures réglementaires existantes.

Le développement le plus significatif de cette tendance à « gouverner » internet est la création d'ICANN (Internet Corporation for Assigned Names and Numbers). Créée en 1998, ICANN est une association privée à but non lucratif, ayant reçu le mandat officiel d'effectuer la coordination technique des ressources fondamentales d'internet, tout particulièrement les noms de domaine (par exemple *monordinateur.org*). Bien qu'elle soit implantée en Californie, son autorité s'étend, directement ou indirectement, à tous les utilisateurs d'internet.

ICANN a le potentiel de changer radicalement la nature d'internet. En mettant en place tous les mécanismes nécessaires à la création, à la promulgation et au renforcement de la régulation, ICANN rend possible, pour la première fois, une vraie gouvernance d'internet. Internet ne sera plus désormais cette Hydre incontrôlable. Or, les mécanismes de gouvernance d'ICANN rendent possibles toutes sortes de régulations. A de nombreuses reprises, ces dernières années, des tentatives de réglementation d'internet sont apparues, signe d'un intérêt grandissant pour de tels mécanismes (Froomkin, 1997). Selon les points de vue, la création d'une capacité de gouvernance implique la promesse ou la menace d'une maîtrise de la frontière électronique.

Je vais présenter une analyse détaillée d'ICANN, pour rendre compréhensible le rapport mutuel entre technologie, administration et

gouvernance, en expliquant comment le système d'adressage d'un réseau d'ordinateurs facilite un système de gouvernance. Pour ce faire, je commencerai par expliquer ce qu'est la gouvernance, le fonctionnement du système des noms de domaines sur internet (DNS) et la manière dont le DNS permet la gouvernance.

Cette mise au point pourra éclairer la politique des décideurs comme celle des utilisateurs d'internet. Le fait qu'internet a un point de contrôle central et qu'ICANN exerce une politique publique globale est loin d'être communément admis. La reconnaissance de ces capacités de gouvernance justifie l'application des critères normatifs de légitimité, de responsabilité et d'équité à l'institution et à son fonctionnement. Notre étude participe d'ailleurs d'un ensemble croissant de travaux qui analysent politiquement ICANN dans la perspective de ses origines historiques (Mueller, 1999 ; Klein, 2001a), de son statut légal (Froomkin, 2000 ; Klein, 2001c) et de sa conception institutionnelle (Post, 1998).

Elle prend aussi en compte les débats théoriques portant sur le rapport entre systèmes technologiques et contexte social. Des études récentes sur la construction sociale de la technologie ont souligné l'influence des facteurs sociaux sur les modalités du changement technologique (Bijker, 1995 ; Bijker, Hughes, Pinch, 1987 ; Klein et Kleinman, 2002). De même, des spécialistes de la politique des techniques ont insisté sur le fait que concevoir un système informatique s'apparente à légiférer, dans la mesure où les deux activités engendrent des structures sociales qui contraignent le comportement humain (Lessig, 1999 ; Kapor, 1990 ; Klein, 2000). ICANN présente à l'évidence les caractéristiques d'une telle structuration sociale, dans la mesure où le système de noms de domaine (DNS) définit des paramètres importants de gouvernance.

Je considérerai tout d'abord les facteurs technologiques et institutionnels qui ont, jusqu'ici, empêché la régulation d'internet, puis je discuterai plus largement la notion de gouvernance. Ensuite j'examinerai le système des noms de domaine en tant que hiérarchie technologique et administrative, en identifiant les caractéristiques qui permettent la gouvernance. Suivra une analyse des mécanismes de gouvernance d'internet, tels que concrétisés par ICANN. Puis, pour illustrer la manière dont les mécanismes de gouvernance fonctionnent en pratique, j'étudierai la politique publique mondiale d'ICANN à travers la façon dont elle a défini les droits de propriété pour les noms de domaine. Enfin je considérerai le problème de légitimité posé par ICANN et je m'interrogerai sur les aires de régulation envisageables pour l'avenir.

Le problème de la gouvernance d'internet

Que l'on soit pour ou contre des régulations spécifiques, on reconnaît généralement que la régulation d'internet s'est toujours avérée difficile. Copier une musique, des logiciels et d'autres formes de propriété intellectuelle devient de plus en plus aisé, et la multiplication des actions en justice à l'encontre de ceux qui violent la propriété ne représente sans doute qu'une part infime des cas de copies non autorisées (Fryer, 1995). Des tentatives de contrôle des contenus [d'internet] par des gouvernements nationaux ont buté sur la nature mondiale d'internet et des conflits interjuridictionnels (Andrews, 1999).

Les barrières à la régulation proviennent en partie des caractéristiques de la technologie. Les communications d'internet ne passent pas par un canal central mais, au contraire, par plusieurs réseaux indépendants, et les messages eux-mêmes se séparent en espèces de paquets numériques qui suivent divers itinéraires de leur source à leur destination (Cerf et Kahn, 1974). De multiples émetteurs indépendants envoient de multiples paquets indépendants à travers de multiples canaux indépendants : il n'existe donc pas de canal central de communication qui pourrait servir de point de contrôle pour la promulgation et l'application des règles.

La régulation bute également sur des facteurs institutionnels. Internet met à l'épreuve les juridictions établies (Johnson et Post, 1997 ; Perrit, 1997). L'autorité publique relève de l'Etat, dont la caractéristique de base est d'exercer son contrôle sur un domaine géographiquement défini (Schroeder, 1998). Or la nature « a-spatiale » d'internet met en cause ces fondements géographiques de l'autorité publique (Holitscher, 1999). La discordance entre un réseau mondial et des règles nationales sape bien des tentatives réglementaires (Froomkin, 1997).

Pour comprendre l'essence de cette situation, il est utile de prendre du recul par rapport aux détails et de considérer la gouvernance d'un point de vue théorique. Qu'est-ce que la gouvernance ? Qu'est-ce qui est nécessaire pour gouverner ? Que requiert la gouvernance d'internet ?

Dans son ouvrage *La démocratie et ses critiques* (1989), Robert Dahl explique ce qu'est la gouvernance et comment l'atteindre. Il identifie une série d'« hypothèses politiques » (p. 106-107) qui précisent les conditions minimales pour un système de gouvernance. Ces conditions, je les appelle les « mécanismes de la gouvernance ». En paraphrasant la définition de Dahl, on peut identifier quatre de ces mécanismes, dont le premier sera *l'autorité*. La gouvernance demande un gouverneur ou un souverain. Une

entité – individu ou groupe – doit prendre les décisions politiques qui s'appliquent aux membres de la communauté. Un deuxième mécanisme de gouvernance est *la loi*. Les lois mettent en œuvre des décisions politiques, sous la forme soit d'une taxe, soit d'une autorisation, ou simplement d'une règle qui engage. Troisièmement, il faut un mécanisme pour imposer des *sanctions* qui permettent de punir ceux qui violent les lois. Enfin, la gouvernance exige une définition de la *juridiction*. Celle-ci définit l'espace au sein duquel l'autorité peut appliquer ses décisions et où les lois sont applicables sous peine de sanctions. Ces quatre mécanismes rendent possible la gouvernance : *l'autorité* gouvernante peut prendre une décision politique qui s'appliquera à l'intérieur de sa juridiction, en incorporant cette décision dans des *lois* et en imposant des *sanctions* à tous ceux qui ne s'y conforment pas (cette analyse se retrouve dans l'appendice de *Code* [Lessig, 1999]).

Le caractère ingouvernable et tant vanté d'internet résulte de l'absence de ces quatre mécanismes. La régulation est difficile parce que l'autorité, la loi, les sanctions et la juridiction ne sont pas assurées.

Or ICANN réalise ces quatre mécanismes à travers son contrôle du système de noms de domaine internet (DNS). Contrairement aux autres aspects d'internet, le DNS est centralisé : bien que la communication par internet soit décentralisée, l'adressage sur internet est centralisé. Le DNS fournit le point de contrôle à partir duquel il est possible de réguler les utilisateurs. Le DNS est aussi une ressource essentielle, et comme tel fournit un moyen d'appliquer des sanctions aux utilisateurs : le refus d'accès aux noms de domaine est l'équivalent du bannissement d'internet. En outre, le DNS définit en grande partie les juridictions d'internet. L'organisation logique du DNS répartit l'autorité sur des zones distinctes. Les fondements contractuels du DNS permettent de promulguer des règles. Associées les unes aux autres, ces caractéristiques rendent ICANN capable de gouvernance.

Mais pour comprendre ICANN, il faut d'abord comprendre le système des noms de domaines.

Le DNS et la gouvernance : état des lieux

Je vais analyser le DNS en deux étapes, le présentant d'abord sous sa forme simplifiée : un système unique et non distribué. Dans cette perspective, les caractéristiques de la gouvernance du DNS sont plus visibles. J'étudierai par la suite la structure interne et distribuée du DNS et

présenterai les divers mécanismes utilisés pour assurer la cohérence de l'administration et de la décision politique.

Le DNS, point de contrôle d'internet

Commençons par une réalité méconnue : internet consiste dans la réunion de deux « systèmes », dont l'un vise la *communication* (les protocoles TCP/IP) et l'autre l'*adressage* (le DNS). Le système de communication est l'aspect le plus connu d'internet. Il est extrêmement décentralisé – on pourrait même dire qu'il n'est pas un « système » mais plutôt une série de protocoles grâce auxquels des réseaux d'ordinateurs indépendants peuvent s'envoyer des données. C'est lui qui nourrit l'image d'internet dans le grand public et les prétentions à l'« ingouvernabilité » (Froomkin, 1997).

Le système d'adressage – le DNS – est au contraire centralisé. Presque toutes les communications sur internet en dépendent. On peut concevoir le DNS comme l'annuaire et les renseignements téléphoniques d'internet. Avant qu'un ordinateur puisse communiquer avec un autre, il doit composer l'équivalent du « 12 », donner le nom de celui qu'il appelle, puis attendre la composition du numéro. C'est un préalable indispensable à la communication.

Chaque fois qu'un utilisateur clique sur un lien de page web ou envoie un e-mail qui comporte un nom de domaine, le DNS doit *résoudre* ce nom de domaine. Du point de vue de sa structure interne, le DNS consiste en une base de données et un service de recherche dynamique. Les entrées dans la base de données comprennent un identifiant alphanumérique convivial (le *nom de domaine*) et un identifiant numérique pour la machine (le numéro ou adresse *IP*, Internet Protocol). Ainsi, le nom de domaine d'un ordinateur serait *monordinateur.org*, et son numéro IP correspondant *12.34.56.78*. Le DNS reconnaît le nom de domaine et forme le numéro correspondant. Les ordinateurs qui effectuent cette opération s'appellent des *name servers* (serveurs de noms). Une fois celle-ci effectuée, la correspondance par courrier électronique ou la communication sur le web peuvent s'engager[2].

Ce processus à deux étapes est immédiatement perceptible avec la plupart des navigateurs (comme Netscape). Une fois que l'utilisateur a tapé

2. Cette explication simplifie un peu les choses. De fait, si l'on utilise les numéros IP directement, on n'a plus besoin d'interagir avec le DNS pour communiquer *via* internet. Note au lecteur : selon mon expérience, à toute affirmation concernant le DNS on peut trouver une exception. Merci d'en tenir compte en lisant cette partie de l'article, simplificatrice à l'extrême par souci de clarté.

le nom du domaine, le navigateur indique qu'il est en correspondance avec le DNS avec un message du genre : « Recherche de l'hôte... » Plusieurs secondes peuvent s'écouler avant que la résolution soit effectuée et que la communication entre ordinateurs puisse commencer. Parfois la résolution du nom échoue, comme par exemple quand une faute de frappe ou d'orthographe donne un message du genre « Impossible de trouver l'hôte... », et aucun numéro ne répond. En regardant les messages sur l'écran du navigateur, un utilisateur peut observer le processus de résolution du nom.

Au cœur du DNS se situe l'*espace de nommage* d'internet. Celui-ci fournit une liste de (presque) tous les ordinateurs connectés à internet[3]. A ce jour, l'espace de nommage contient des dizaines de millions d'entrées. Dans les statistiques sur la croissance d'internet, les chiffres se réfèrent en général à l'étendue de l'espace de nommage, qui fournit une approximation du nombre d'utilisateurs individuels : puisque la plupart des ordinateurs qui figurent sur la liste du DNS sont des portails d'accès aux réseaux privés connectant un grand nombre d'utilisateurs individuels, le nombre d'utilisateurs est bien plus élevé que celui des entrées dans l'espace de nommage.

En d'autres termes, l'espace de nommage *est* internet. Pour exister sur internet, un ordinateur doit figurer sur la liste de l'espace de nommage. A défaut (donc sans nom de domaine et sans numéro IP), un ordinateur ne pourra pas être trouvé par d'autres. Enlever un ordinateur du listing de l'espace de nommage, c'est comme le bannir d'internet, car l'ordinateur disparaît de la liste des ordinateurs adressables. Quelle que soit l'entité qui contrôle l'espace de nommage, elle contrôle aussi effectivement internet. On reverra cela en détail plus loin.

Dans sa conception actuelle, l'espace de nommage doit se conformer à certains principes (IAB, 2000 ; ICANN, 2001). Les concepteurs du système prétendent que l'espace de nommage doit être *unique* et géré par une seule entité. Il ne peut exister qu'une seule base de données qui constitue le listing définitif des ordinateurs sur internet. Il peut y avoir des copies, mais non pas des espaces de nommage indépendants : si c'était le cas, tout nom de

3. C'est peut-être trop dire. Certains ordinateurs figurent sur la liste plusieurs fois. D'autres n'y figurent peut-être pas du tout et ne peuvent être contactés qu'en tapant l'adresse IP directement. Dans la majorité des cas, pourtant, un ordinateur sur internet = une entrée dans l'*espace de nommage* du DNS. Or, comme on le verra plus loin, la plupart des ordinateurs présents dans le DNS ne sont pas des ordinateurs individuels mais des portails d'accès aux réseaux privés au sein desquels existent des comptes d'utilisateurs individuels.

domaine pourrait correspondre à des adresses IP différentes selon l'espace de nommage utilisé, ce qui ôterait toute fiabilité à la communication. Cet impératif technologique du caractère unique sous-tend la centralité du DNS, car toute communication utilise un espace de nommage unique et obligatoire. Le recours, sur internet, à un espace de nommage unique (avec un administrateur unique) « *... est une nécessité technique, et non un choix politique* » (IAB, 2000). (Si cette caractéristique n'était pas impérative, l'éventail des choix politiques serait largement ouvert.)

L'administration

Le DNS est plus qu'un système technique : c'est aussi un système administratif et politique. Poursuivant notre présentation simplifiée du DNS comme base de données unique et non distribuée, on peut l'examiner sous l'angle de l'administrateur unique et de l'autorité politique exclusive. L'entité d'*autorité politique* formule des règles générales pour tout changement apporté à l'espace de nommage, décidant, par exemple, des noms de domaine admissibles, du coût d'enregistrement dans l'espace de nommage et des restrictions sur l'ajout ou la suppression de noms. L'*administrateur* met en œuvre ces décisions, en ajoutant, supprimant, ou modifiant les entrées dans la base de données pour refléter l'entrée, la sortie ou le changement de statut de divers ordinateurs. L'administrateur garantit également la fiabilité du serveur de noms.

L'obligation du caractère unique du DNS implique que l'autorité politique et l'administrateur exercent un pouvoir de type monopolistique. Il y a impérativement un espace de nommage unique, géré par un administrateur unique qui, à son tour, est sujet à l'autorité politique unique. « *La conception comme le fonctionnement du protocole du DNS sont puissamment conditionnés par l'existence d'un propriétaire ou administrateur unique...* » (IAB, 2000). La fiabilité du fonctionnement de l'espace de nommage est à ce prix. Directement ou indirectement, cet administrateur unique du DNS passe un contrat avec tout réseau connecté à internet. Ainsi, la centralisation administrative et politique va de pair avec la centralisation technique du DNS.

L'administrateur du DNS s'appelle aussi un *registry*. Pour qu'un ordinateur soit disponible sur internet, l'utilisateur doit demander à l'administrateur d'être *enregistré*. Le registry enregistre l'ordinateur en ajoutant le couple nom-numéro de l'utilisateur à l'espace de nommage.

Le mécanisme légal qui relie l'autorité politique centrale aux utilisateurs est un *contrat*. Internet est un réseau de réseaux : la plupart des ordinateurs

enregistrés dans l'espace de nommage sont en fait des portails d'accès à des réseaux privés, gérés à leur tour par des administrateurs de réseau. Chaque entrée dans le DNS s'accompagne d'un contrat entre l'administrateur central du DNS et un *administrateur de réseau*. Ce contrat précise les règles et conditions pour l'inclusion dans l'espace de nommage, c'est-à-dire la fourniture des coordonnées de contact, le règlement d'une cotisation annuelle, la reconnaissance du rôle de l'administrateur du DNS, etc. Ainsi, tout réseau d'internet passe un contrat avec l'entité unique qui supervise le DNS.

Le DNS et la gouvernance d'internet

A partir de cette vision simplifiée du DNS, on voit comment la gouvernance est envisageable. Il suffirait de quelques modifications mineures pour mettre en œuvre les quatre mécanismes de l'autorité, de la loi, des sanctions et de la juridiction.

Le DNS instaure une autorité centrale pour internet. L'obligation du caractère unique de l'espace de nommage exige une autorité centrale unique dont les décisions s'appliquent à tous les serveurs dans l'espace de nommage. Pour faire de l'autorité politique du DNS une vraie entité régulatrice, il faudrait simplement que son champ de décision s'étende aux enjeux de politique publique, tels que la réglementation de la propriété intellectuelle ou le contrôle du contenu. Puisqu'il y a très peu de barrières techniques à une telle expansion, il s'agirait bien alors d'un choix politique. L'exercice de la gouvernance sur internet exigerait donc simplement d'élargir la gamme des sujets régulés par l'autorité politique du DNS.

Le DNS définit également le deuxième mécanisme de gouvernance : la loi. La loi d'internet s'exprime dans les contrats pour l'enregistrement des noms de domaine. Les contrats avec les administrateurs de réseaux détaillent les règles à respecter. Pour réguler de plus vastes questions, il suffirait d'élargir la formulation des contrats.

Troisièmement, le DNS intègre un puissant mécanisme de sanctions : le refus d'un nom de domaine (par exemple, suppression du couple nom-numéro d'un utilisateur du listing de l'espace de nommage). C'est le pouvoir de bannir : les administrateurs de réseaux refusant de se conformer aux règles précisées dans leurs contrats pourraient être éliminés de l'espace de nommage et contraints à la disparition informatique. L'enregistrement des noms est donc conçu comme un privilège, révocable en cas de transgression.

Le DNS résout tout aussi nettement le problème de la juridiction. La juridiction de l'autorité politique du DNS s'étend à tout ordinateur relié à internet, mais ne va pas plus loin. C'est le contrat d'enregistrement qui manifeste la juridiction. Tout administrateur de réseau est lié contractuellement à l'autorité politique du DNS.

C'est ainsi que le système de noms de domaines fournit les moyens de la gouvernance. Il suffirait de quelques changements mineurs pour conforter chaque mécanisme. L'autorité politique du DNS n'aurait qu'à élargir son champ de régulation pour inclure des réglementations plus larges dans les contrats signés avec les administrateurs de réseau. Le refus d'un nom de domaine fournit un mécanisme suffisant pour sanctionner ceux qui ne se conforment pas aux règles. Et la juridiction de l'autorité politique s'appliquerait exactement à internet, ni plus ni moins.

Mais pour assurer plus complètement la gouvernance d'internet il faut considérer deux problèmes supplémentaires. Le premier est pratique : il faudrait trouver le moyen d'étendre l'autorité politique jusqu'à l'utilisateur individuel. Le contrat d'enregistrement du nom de domaine étant convenu entre l'autorité centrale et un administrateur de réseau, les utilisateurs individuels ne sont pas directement soumis à ces régulations. La régulation des utilisateurs individuels impliquerait un *contrat aval*. Les administrateurs de réseau demandent en général aux utilisateurs de signer un accord lorsqu'ils prennent un compte, et cet accord avec l'utilisateur pourrait reprendre les termes du contrat des administrateurs. Ainsi une seule série de règles irriguerait tous les niveaux, de l'administrateur central du DNS aux administrateurs de réseaux locaux et, dès lors, à tout utilisateur. De façon indirecte, tous les utilisateurs d'internet se verraient alors régulés par l'administrateur central du DNS. Toute violation du contrat par l'utilisateur pourrait faire interdire d'accès son compte. Et les administrateurs de réseau qui ne réussiraient pas à imposer des contrats « aval » avec leurs utilisateurs se verraient soumis au refus du nom de domaine, c'est-à-dire au bannissement d'internet. Bien qu'un tel contrat reste aujourd'hui théorique, il est néanmoins tout à fait envisageable. Dans un paragraphe ultérieur, je résumerai les types de régulation qui ont été ou qui pourraient être instaurés au moyen d'un tel système.

Une deuxième considération à propos de la gouvernance est de nature plus normative. Si l'autorité politique du DNS devenait un régulateur à visée générale, il faudrait alors repenser fortement sa *légitimité*. Avec l'extension de sa capacité décisionnelle, son autorité devrait se fonder sur un principe de compétence. Ce serait le cas si l'on plaçait l'autorité politique ultime entre les mains des gouvernements ou d'une institution

représentative constituée à cet effet. Comme on le verra plus loin, quand l'autorité politique fut confiée à ICANN, celle-ci adopta un processus représentatif pour assurer sa légitimité.

Jusqu'ici, j'ai développé une hypothèse simplificatrice : l'espace de nommage d'internet se compose d'une seule base de données centralisée. Au tout début du développement d'internet, c'était le cas. Dans les années 1970, l'espace de nommage tout entier se trouvait dans un seul fichier appelé « hosts.txt » (Froomkin, 2000). A partir de 1983, pourtant, la croissance continue du réseau conduisit les chercheurs à reconceptualiser l'espace de nommage et à le fragmenter en pièces multiples et interconnectées. L'espace de nommage est moins centralisé que je ne l'ai représenté jusqu'ici, et cette décentralisation rend bien plus complexe la gouvernance d'internet. Je vais maintenant procéder à l'analyse de cette architecture complexe.

Le DNS comme système distribué

L'espace de nommage est une base de données *distribuée*. Théoriquement toutes les paires nom-numéro pourraient être incluses dans une seule base de données centrale, comme décrit plus haut. Mais, puisqu'à chaque seconde ont lieu des milliers de requêtes de noms, un ordinateur centralisé en charge du DNS serait facilement débordé. L'espace de nommage est donc distribué entre de multiples ordinateurs pour partager la tâche.

L'espace de nommage consiste en une collection de bases de données partielles, séparées les unes des autres, tournant sur des ordinateurs distincts. Chaque base de données partielle s'appelle un *fichier-zone* (ou « zone »). Une zone comprend un sous-ensemble de la liste générale de paires nom-numéro. A chaque zone est associé un *serveur de noms* (ou « serveur » – un logiciel pour la résolution des noms) et un *ordinateur hôte* (ou « hôte » – le matériel où se logent le dossier de zone et le serveur de noms). Ainsi l'espace de nommage tout entier est un système distribué de bases de données et de résolution de noms dont la pierre angulaire est la triade fichier-zone/logiciel du serveur de noms/ordinateur-hôte.

Comme pour toute base de données distribuée, le rapport entre les membres est soigneusement structuré. Les diverses zones sont *liées* entre elles pour former une hiérarchie pyramidale inversée ou un arbre à l'envers (avec les racines en haut). Au sommet de la hiérarchie se trouve une zone unique, la *racine*. Cette zone-racine et reliée à de multiples zones situées juste en-dessous, reliées à leur tour à de nombreuses autres zones inférieures, etc. (C'est la même structure qu'on retrouve pour les dossiers d'un ordinateur

personnel.) Les strates de la hiérarchie sont faciles à identifier : la zone-racine est liée aux zones « haut niveau », qui sont reliées à leur tour à des zones de « deuxième niveau », viennent ensuite les zones de « troisième niveau », etc.

Bien qu'une zone donnée puisse être reliée vers le bas à de multiples zones, elle ne peut l'être vers le haut qu'à une seule. De façon directe ou indirecte, toutes les zones sont reliées vers le haut à la zone-racine unique. L'existence d'une racine unique dans l'espace de nommage satisfait à l'obligation d'unicité.

Les sous-arbres dans ce système s'appellent des *domaines*. Un domaine est constitué d'une zone et de toutes les zones inférieures. On parle souvent des noms de domaine selon leur niveau dans l'arbre. Ceux qui relèvent des zones de haut niveau s'appellent « domaines de haut niveau » (*top-level domains*, ou TLDs) ; ceux qui relèvent du niveau suivant sont des « domaines de deuxième niveau », etc. Le domaine de la racine est l'espace de nommage global. L'ensemble du système constitue le « système des noms de domaines » ou DNS. Les termes « zone » et « domaine » sont souvent employés de façon interchangeable, mais la « zone » se réfère à un seul fichier et le « domaine » à ce même fichier et tout autre fichier inférieur à lui dans son sous-arbre.

Un domaine possède un nom – qui, sans surprise, s'appelle un *nom de domaine*. Les noms de domaine de haut niveau les plus connus sont *.com*, *.org*, et *.net*. Le domaine le plus vaste dans l'espace de nommage, *.com*, est relié à des millions de domaines d'échelon inférieur. Une adresse internet comme *monordinateur.com* associe un domaine de deuxième niveau (*monordinateur*) à un domaine du premier échelon (*.com*). Une série de noms de domaine, où les niveaux sont séparés par des points, identifie de manière précise et unique tout ordinateur dans l'espace de nommage.

Cette hiérarchie distribuée définit les rapports de contrôle de haut en bas. N'importe quel fichier-zone peut être modifié pour lier (inclure) ou délier (exclure) les zones situées plus bas que lui dans l'espace de nommage. Comme un pouvoir de vie ou de mort virtuelle... Quand un serveur de noms se connecte à la racine à travers une série de liens, il existe dans l'espace de nommage. Si l'on modifie un fichier-zone pour éliminer un lien, le ou les ordinateurs inférieurs à lui dans la hiérarchie seront exclus de l'espace de nommage. Chaque serveur situé dans la hiérarchie contrôle la route jusqu'à la racine pour les serveurs de niveau inférieur.

On peut illustrer ce processus par un exemple. Disons que je voudrais connecter ma société au courrier électronique par internet. Je possède déjà

un réseau interne, et maintenant je cherche à relier mon réseau à internet. Pour ce faire, il faut d'abord que je connecte un ordinateur-hôte de mon réseau à l'espace de nommage, *i.e.* que j'enregistre le nom de domaine et l'adresse IP de l'hôte dans un fichier-zone du DNS. L'espace de nommage étant une base de données distribuée, il existe plusieurs fichiers-zones auxquels je pourrais me lier : un registry en Virginie gère un fichier-zone qui s'appelle *.com*, un autre en Angleterre en gère un qui s'appelle *.uk*, ma maison-mère en gère un qui s'appelle *.holdingcompany* (qui, à son tour, est relié au fichier-zone *.com*). Quand j'enregistre mon hôte dans un fichier-zone disponible, il est intégré à l'espace de nommage et commence à exister sur internet. Parallèlement, si mon entrée dans le fichier-zone se trouvait déliée (si le nom de domaine était annulé), mon hôte disparaîtrait d'internet. La modification du fichier-zone qui me permet d'entrer ou de sortir d'internet ne dépend pas de moi mais de l'administrateur du fichier-zone immédiatement supérieur au mien, dont je dépends toujours pour être présent sur internet.

L'administration

Dans une approche simplifiée, j'ai écrit que l'administration et l'autorité politique du DNS reposent sur un couple unique d'organisations. Dans le DNS distribué, *tout* domaine doit avoir une telle paire administration-politique (j'en parlerai simplement comme « administrateur » ; dans certains cas, les deux peuvent relever de la même organisation). Ces organisations fonctionnent selon la structure distribuée de l'espace de nommage : l'administration globale du DNS est une hiérarchie multi-organisations, dans laquelle chaque administrateur exerce son contrôle sur les administrateurs des échelons inférieurs. Au sommet se trouve l'administrateur de la racine.

Chaque administrateur exerce un contrôle monopolistique sur son fichier-zone immédiat (qui lui assure l'exclusivité de sa portion de l'espace de nommage). D'ailleurs, tout administrateur exerce son autorité sur l'intégralité du niveau inférieur. Quand il enregistre un hôte de deuxième ou de troisième niveau, il *délègue* de l'autorité à un administrateur de niveau inférieur, qui à son tour exerce le contrôle monopolistique sur ce fichier-zone inférieur. L'autorité tombe en cascade depuis l'administrateur de la zone-racine, responsable pour tout l'espace de nommage, jusqu'aux ordinateurs-hôtes individuels des zones inférieures. Chaque administrateur est soumis aux politiques des entités supérieures. C'est ainsi que des politiques décidées à la racine peuvent être transmises à toute la hiérarchie pour s'appliquer, directement ou indirectement, à tous les administrateurs du

DNS. En tant que groupe, les administrateurs sont les gardiens de l'espace de nommage et donc d'internet.

Tout comme les fichiers-zone sont entrelacés, les administrateurs sont liés par des contrats. L'administrateur-racine formalise sa délégation d'autorité aux administrateurs inférieurs par un contrat, dont plusieurs articles peuvent devenir obligatoires dans les contrats subséquents. De cette manière, les règles peuvent circuler dans toute la hiérarchie jusqu'à l'administrateur de réseau individuel, ou même à l'utilisateur individuel, comme on l'a déjà vu.

On ne s'étonnera pas de ce que l'administration de la zone-racine soit d'une importance toute particulière. Tous les autres hôtes sur internet n'accèdent à l'espace de nommage que par une délégation d'autorité qui provient directement ou indirectement de la racine. L'autorité politique sur la racine – le pouvoir d'ajouter ou de supprimer les domaines de haut niveau – confère un contrôle direct sur tout domaine de haut niveau et un pouvoir indirect sur tout domaine de niveau inférieur. L'exercice de l'autorité sur la zone-racine s'étend à internet tout entier.

Pour résumer, cette approche plus précise du DNS révèle une complexité technique et administrative de grande ampleur. Considéré dans son ensemble, le DNS est bien un point de contrôle centralisé d'internet. Et pourtant, puisqu'il est un système décentralisé, le DNS possède une structure interne qui compte sur le contrôle hiérarchique et les contrats pour rendre effectif son potentiel d'action politique unificatrice.

Les facteurs historiques du DNS

On peut maintenant passer de l'analyse technique à une analyse historique. Notre propos a jusqu'à présent dessiné le fonctionnement du DNS et de sa structure en tant que base de données distribuée. L'analyse historique mettra en lumière l'évolution de l'espace de nommage du DNS et de sa hiérarchie administrative.

Internet a vu le jour comme projet de recherche dans les années 1970, et les scientifiques du monde de l'informatique qui l'ont développé ont formaté l'évolution de ses institutions administratives et politiques (Hafner et Lyon, 1998). Cette communauté de chercheurs a trouvé son assise dans des institutions comme l'Internet Engineering Task Force (IETF), l'Internet Architecture Board (IAB), l'Institut des sciences informatiques de l'Université de la Californie du Sud (ISI) et l'Internet Society (ISOC) (Leiner *et al.*, 2000).

Une personne en particulier a joué un rôle-clé dans le développement du DNS : le Dr. Jon Postel, informaticien à l'Université de Californie du Sud. Bénéficiant d'une bourse de recherche gouvernementale, Postel a exercé l'autorité politique sur la racine, dans le cadre de l'Internet Assigned Number Authority (IANA). A la tête d'IANA, Postel gérait le fichier-zone de la racine, autorisait l'ajout de nouveaux TLD (domaines de haut niveau), sélectionnait les administrateurs auxquels déléguer l'autorité et il accomplit d'innombrables autres tâches. Postel avait d'abord assumé ce rôle dans les années 1970 en tant qu'étudiant. A proportion de la croissance d'internet, l'importance des décisions de Postel crût jusqu'aux années 1990, où elles eurent des implications mondiales. Cependant l'autorité politique sur la racine reposait toujours sur sa personne. Et, puisqu'il travaillait sous contrat avec le gouvernement, l'autorité finale demeurait officiellement entre les mains du gouvernement des Etats-Unis – mais, la plupart du temps dans les années 1980 et 1990 c'est Postel qui a exercé son autorité personnelle sur le DNS.

En 1984, dans un document connu sous le sigle RFC920, Postel, avec son collègue Joyce Reynolds, définit la trajectoire d'évolution de l'espace de nommage (Postel et Reynolds, 1984). RFC920 établit le nombre de zones de haut niveau et leurs noms. Bien que l'espace de nommage se limite à un seul fichier-zone de racine, Postel et Reynolds annoncent en 1984 que l'échelon supérieur consistera en quelque 250 fichiers-zone. RFC920 sert de canevas pour structurer l'espace de nommage et sa croissance future. Le nombre de fichiers-zones ne se fonde sur aucune nécessité technique, il aurait pu être plus grand ou plus petit.

RFC920 précise également les chaînes numériques d'identification des fichiers-zone. Les 250 TLD se divisent en deux classes de nommage : six TLD « génériques » (des « gTLD » : *.gov*, *.edu*, *.com*, *.org*, *.mil*, et *.net*), et 244 TLD codes-pays (des « ccTLD », ayant pour base la liste de référence ISO 3166-1 des codes-pays à deux chiffres, tels *.uk* pour le Royaume Uni, *.fr* pour la France, *.jp* pour le Japon, etc.). Encore une fois, les chaînes numériques particulières utilisées dans les noms de domaine n'ont aucune signification technique ; il suffit qu'elles soient uniques. Elles ont néanmoins une grande incidence politique, car elles donnent forme à des décisions concernant l'utilisation d'internet. Les 250 TLD définissent un espace de nommage fondé en partie sur des fonctions (*.com* pour *commercial*, *.mil* pour *militaire*, etc.) et en partie sur des identifiants géopolitiques (noms de pays). Décidés bien avant qu'internet n'acquière une importance mondiale, le nombre de TLD et la signification y attachée vont avoir des conséquences à long terme.

RFC920 définit la structure et les conventions de nommage du DNS et sa mise en œuvre s'étale sur plusieurs années. L'instauration des TLD exige la sélection d'un administrateur pour gérer le fichier-zone et le serveur des noms. L'instauration des TLD génériques procède de façon très différente de celle des TLD de codes-pays : les premiers sont sélectionnés par le gouvernement des Etats-Unis, les seconds choisis par IANA.

Postel et IANA possèdent l'autorité politique sur la racine, mais l'administrateur est une entreprise privée : Network Solutions, Inc. (NSI), qui administre et exerce l'autorité politique sur *.com*, *.net*, et *.org*. NSI prend ses ordres d'IANA, mais travaille en réalité sous contrat avec le gouvernement des Etats-Unis.

La croissance du domaine *.com* procure à NSI richesse et puissance. Lorsque le gouvernement des Etats-Unis ouvre internet aux usages commerciaux, en 1994, l'enregistrement en *.com* explose. A la fin des années 1990, *.com* atteint plus de dix millions d'enregistrements – plus de la moitié de tout l'espace de nommage. Cette concentration ne relève pas d'un caractère inné du DNS, mais provient d'un développement inattendu – la combinaison du bon marketing de NSI et de la large acceptation de la convention de nommage du DNS, qui identifie *.com* comme LE domaine commercial. Au bout du compte, le domaine *.com* représente une telle proportion de l'espace de nommage total qu'il rivalise d'importance avec la racine pour l'ensemble du réseau (Mueller, 1999). Des frais annuels de $35 USD (environ 190FF ou 40 €) par nom de domaine enregistré permettent à NSI d'amasser des centaines de millions de dollars de revenus du fait de son monopole sur le seul domaine commercial d'internet.

En revanche, les administrateurs de TLD de codes-pays sont majoritairement, tout comme IANA, des sociétés sans but lucratif, souvent affiliées aux centres de recherches universitaires. Parce qu'IANA a défini les fichiers-zone en termes de codes-pays et créé un seul fichier-zone par pays, il n'y a qu'un seul administrateur par pays. Chacun d'eux constitue un monopole national implicite : le registre *.fr* est le seul pour la France, de même *.uk* pour le Royaume-Uni, etc. Même s'il n'y a aucune base technique pour les monopoles nationaux, la convention de nommage de RFC920 génère un tel système. En termes d'organisation, le système des monopoles nationaux ccTLD rappelle celui des sociétés nationales de téléphone (les PTT), qui opéraient en tant que monopoles nationaux dans la plupart des pays.

En octobre 2000, l'espace de nommage global compte plus de 30 millions de paires nom-numéro (NetNames, 2000). Vu qu'IANA n'a pas étendu le

nombre de domaines de haut niveau depuis la sortie de RFC920, ce sont les domaines de deuxième niveau qui ont connu la plus forte croissance. La majorité relève du TLD, *.com*, où NSI a enregistré plus de 18 millions d'hôtes. Les TLD en *.org* et de *.net*, également gérés par NSI, abritent 5 millions d'hôtes supplémentaires. Le reste de l'espace de nommage se distribue pour l'essentiel en divers TLD de codes-pays. A la tête d'IANA, Jon Postel supervise la délégation d'autorité aux nouveaux administrateurs.

Le DNS de la fin des années 1990 est encore bien plus complexe que le système décrit ici. D'abord, il est décentralisé. En 1983 le DNS a été créé comme une base de données distribuée (Mockapetris, 1983). Puis, au fil des ans, de nombreux développements non techniques ont formaté le système. La majorité des TLD portent des identificateurs de codes-pays, qui les associent aux gouvernements nationaux. Un fichier-zone dans la hiérarchie *.com*, contient presque tout l'espace de nommage (battant ainsi en brèche la décentralisation). Dans une communauté de petits administrateurs à but non lucratif, Network Solutions commence à émerger comme un géant du commerce. Et surtout, l'autorité politique sur l'ensemble du DNS est concentrée sur une seule personne, Jon Postel. La complexité du DNS est lourde de conflits potentiels.

DNS et gouvernance

Cependant le DNS peut toujours permettre d'exercer les mécanismes de la gouvernance. Bien que des accords plus complexes que ceux qu'on a mentionnés soient nécessaires, un DNS décentralisé rend possibles l'autorité, la loi, les sanctions, et les juridictions. Dans cette section, je discuterai de quelle manière la technologie du DNS rend théoriquement possible la gouvernance.

La décentralisation n'a pas d'effet majeur sur la mise en œuvre de deux mécanismes : la loi et les sanctions. Même si elle engendre de multiples niveaux hiérarchiques, les contrats-aval acheminent néanmoins les règles jusqu'aux utilisateurs. La décentralisation exige une succession de contrats en cascade, mais elle ne remet pas en cause ce mécanisme. De même, le refus (d'accès) à un nom de domaine est une sanction efficace. Si tout administrateur dans l'espace de nommage, de la racine à l'étage le plus bas, exerce un contrôle monopolistique sur son fichier-zone, chacun peut déconnecter des hôtes de niveau inférieur. Ainsi l'enregistrement d'un nom reste un privilège, révocable si l'enregistreur viole les règles.

Au contraire, la décentralisation entrave l'exercice des deux autres mécanismes de gouvernance. Elle fragmente l'autorité politique et la

juridiction, surtout dans les domaines de codes-pays. Celles-ci restent unifiées à la racine : IANA peut réglementer tout l'espace de nommage et promulguer les règles à travers toute la hiérarchie. Mais dans les domaines de haut niveau (TLD), le risque existe d'une contradiction avec un autre échelon d'autorité. La distinction entre les TLD génériques (gTLD) et ceux des codes-pays (ccTLD) peut affaiblir l'unité d'autorité et de juridiction.

Les ccTLD sont associés aux pays, et par conséquent à l'autorité politique des gouvernements nationaux. Ceux-ci peuvent prétendre à exercer leur juridiction sur les ccTLD correspondants. Même si les domaines des gouvernements nationaux représentent un niveau inférieur à IANA dans la hiérarchie du DNS, IANA n'est pas en situation de revendiquer sur eux une quelconque autorité. L'institution de gouvernance d'internet serait bien en peine de remettre en question le droit d'un gouvernement national à décider de sa politique publique. Même si les gouvernements ignorent le DNS (dans la majorité des cas), l'exercice proactif de l'autorité politique par IANA peut provoquer une réaction de leur part. Aussi est-il difficile pour l'autorité politique sur la racine d'affirmer son pouvoir sur les ccTLD.

Autre source de complexité : la pléthore d'autorités au sein des ccTLD. Les TLD de codes-pays sont indépendants les uns des autres, et chacun peut décider de ses propres politiques dans son domaine, source de possibles divergences, voire de contradictions. La décentralisation du DNS a créé des centaines d'autorités, dont chacune peut implicitement prétendre à la juridiction sur son ccTLD. La gouvernance intégrée d'internet apparaît donc impossible. La décision des ingénieurs informatiques d'organiser l'espace de nommage d'après les grandes lignes politiques dont témoigne RFC920 a fragmenté l'autorité et la juridiction.

Une gouvernance intégrée paraît possible, au contraire, dans les gTLD. IANA peut réguler les domaines tels que *.com*, *.org*, et *.net*, car ceux-ci ne sont pas redevables vis-à-vis d'autorités extérieures au DNS. Quelle que soit l'autorité dont ils disposent, ils ne la détiennent que par délégation d'IANA. Or, les gTLD ont beau n'être qu'un sous-ensemble du total des domaines, ils se taillent néanmoins la part du lion en nombre d'utilisateurs. L'autorité effective dans ces domaines s'étend de fait à la majorité des internautes.

Le DNS ne permet pas une gouvernance pleine et entière, mais autorise un certain degré de gouvernance. L'exercice d'une autorité et d'une juridiction uniques dans les domaines en *.com*, *.org* et *.net* est aisé. D'ailleurs, vue la grande concentration d'enregistrements dans les gTLD, cette juridiction concerne également la plus grande part des utilisateurs. L'autorité politique de la racine peut les réguler *via* les contrats-aval assortis

de la menace du refus d'accès au nom de domaine. La fragmentation de l'autorité demeure, mais elle est limitée.

Pour la limiter davantage, IANA, tout comme les gouvernements nationaux cherchent à coordonner les diverses politiques. Bien qu'il y ait des centaines de ccTLD, les enregistrements ne sont pas également répartis. Des domaines tels que *.jp* ou *.uk* comptent beaucoup plus d'enregistrements que d'autres, par exemple *.bg* (la Bulgarie). La coordination des ccTLD les plus importants avec IANA suffit à unifier les politiques, pour s'approcher d'une gouvernance intégrée.

Enfin, l'on peut revendiquer d'autant plus de cohésion politique que l'on a la possibilité de mettre la pression sur des ccTLD récalcitrants. Si un petit ccTLD hésite à appliquer quelque politique soutenue par IANA et par les grands gouvernements, son autorité peut être remise en cause. IANA peut exercer sa capacité de déconnecter un domaine de haut niveau ou de le réaffecter vers un administrateur plus conciliant. Ainsi les plus petits ccTLD peuvent se laisser persuader (ou intimider) d'adopter les politiques agréées par les plus grands. La cohésion politique générale ne peut qu'y gagner.

Avant de clore ce chapitre, il faut encore considérer le rôle du gouvernement des Etats-Unis. Ce dernier, grâce à Jon Postel et Network Solutions, revendique l'autorité finale sur le fichier-zone racine. IANA, autorité politique supérieure aux Etats-Unis, fonctionne sous l'autorité politique des Etats-Unis. Instaurer les quatre mécanismes de gouvernance, en l'absence d'un changement de statut des Etats-Unis, serait en quelque sorte permettre à ce pays d'exercer l'autorité ultime sur internet. Nouvelle cause de tensions avec les autres gouvernements nationaux qui se trouveraient subordonnés aux Etats-Unis.

Pour résumer, un DNS décentralisé ne peut permettre la réalisation pleine et entière des mécanismes de gouvernance. La loi et les sanctions peuvent s'appliquer, mais l'autorité et la juridiction sont fragmentées. La majorité des utilisateurs se situant dans des domaines génériques (les gTLD) peuvent être régulés par IANA. Mais soumettre l'espace de nommage tout entier à l'autorité d'IANA exigerait des négociations avec un nombre considérable d'autorités nationales autonomes.

D'IANA à ICANN

Ayant passé le DNS en revue, on peut se tourner désormais vers l'Internet Corporation for Assigned Names and Numbers (ICANN). Créée en 1998, et quoique non stabilisée à ce jour, ICANN met en œuvre le

potentiel de gouvernance du DNS, en se servant de l'adressage sur internet comme d'un levier pour accomplir la gouvernance globale. ICANN n'a pas seulement créé des capacités de régulation, elle les a aussi utilisées : en 1999, elle a promulgué une décision de politique publique mondiale qui définit les droits de propriété intellectuelle sur les noms de domaine. Je vais ici identifier les caractéristiques spécifiques d'ICANN aux moyens desquelles elle met en pratique l'autorité, la juridiction, la loi et les sanctions.

Commençons par planter le décor historique. A la fin des années 1990, le DNS est contesté de diverses parts. Internet a rapidement débordé ses institutions d'origine, notamment la « personnalisation » d'IANA, dont la légitimité se fondait sur la réputation d'un seul homme. Si quelque malheur arrivait à Jon Postel, IANA serait complètement déstabilisée. Une autre source de tension provient des entreprises qui, au nom de la concurrence, veulent ébranler le monopole de NSI : elles commencent à proposer d'autres espaces de nommage, d'autres TLD (par exemple *.web*), et des « registries » indépendants (Mueller, 1998). Ce qui fait peser de nouvelles menaces de fragmentation sur l'espace de nommage. La nature globale d'IANA pose un autre problème. L'Union internationale des télécommunications (ITU) de l'Organisation des Nations unies s'en mêle et cherche à revendiquer l'autorité sur l'espace de nommage. Des gouvernements nationaux et la Commission européenne s'y intéressent eux aussi, estimant que le contrôle exercé par les Etats-Unis sur cette nouvelle infrastructure informatique mondiale menace leur souveraineté. Des controverses naissent sur les questions de souveraineté et de juridiction. Des conflits sérieux émergent autour des noms de domaines correspondant aux marques déposées (par exemple, *coca-cola.com*). L'organisation mondiale de la propriété intellectuelle (WIPO) de l'ONU, ainsi que des lobbies nord-américains font pression pour faire respecter le droit des marques déposées dans l'univers des noms de domaine (Shaw, 1997). Ce mélange politique est d'autant plus détonnant que les conflits se développent au rythme d'internet ; chaque mois qui passe témoigne de la croissance exponentielle du réseau et de ses enjeux politiques.

Le processus par lequel la communauté des chercheurs, les titulaires de marques déposées, les entreprises de communication et les gouvernements nationaux se sont concertés pour créer une nouvelle institution à la place d'IANA a été décrit ailleurs (Mueller, 1999 ; Klein, 2001a). Je concentrerai mon attention sur le fruit de ce processus long et litigieux, c'est-à-dire ICANN, en l'analysant sous sa configuration de l'an 2000.

On comprend mieux ICANN si on la perçoit comme un ensemble d'institutions semi-autonomes. Cet ensemble comprend non seulement

ICANN en tant que société mais aussi certaines entités externes, telles que le comité des gouvernements nationaux (GAC) et les administrateurs des TLD. Pour bien distinguer entre ICANN vue comme un ensemble d'institutions et ICANN vue comme entité institutionnelle, j'appellerai celle-là « le système ICANN » et celle-ci simplement « ICANN ».

Les quatre mécanismes de gouvernance sont si profondément enracinés dans le système administratif d'ICANN qu'il est difficile de les identifier. Le paragraphe qui suit va analyser les caractéristiques d'ICANN dans leurs fonctionnalités relatives à la gouvernance. Je m'intéresserai tout d'abord à la façon dont ICANN a mis en œuvre les mécanismes d'autorité et de juridiction, puis je me concentrerai sur les mécanismes de la politique et des sanctions.

L'autorité et la juridiction

L'autorité politique sur la racine est transférée de Jon Postel à la nouvelle instance. ICANN résout le problème de la stabilité : une personne est remplacée par une institution, ICANN peut fonctionner indépendamment d'un seul individu. ICANN résout aussi, au moins en partie, le problème du conflit intergouvernemental : en tant que société privée, elle stipule dans son règlement intérieur qu'aucun fonctionnaire ne peut être membre de son conseil d'administration. Ainsi, même si son autorité s'étend au monde entier, la nature de celle-ci est délibérément non gouvernementale et respecte ainsi la souveraineté des gouvernements nationaux. En outre, son rôle étant simplement d'assurer la coordination technique de l'internet, ICANN ne revendique aucune mission de politique publique.

La composition du comité directeur soulève un problème de légitimité. Certes une personne, Postel, est remplacée par un conseil représentatif ; mais la légitimité issue de l'expertise et de la réputation personnelles est remplacée par la légitimité et la responsabilité reconnues aux représentants. Le comité directeur d'ICANN représente divers collèges sur une base fonctionnelle et géographique. Sur les dix-neuf directeurs, neuf représentent des groupements d'experts techniques, neuf autres les utilisateurs, le dernier n'est autre que le « patron » de l'organisation.

Le conseil d'ICANN est cependant soumis à une autorité supérieure : le gouvernement des Etats-Unis, dont le Département du Commerce (DoC) garde le contrôle de la racine, conservant ainsi un droit de veto sur les décisions politiques d'ICANN. En dépit de la privatisation d'internet (qui fit grand bruit), les Etats-Unis n'ont jamais entièrement lâché prise. Comme l'expliquait un document officiel du DoC, « *le département du commerce n'a pas*

l'intention de transférer à quelqu'entité que ce soit son autorité politique sur le serveur-racine » (DOC, 1999). Ainsi internet n'est internationalisé et privatisé que sous la houlette du gouvernement des Etats-Unis.

En-dessous de la racine, les contrats étendent l'autorité d'ICANN et des Etats-Unis jusqu'aux administrateurs des gTLD et des ccTLD. Les TLD génériques s'intègrent plus aisément à l'organisation, puisqu'ils sont presque tous administrés par NSI et que cette entreprise subit la pression des Etats-Unis pour participer à ICANN. Après quelques négociations sur les modalités, NSI et ICANN se mettent d'accord en 1999. ICANN assure ainsi son autorité politique sur les domaines les plus peuplés. Les ccTLD sont plus circonspects, et jusqu'en 2001 ICANN a peu progressé dans ce domaine (ICANN, 2001). L'autorité politique hiérarchique ne s'y est pas établie, ce qui perpétue l'instabilité pour l'ensemble du système.

Le conflit d'autorité implicite entre ICANN et les gouvernements nationaux se manifeste dans le Governmental Advisory Committee (GAC). Le GAC est un comité officiel consultatif ; des gouvernements nationaux peuvent s'y rencontrer, débattre et coordonner leurs actions. Individuellement, chaque gouvernement national peut affirmer son autorité politique sur les fichiers-zone qui portent son code-pays. Les gouvernements nationaux peuvent aussi coordonner une politique décidée collectivement au sein du GAC.

Le GAC entend légitimer les prétentions de ses membres à exercer l'autorité politique. D'emblée il affirme que « *le système de nommage d'internet est une ressource publique en ce sens que ses fonctions doivent être administrées en vue de l'intérêt général ou partagé* » (GAC, 2000). En précisant que le DNS doit être un bien public, tout comme le spectre électromagnétique, le GAC ouvre la voie au contrôle gouvernemental. Ensuite le GAC associe cet intérêt commun à l'autorité des gouvernements nationaux : « *l'autorité politique publique ultime sur le* [domaine code-pays] *demeure du ressort du gouvernement...* » (GAC, 2000). Ceci justifie la prétention des autorités nationales à exercer la juridiction sur les ccTLD.

ICANN prétendait que l'autorité des ccTLD dérivait de son autorité supérieure sur la racine. Si les administrateurs ne suivent pas les décisions politiques d'ICANN, celle-ci peut redéléguer l'autorité à une autre partie. Les gouvernements nationaux, affirmant que leur fichier-zone est une ressource publique, cherchèrent à placer les ccTLD sous leur propre autorité. Les administrateurs des ccTLD se trouvaient donc soumis à deux autorités – et ils en proposèrent une troisième, de leur cru, citant des documents officiels qui situent l'autorité dans « la communauté internet locale » plutôt

que dans ICANN ou les gouvernements (Postel, 1994). Cette perspective les rendait responsables vis-à-vis des utilisateurs d'internet dans leurs pays respectifs, et non vis-à-vis de leurs gouvernements ou d'ICANN.

Les membres du GAC cherchèrent à résoudre cette ambiguïté à leur profit en demandant à ICANN un pouvoir de veto sur les ccTLD identique à celui du gouvernement des Etats-Unis sur la racine. Le GAC proposa de transférer le pouvoir de redélégation d'ICANN aux gouvernements nationaux : « *quand ICANN sera avertie par le gouvernement ou l'autorité publique concernée qu'un* [administrateur] *a enfreint les termes du contrat... elle devra réagir en urgence pour réaffecter la délégation...* » (GAC, 2000). Les gestionnaires des codes-pays n'auraient donc eu accès à la racine qu'autant que leurs gouvernements le leur permettaient. ICANN refusa cette proposition, qui la subordonnait aux gouvernements nationaux. Au moment où cet article est rédigé, la fragmentation de l'autorité sur les ccTLD reste un problème non résolu.

Les débats du GAC eurent pour effet que la coordination des gouvernements nationaux s'applique à une large gamme de décisions politiques. Le GAC a entamé la rédaction d'un document de « bonnes pratiques » pour les gestionnaires de codes-pays, afin que les autorités nationales puissent standardiser leurs opérations (GAC, 2000). Une fois définies les politiques communes, tout gouvernement national peut promulguer et imposer ces pratiques dans sa propre juridiction.

Au sein d'ICANN, les mécanismes de l'autorité et de la juridiction reposent donc sur la conception même d'ICANN, sur le GAC et sur la pérennisation du rôle des Etats-Unis. La gouvernance effective d'internet est envisageable dans les domaines où les membres d'ICANN et du GAC peuvent se mettre d'accord. En dépit de la fragmentation de l'autorité, la majorité des utilisateurs d'internet, situés dans les gTLD, sont soumis à celle d'ICANN dans une juridiction unifiée.

La politique et les sanctions

Ayant examiné l'autorité et la juridiction, j'aborderai maintenant la question de la loi et des sanctions. Les premières régulations d'ICANN s'appliquèrent aux domaines en *.com*, *.org* et *.net* de l'espace de nommage, ces derniers étant combinés dans un seul système partagé (*Shared Registry System*, SRS). Au moment où j'écris cet article, l'extension des régulations d'ICANN sur les domaines des codes-pays n'est pas encore effective.

ICANN régule les utilisateurs, mais n'est pas directement en contact avec eux. Le SRS définit plutôt un système à quatre étages : ICANN au sommet, les utilisateurs à la base et deux sortes d'organisations intermédiaires : les « registries » et les « registrars ». Au sommet, ICANN utilise son autorité pour créer des régulations. En dessous, les registries gèrent les fichiers-zones et font fonctionner les serveurs (comme décrit plus haut). Encore en-dessous, les registrars font l'interface avec les utilisateurs clients. Ce sont des détaillants en noms de domaines, chargés aussi du service après-vente et souvent de services annexes, comme la fourniture d'accès à internet. Enfin, à l'étage inférieur se trouvent les administrateurs de réseaux. (Bien entendu, la plupart des utilisateurs d'internet ne possèdent pas leur propre nom de domaine, mais utilisent celui d'une tierce partie, comme *aol.com*, et constituent ainsi un cinquième niveau de la hiérarchie.)

Une cascade de contrats dévale tous les étages. Les régulations d'ICANN sont contenues dans les contrats avec les registries, puis transmises dans leurs contrats avec les registrars, qui à leur tour les insèrent dans leurs contrats avec les administrateurs de réseaux. Les décisions politiques circulent ainsi de haut en bas, d'ICANN aux registries jusqu'aux réseaux privés. Les termes du contrat définissent les lois d'internet.

A chaque niveau, le contrat avec ICANN est garanti par la menace d'un refus d'accès au nom de domaine. Tout registry qui ne s'y conforme pas peut voir son domaine redélégué. De même pour les registrars, qui peuvent être privés d'accès aux registries et donc de leur capacité d'offrir les noms de domaine aux utilisateurs. Quant aux utilisateurs récalcitrants, ils risquent de voir leurs noms de domaine supprimés à l'intérieur de l'espace de nommage, ou même affectés à quelqu'un d'autre.

Le contrat ICANN d'accréditation de registrar (ICANN, 1999a) est le mécanisme primaire de promulgation de la loi. Toute organisation qui veut devenir registrar doit se conformer aux termes de ce contrat, y compris à la clause suivante, pourtant très vague : « *le registrar se conformera... à toute politique adoptée par ICANN...* » (Section II.D.1.b.i)[4]. Comme les politiques

4. Ce passage de l'accord (Registrar Accreditation Agreement) est important mais pas particulièrement succinct. Le texte entier de la section D.1.b.i dit : « *D. Les obligations générales du registrar. 1. Pendant la durée de l'accord : b. le registrar se conformera à toute politique adoptée par ICANN en ce qu'elle : i. est relative à l'une ou à plusieurs des questions suivantes : (A) toute question dont la résolution uniforme ou coordonnée s'avère raisonnablement nécessaire pour faciliter l'interopérabilité, la fiabilité technique et/ou le fonctionnement stable de l'internet ou du DNS, (B) toute politique de registrar nécessaire dans les limites de la raison pour l'implémentation des politiques de consensus relatives aux*

d'ICANN changent et que l'accord d'accréditation évolue (comme prévu dans la Section II.O, « Le droit de remplacer un accord après sa mise à jour »), ainsi en est-il des conditions imposées à l'utilisation de tout nom de domaine. C'est ce « chèque en blanc » contractuel qui, d'évidence, accorde à ICANN le droit d'exercer la gouvernance sur un champ très large. Les termes du contrat sont répétés aux niveaux inférieurs entre les registrars et les utilisateurs ; la circulation fluide des régulations est ainsi assurée, d'ICANN aux registrars, et éventuellement aux utilisateurs. Au besoin, des sanctions sont explicitement prévues : « *Le locataire* [du nom de domaine] *reconnaît que son enregistrement du nom* [de domaine] *est susceptible de suspension, d'annulation, ou de transfert conformément à toute politique adoptée par ICANN... pour la résolution des conflits...* » (Section II.J.7.i).

Les mécanismes fondamentaux de gouvernance sont ici assurés par la circulation des contrats, assortie de la menace de refus du nom de domaine. Le contrat d'accréditation stipule les règles en vigueur sur internet, que renforce le pouvoir de révocation d'un nom de domaine. Les utilisateurs d'internet ne peuvent jouir de l'accès à l'espace de nommage que s'ils se conforment aux règles établies par ICANN ; sinon, leur nom de domaine peut être suspendu, annulé, ou transféré.

Une politique publique mondiale

Mon exposé sur le DNS, la gouvernance et la conception institutionnelle d'ICANN a cherché à décrire et analyser des données objectives. Si l'on accepte la quadruple définition de la gouvernance, et si l'on admet que ces mécanismes sont bien à l'œuvre dans ICANN, il n'est pas douteux qu'ICANN est capable d'assumer la gouvernance d'internet. Jusqu'ici, on a très peu traité d'une double question : est-ce qu'ICANN exerce cette capacité ? ce système de gouvernance est-il légitime ? Le dernier chapitre va aborder ces éléments, beaucoup plus sujets à controverses.

La politique d'ICANN

ICANN possède la capacité de gouverner et l'a déjà exercée. ICANN a institué une politique publique mondiale. Je vais expliquer maintenant ce que signifie « instituer une politique publique », ainsi que la manière dont ICANN s'y est prise.

---

registries, ou (C) la résolution de toute controverse à propos de l'enregistrement des noms de domaine (en tant qu'il contrevient à l'utilisation des noms de domaine en question)... »

Aussitôt instaurées dans ICANN, les capacités de gouvernance furent mises en pratique. En août 1999, ICANN promulgua sa première décision politique importante : la Uniform Dispute Resolution Policy (UDRP), procédure visant à déterminer qui possède le droit de propriété sur un nom de domaine (ICANN, 1999b). L'UDRP constitue la première décision de politique publique d'ICANN à visée mondiale.

A la fin des années 1990, les noms de domaine ont pris de la valeur, des noms comme *yahoo.com* et *amazon.com* sont devenus des actifs commerciaux d'envergure. De sorte que surgissent des conflits autour du droit des noms : quand des individus déposent une marque sur laquelle ils n'ont aucun droit (pour un nom de domaine quelconque), avec l'intention de la revendre à son propriétaire ; quand des titulaires de marques déposées tâchent d'interdire à d'autres utilisateurs l'utilisation d'une chaîne de caractères valorisée. Parfois les droits de propriété entrèrent en conflit avec les droits d'usage équitable ou la liberté d'expression (Kleiman, 1999). Source du problème : la législation existante ne permet pas de résoudre les conflits puisque la loi des marques est nationale et l'origine du conflit internationale. L'application des législations nationales en vigueur pour résoudre des conflits internationaux sur les noms de domaine coûte très cher et s'avère peu maniable (Littman, 2000).

L'UDRP d'ICANN a défini les procédures de résolution de tels conflits, établissant ainsi des règles de propriété. Selon une procédure alternative, des arbitres certifiés et privés décideront de la question des droits, en utilisant un critère défini par ICANN. Les décisions d'arbitrage seront exécutées par la révocation ou le transfert du nom disputé. C'est un système « amiable » en ce sens que les parties non satisfaites par la décision de l'arbitre peuvent encore recourir aux enceintes juridiques existantes. Mais ces recours étant hors de prix, dans la majorité des cas c'est l'UDRP qui détermine les droits de propriété. Elle prend *de facto* force de loi.

La mise en œuvre de l'UDRP illustre la manière dont ICANN se sert des quatre mécanismes de gouvernance à la fois. D'abord, l'UDRP a pris forme à travers les suggestions des permanents d'ICANN et l'expression de points de vue divers, et finalement elle a été adoptée par le conseil d'administration d'ICANN dans un exercice d'autorité. Ensuite, la décision politique a pris force de loi dans l'Accord d'accréditation des registrars : ICANN a fait de l'UDRP une condition de leur accès à l'espace de nommage, et ils se trouvent dans l'obligation de l'inclure dans leurs contrats de détaillants (il faut qu'elle « circule de haut en bas »). Troisièmement, l'UDRP est assortie de sanctions : tout utilisateur refusant d'y souscrire peut se voir refuser l'accès à l'espace de nommage et toute violation peut entraîner la suppression ou la

réaffectation du nom de domaine de l'utilisateur. Enfin, l'UDRP s'applique à la juridiction d'ICANN. Elle régule les noms de domaine pour les *.com*, *.net*, et *.org*. Pour les domaines de codes-pays, où l'autorité d'ICANN ne s'applique pas directement, c'est aux administrateurs des codes-pays de décider d'adopter ou non l'UDRP. A ce jour c'est le cas dans certains domaines, mais non partout.

En instituant l'UDRP, ICANN a institué une politique publique mondiale. L'UDRP réglemente un sujet d'intérêt général : les droits de propriété. Les règles concernant les marques déposées, le copyright, la propriété intellectuelle, sont traditionnellement établies par les gouvernements. La Constitution des Etats-Unis, par exemple, précise les règles de protection de la propriété intellectuelle sur les brevets. Au niveau mondial, le manque de régulation s'explique non pas parce que les règles de la propriété sont d'un moindre intérêt public, mais parce qu'aucune institution publique reconnue n'a établi de telles règles. ICANN a souhaité pallier ce manque. En instituant des règles mondiales sur la propriété, ICANN a pris une décision qui concerne aussi les valeurs publiques. L'UDRP n'aura peut-être pas une énorme incidence politique, parce que les droits de propriété sur les noms de domaine concernent un champ de régulation assez limité, mais elle représente un premier pas vers la prise de décision proprement politique[5].

La légitimité

Si ICANN instaure une politique publique mondiale, il faut lui appliquer des critères politiques comme la légitimité, la responsabilité et l'équité. Et c'est autour de telles questions que sont apparues la plupart des controverses (Weinberg, 2000 ; Froomkin, Post, Farber, 1996b ; Klein, 2001c). Je résumerai brièvement certaines des interrogations qui ont surgi autour de la légitimité du Conseil d'ICANN.

La politique suivie par les Etats-Unis pour la création d'ICANN a été explicitée dans le « White Paper » du Département du Commerce. Il définit des principes, dont deux concernent particulièrement la légitimité : ICANN doit s'engager à mettre en place une « coordination privée ascendante » et une « représentation... (qui prenne en compte) la communauté vaste et croissante des utilisateurs d'internet » (DOC, 1998b). Certains de ces

5. Je ne me demande pas si l'UDRP est de « bonne » ou de « mauvaise » politique publique. La substantialité de la régulation n'est pas en question. L'UDRP a suscité autant de louanges (Cohen, 2000) que de condamnations (Flynn, 2000 ; Mueller, 2001). L'important, ici, est le fait qu'ICANN assure une régulation globale.

principes ont inspiré le règlement intérieur d'ICANN, surtout en ce qui concerne les mécanismes de la représentation au sein du conseil d'administration (Klein, 2001a).

Dans de nombreuses instances ces principes furent malmenés. J'en mentionnerai trois. Le premier comité directeur d'ICANN était composé de neuf membres, à titre transitoire. Ce premier groupe fut nommé sans la participation ni même la consultation du public – ce qui suscita maintes protestations publiques et auditions devant le congrès des Etats-Unis. La sélection eut lieu à huis clos, processus décrit par Jon Postel lui-même comme « non démocratique et fermé » (Daley, 1998). Ce fut pourtant ce Bureau qui promulgua l'UDRP.

La constitution du conseil d'administration d'ICANN fut tout aussi inégalitaire. Les directeurs représentant les neuf collèges d'experts furent installés en l'espace d'à peu près un an après la création d'ICANN, et ils cherchèrent aussitôt à réduire la représentation des utilisateurs d'internet. Lors d'une série de réunions en 1999 et 2000, les directeurs nommés, tous des experts, cherchèrent à éliminer, réduire, ou différer l'installation de directeurs élus (ICANN, 2000). A cette fin, ils révisèrent sans arrêt le règlement intérieur qui contraignait les actions du conseil. Comme le déclara un haut fonctionnaire lors d'une réunion tenue en juillet 2000, « *le conseil donne de plus en plus l'impression d'être extrêmement cavalier en ce qui concerne les modifications du règlement intérieur* » (Wilkinson, 2000). Peu après, le conseil décida de modifier une nouvelle fois le règlement pour retarder le dernier tour des élections de directeurs jusqu'en 2002 – soit quatre ans après la création d'ICANN.

Enfin, ce premier conseil afficha sa nette préférence pour que la représentation des utilisateurs d'internet soit assurée par les professionnels de l'industrie. Lors du premier tour, partiel, de l'élection des directeurs, presque tous les sièges furent pourvus par des candidats nominés par lui, dont beaucoup de personnalités issues des géants des télécommunications comme France Telecom, Fujitsu, Deutsche Telekom et Verizon (ICANN, 2000). Lors de la réunion d'ICANN de juillet 2000, cette tendance à favoriser l'industrie des télécommunications plutôt que les utilisateurs d'internet sauta aux yeux d'un officiel australien, qui déclara : « [ICANN] *court le risque de se transformer* de facto *en association d'industriels* » (Twomey, 2000). La légitimité du Conseil fut encore affaiblie par la tendance de certains groupes d'intérêt à rechercher (et, probablement, à obtenir) une influence disproportionnée sur ses décisions.

Dans la mesure où ICANN exerce une mission de politique publique, son manque de légitimité est frappant. Bien que les élections de l'an 2000 aient

instillé une certaine dose de représentation des utilisateurs dans ICANN, elles ont échoué à instaurer le niveau de représentativité exigé par son règlement initial (Klein, 2001b ; Klein, 2001c).

La politique future

Les institutions ne sont pas des entités statiques : elle grandissent avec le temps et souvent modifient et élargissent leurs domaines d'activité. Tel semble être le cas pour ICANN. En tant qu'entité de gouvernance d'internet, quelles pourraient être les politiques promulguées par ICANN à l'avenir ? Je me livrerai rapidement à quelques spéculations.

Le domaine d'expansion politique le plus probable est celui de la protection de la propriété intellectuelle. Un accroissement des pouvoirs dans ce domaine, revendiqué dès les débuts d'ICANN, serait cohérent avec ses objectifs initiaux (Froomkin, 1999a). L'UDRP pourrait être élargie jusqu'à donner des droits d'enregistrement spéciaux aux propriétaires de noms célèbres, de marques déposées, de noms géographiques, etc. ICANN deviendrait alors une instance régulatrice mondiale au service de la propriété et du commerce électronique.

Le contrôle de l'espace de nommage pourrait aussi servir de levier pour promouvoir la justice sociale. ICANN et les monopoles ccTLD pourraient collecter des fonds pour financer un service universel permettant de surmonter la division numérique du monde, les pays pauvres payant leur accès à internet moins cher que les pays riches. Au cours de conversations privées, certains des directeurs d'ICANN issus des pays en voie de développement ont défendu devant moi de telles orientations politiques.

Le potentiel politique d'ICANN pourrait également concerner la régulation des contenus. Des sites contrevenants pourraient être censurés par la révocation ou la réaffectation de leurs noms de domaine. Le premier à être ainsi sanctionné fut le site *voteauction.com*, qui proposait un contenu illégal (un système de vente et d'achat de votes aux enchères en ligne). Le registrar du domaine a annulé l'enregistrement pour supprimer son contenu (Perritt, 2001). En théorie, ICANN pourrait renforcer ses impératifs de régulation en utilisant plus largement de tels mécanismes.

ICANN pourrait aussi devenir un instrument de taxation, permettant à un gouvernement de collecter l'impôt sur le e-commerce, ou dégageant les moyens de financer son propre personnel. Si les noms de domaine étaient accordés *via* une source unique, les utilisateurs devraient payer les frais correspondants, ou à défaut se verraient refuser l'accès. De fait, des

législateurs nord-américains et des ccTLD mécontents ont déjà accusé ICANN de lever des taxes (McCullagh, 1999 ; Ward, 2000).

Enfin, ICANN pourrait devenir un instrument de la politique nationale des Etats-Unis. En temps de guerre ou de terrorisme, un pays qui s'opposerait aux Etats-Unis pourrait voir disparaître d'internet ses domaines. Des enregistrements individuels pourraient être annulés ou transférés pour affaiblir des entités hostiles. Le rapport entre la politique d'ICANN et la politique nationale des Etats-Unis s'est déjà manifesté quand le Département du Commerce a approuvé l'ajout du domaine *.ps* – pour la Palestine – à la zone-racine. Bien que les Etats-Unis n'aient pas été guidés par un intérêt national étroit, l'affaire a fait grand bruit en raison de son potentiel conflictuel (Cisneros, 2001).

Les mécanismes de gouvernance étant mis en place, une « campagne d'infiltration » – l'expansion continue du champ régulatoire d'ICANN – semble possible. La combinaison de mécanismes efficaces de gouvernance et de mécanismes faibles de légitimité pourrait même conduire à créer des règles en fonction des opportunités.

Conclusion

Admettre tout simplement qu'ICANN est chargée de la gouvernance d'internet est lourd de significations. C'est contrecarrer des croyances bien établies et susciter des inquiétudes quant au type de gouvernance qui est en train de s'instaurer. Cela nous oblige à nous demander ce qu'il faudrait faire.

ICANN contredit la vulgate de l'anarchie bienveillante d'internet. En fait, on découvre qu'internet *peut* être contrôlé. Le DNS fournit la base d'un contrôle descendant, et ICANN l'utilise pour mener une véritable politique. Les implications de cet état de fait sont de plus en plus vastes et ne seront vraiment perçues qu'avec le temps. Pour cette raison, tout utilisateur d'internet est tenu de s'intéresser à l'avenir d'ICANN.

Je terminerai par quelques observations sur le rapport entre technologie et société. ICANN révèle sous trois facettes la manière dont la technologie modèle la société.

Les traits objectifs de la technologie ont dessiné le système administratif et régulateur. En particulier, les caractéristiques techniques d'une base de données distribuée ont effectivement paramétré la politique. Le besoin d'un espace de nommage unique avec une racine unique a créé un point de contrôle central. De même, le besoin d'identifiants uniques (afin qu'un nom corresponde à un seul ordinateur-hôte) a créé des problèmes de contrôle et

de monopole. La définition d'une zone *.com* unique, à l'intérieur de laquelle ne peut être enregistré qu'un seul *.ibm*, a engendré un système de registries monopolistiques et suscité des conflits autour du droit des marques. Peut-être toutes ces caractéristiques n'étaient-elles pas absolument nécessaires (bien qu'aucune alternative crédible n'ait été avancée, même par les plus critiques envers ICANN). On doit pourtant reconnaître que l'histoire les a si bien ancrées dans la conception et le fonctionnement du système qu'elles ont acquis un caractère de quasi-nécessité. Toute tentative de changer le statut régulateur d'ICANN impliquera sans doute de concevoir une nouvelle technologie de base (ceci concerne en particulier l'exigence d'une racine unique sous le contrôle d'un administrateur unique).

La technologie a formaté la société d'une autre manière, qui concerne le rôle des ingénieurs dans l'établissement d'une politique. La sélection des noms de domaine des codes-pays fut une décision historique aux conséquences politiques majeures. Cette décision fut prise si tôt dans le processus du développement d'internet que les seuls protagonistes furent les ingénieurs de recherche. Ceux-ci ont décidé qu'internet devait être gouverné par les gouvernements nationaux. S'ils avaient choisi d'autres identifiants alphanumériques – couleurs, séquence de chiffres, table d'éléments –, la répartition « un domaine par pays » des registries ne serait guère fondée, non plus que l'affirmation subséquente de l'autorité nationale sur les registries. Les ingénieurs ont choisi d'organiser internet sur le modèle des PTT nationales. Ils n'ont pu prendre de telles décisions que parce que celles-ci sont intervenues très tôt dans l'histoire du développement de la technologie, à un moment où eux seuls étaient concernés.

Troisièmement, la technologie influence la société dans la mesure où elle peut légitimer des décisions prises sous le sceau du secret. Quand des décisions politiques sont classifiées « techniques », il ne paraît pas illégitime qu'elles soient prises par des élites, derrière des portes fermées. La politique disparaît alors de la vue publique (Lessig, 1999). Les groupes qui ont gagné le contrôle d'ICANN ont invoqué ce voile de légitimité technique pour minimiser la critique. Même les avocats d'ICANN, pourtant dépourvus de compétence technique, ont justifié leurs prises de position par une prétendue neutralité de l'expertise technique (McLaughlin, 2000).

ICANN utilise le contrôle de l'adressage sur internet comme levier d'une politique publique mondiale. A travers ICANN, la technologie a modelé la société, des technologues ont pris des décisions politiques majeures et des groupes d'intérêts ont exploité la légitimité technologique. On a peut-être ici le schéma régulateur de l'infrastructure informatique mondiale du siècle prochain, et c'est ce qui nous importe.

Bibliographie

AFP (Agence France-Presse). 1999. "internet Pioneer Vinton Cerf Pans French Ruling Against Yahoo!" November 25.

Albitz, Paul, and Cricket Liu. 1998. *DNS and BIND.* Cambridge, MA : O'Reilly.

Andrews, Edmund, "German Court Overturns Pornography Ruling Against Compuserve," The New York Times, November 18, 1999.

Akdeniz, Yaman, "The Regulation of internet Content in Europe : Governmental Control versus Self-Responsibility," *Swiss Political Science Review* 5(1) : 123-131, 1999.

Barlow, John, "Thinking Locally, Acting Globally," *Cyber-rights Electronic List,* January 15, 1996. (Cited in Akdeniz, 1999).

Bijker, Wiebe, 1995. *Of bicycles, bakelites, and bulbs : Toward a theory of sociotechnical change.* Cambridge, MA : MIT Press.

Bijker, Wiebe, Thomas Hughes, and Trevor Pinch, eds. (1987). *The social construction of Technological systems : New directions in the sociology and history of technology.* Cambridge, MA : MIT Press.

Bliley, Thomas, 1999. Bliley Statement on Domain Name Privatization. House Committee on Commerce News Release. July 22. Viewed at: http://com-notes.house.gov/cchear.

Bridis, Ted, "Clinton Administration Says internet Reconfiguration Was Rogue Test," The Associated Press/Nando.Net, February 5, 1998.
http://www.techserver.com/newsroom/ntn/info/020598/info20_1882_noframes.html (viewed April 2000).

Brock, Gerald, 1994. Telecommunications Policy for the Information Age : From Monopoly to Competition. Cambridge, Massachusetts : Harvard University Press.

Cailliau, Robert. 2000. *How the web was born.* (Oxford University Press).

Cerf, Vint, and Robert Kahn. 1974. « A protocol for packet network interconnection" *IEEE Transactions on Communications* v.COM-22 n.5 (May), p. 637-648.

Cisneros, Oscar. 2001. Dot-PS : Domain without a country. Wired News. January 12. Viewed at: http://www.wired.com/news/politics/0,1283,41135,00.html.

Cohen, Jonathan. 2000. Presentation on UDRP. Korea internet Forum, Seoul, Korea.

CPSR (Computer Professionals for Social Responsibility), *Governing the Commons : The Future of Global internet Administration,* Proceedings of conference held on September 24-25, 1999, Alexandria, VA, U.S.A. Viewed at:
http://www.cpsr.org/conferences/dns99/dnsconf99.htm

Cukier, Kenneth, "Internet Governance and the Ancien Regime," *Swiss Political Science Review* 5(1) : 127-133, 1999.

Daley, William. 1998. Letter to the Internet Corporation for Assigned Names and Numbers. October 15.

Davies, Simon, "Europe to U.S. : No Privacy, No Trade," *Wired*, May, 1998.

DoC (U.S. Department of Commerce). 1998a. "A Proposal to Improve Technical Management of Internet Names and Addresses (Green Paper)." NTIA : Federal Register. 20 February.

DoC (U.S. Department of Commerce). 1998b. "Management of Internet Names and Addresses (White Paper)." NTIA : Federal Register, No. 63, Vol. 111, 5 June.

Flynn, Laurie. 2000. Trademarks winning domain fights. New York Times on the Web. September 4.

Froomkin, Michael. (2000). Wrong Turn in Cyberspace : Using ICANN to Route Around the APA and the Constitution. *Duke Law Journal*. Vol. 50 :17, p. 17-184.

Froomkin, Michael, 1999a. A Commentary on WIPO's 'The Management of Internet Names and Addresses : Intellectual Property Issues.' Version 1.0, May 17. Viewed at http://www.law.miami.edu/~amf/commentary.htm

Froomkin, Michael, David Post, and David Farber. 1999b. *ICANNwatch*. http://www.ICANNwatch.org Viewed 30 November.

Froomkin, Michael. 1997. « The Internet as a Source of Regulatory Arbitrage » In Kahin, Brian, and Charles Nesson, *Borders in Cyberspace* (Cambridge, MA: MIT Press).

Fryer, Bronwyn, "The Software Police : They Hear from the Snitch You Copied That Disk, They Send in the Marshals to Bust Your Ass. No Joke," *Wired*, May 1995.

GAC (Governmental Advisory Committee), "Principles for Delegation and Administration of ccTLDs," presented at ICANN Board meeting, 23 February 2000. Viewed at http://www.icann.org/gac/gac-cctldprinciples-23feb00.htm

Hafner, Katie, and Lyon, Matthew, *Where Wizards Stay Up Late : The Origins of the Internet* (New York : Touchstone, 1998).

Holitscher, Marc, "Debate : Internet Governance," *Swiss Political Science Review* 5(1) : 115-116, 1999.

Hughes, Thomas P., *Networks of Power : Electrification in Western Society, 1880-1930* (Baltimore : Johns Hopkins University Press, 1983).

ICANN, 1999a. Registrar Accreditation Agreement. May 12, 1999. Viewed at : http://www.icann.org/ra-agreement-051299.html

ICANN, 1999b. Uniform Dispute Resolution Policy (UDRP). October 24. http://www.icann.org/udrp/udrp-policy-24oct99.htm.

ICANN, 1999c. NSI-Registrar License and Agreement. November 9. Viewed at: http://www.icann.org/nsi/nsi-rla--04nov99.htm.

ICANN, 1999d. Amendment 1 to ICANN/DOC Memorandum of Understanding. November 10. Viewed at: http://www.icann.org/nsi/amend1-jpamou04nov99.htm.

ICANN, 1999e. Amendment 19 to Cooperative Agreement Between NSI and the U.S. Government. November 8. Viewed at:
http://www.icann.org/nsi/coopagmt-amend19-04nov99.htm.

ICANN, 1999f. ICANN Bylaws (As Revised). Viewed at:
http://www.icann.org/bylaws-09april99.html.

ICANN, 2000a. Home Page. Viewed May, 2000, at: http://www.icann.org

ICANN, 2000b. Proposed Budget for Fiscal Year 2000-2001. Viewed at:
http://www.icann.org/financials/proposed-budget-04may00.htm.

ICANN, 2001. Third Status Report Under ICANN/US Government Memorandum of Understanding, 3 July 2001. Viewed at:
http://www.icann.org/general/statusreport-03jul01.htm.

IAB (Internet Architecture Board). 1999. Request for Comments 2826 : IAB Technical Comment on the Unique DNS Root. Viewed at http://www.rfc-editor.org/rfc.html.

IPC (Intellectual Property Constituency), "IPC Position Paper on ccTLD Issues," presented at ICANN Board meeting, 1 March 2000. Viewed at:
http://www.icann.org/cairo2000/ipc-position-01mar00.htm

ICANN. 2000. Notes and Minutes. http://www.icann.org/minutes/notes-minutes.htm. Viewed 1 November.

Johnson, David, and Post, David, 1997. *The Rise of Law on the Global Network.* In Kahin and Nesson, eds. (1997).

Kapor, Mitch. 1990. The Software Design Manifesto. Available at:
http://www.kapor.com/homepages/mkapor/Software_Design_Manifesto.html (visited October 20, 2000).

Kahin, B., and Keller, J., eds. 1997. *Coordinating the Internet.* Cambridge, Massachusetts : MIT Press.

Kahin, Brian, and Nesson, Charles, 1997. Borders in Cyberspace. Cambridge, Massachusetts : MIT Press.

Kleiman, Kathryn, 1999. Brief Of Amicus Curiae Association for the Creation and Propagation of Internet Policies. Worldsport Networks Limited v. Artinternet S.A. and Cedric Loison. United States District Court for the Eastern District of Pennsylvania, No. 99-Cv-616. Viewed at::
http://www.domain-name.org/worldsport.html.

Klein, H., "Tocqueville in Cyberspace: Using the Internet for Citizen Associations" in *The Information Society*, Vol. 15, No. 4, November 1999.

Klein, Hans, "System Development in the Federal Government: How Technology Influences Outcomes," *Policy Studies Journal* Vol. 28, No. 2, 2000, 313-328.

Klein, Hans. 2001a. "Online Social Movements and Internet Governance," *Peace Review*, Vol.13, No. 3, September 2001, 403-410.

Klein, Hans. 2001b. "The Feasibility of Global Democracy : Understanding ICANN's At Large Election," *info*, Vol. 3, No. 4, August 2001, 333-348.

Klein, Hans, ed. 2001c. "Global Democracy and the ICANN Elections," special issue of *info*, Vol. 3, No. 4, August 2001.

Klein, Hans, and Kleinman, Daniel, "The Social Construction of Technology : Structural Considerations," *Science Technology & Human Values*, January, 2002.

Leiner *et al.*, "A Brief History Of The Internet By Those Who Made The History, Including Barry Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Lawrence G. Roberts, Stephen Wolff," August, 2000. http://www.isoc.org/internet/history/

Lessig, Lawrence. (1999). *Code and Others Laws of Cyberspace*. (New York : Basic Books).

Levy, Stephen, "Cypher Wars : Pretty Good Privacy Gets Pretty Legal," *Wired*, November, 1994.

Littman, Jessica. 2000. The DNS Wars. (get full reference)

McCullagh, Declan. 1999. ICANN Too Tax You. *Wired News*. June 18. Viewed at: http://www.wired.com/news/print/0,1294,20293,00.html

McLaughlin, Andrew. 2000. "ICANN : Myths and Reality. TIES Conference, Paris, April.

Mockapetris, Paul, 1983. Domain Names -- Concepts and Facilities. Request for Comments 882. Published by Internet Architecture Board. Viewed at: http://www.rfc-editor.org/rfc.html

MSNBC, 2000. Viewed at: http://www.msnbc.com/news/387441.asp.

Mueller, Milton, 1997. *Universal Service: Competition, Interconnection, And Monopoly In The Making Of The American Telephone System*. Cambridge, Massachusetts: MIT Press.

Mueller, Milton, 1998. "The battle over Internet Domain Names: Global or National TLDs". *Telecommunication Policy*. Vol. 22, No. 2.

Mueller, Milton. 1999. "ICANN and Internet Governance: Sorting Through the Debris of 'Self-regulation'" *Info*, Vol. 1, No. 6, December.

Mueller, Milton, 2000. Technology and Institutional Innovation: Internet Domain Names. *International Journal for Communication Law and Policy*. Issue 5, Summer.

Mueller, Milton. 2001. Rough Justice. *The Information Society*, Vol. 17, No. 3.

NetNames. 2000. Press Release : Internet comes of age with 30 millionth domain name. Boston : Netnames.com. October 4.

New York Post, 2000. Viewed at: http://www.nypost.com/business/28458.htm.

Pfeffer, Jeffrey, and Salancik, Gerald, *The External Control of Organizations : A Resource Dependency Perspective* (New York : Harper & Row, 1978).

Perritt, Henry, 1997. *Jurisdiction in Cyberspace: The Role of Intermediaries.* In Kahin and Nesson, eds. (1997).

Perritt, Henry. 2001. "Electronic Commerce : Issues In Private International Law And The Role Of Alternative Dispute Resolution." WIPO Forum on Private International Law and Intellectual Property, Geneva, January, 2001.

Post, David, 1998. Cyberspace's Constitutional Moment. *The American Lawyer* (November).

Postel, J. 1984. RFC :920 : Domain Requirements. USC Information Sciences Institute, at ftp ://ftp.isi.edu/in-notes/rfc920.txt.

Postel, J. 1994. RFC :1591 : Domain Name System Structure and Delegation. ftp://ftp.isi.edu/in-notes/rfc1591.txt.

Rutkowski, Anthony, "Competing Models of Internet DNS Service Governance" 4 November 1998. Viewed at http://www.wia.org/pub/models.html

SBA (Office of Advocacy, U.S. Small Business Administration), "Roundtable Discussion on the Small Business Impact of Changes to the Internet Domain Name System," March 1, 2000, Washington, D.C.

SBA (Office of Advocacy, U.S. Small Business Administration), "Request for a Procedural Policy," Memo to ICANN dated October 27, 1999, Washington, D.C.

Shaw, Robert, 1997. "Internet Domain Names: Whose Domain is This?" In *Coordination of the Internet*, 1997. MIT Press.

Schroeder, Ralph, ed., *Max Weber, Democracy and Modernization* (New York : St. Martin's Press, 1998).

The Standard, March 09, 2000. Quotation is of Vinton Cerf. Viewed at

http://www.thestandard.com/article/display/1,1151,12788,00.html

Twomey Paul. 2000. Spoken comments before the ICANN board of Directors. Available on-line at: http://cyber.law.harvard.edu/icann/yokohama/

Ward, Mark. 2000. Net Groups in World Wide Wrangle. BBC News. July 4. Viewed at: http://news.bbc.co.uk/hi/english/sci/tech/newsid_817000/817657.stm.

Weinberg, J. 2000. ICANN and the Problem of Legitimacy. *Duke Law Journal*. Vol. 50, No. 1, October.

Wilkinson, Christopher. 2000. Spoken comments before the ICANN board of Directors. Available on-line at: http://cyber.law.harvard.edu/icann/yokohama/

Wired News, "Palestine Wins Internet Home," March 23, 2000. Viewed at http://www.wired.com/news/print/0,1294,35151,00.html