La gouvernance d’Internet

Gouvernance : manière dont un domaine d'activités est gouverné. La gouvernance ne renvoie pas nécessairement à une entité unique et décisionnelle, mais plutôt à un système d'entités décisionnelles qui dirige un certain domaine d'activités. La gouvernance est ainsi un concept reposant sur l'approche systémique puisqu'elle se décline irrémédiablement en un « système de gouvernance », impliquant ainsi une structure de gouvernance et un dynamisme de système (processus de gouvernance, activités de gestion, etc).

- Un terme généralement utilisé pour parler de la puissance publique, mais appliqué à de nombreux domaines

⇒ c'est donc l'**existence d'une quelconque autorité capable de créer pour l'usage d'internet des règles globalement applicables et renforcées par des sanctions**

Les problèmes posés par Internet

- Son caractère **global** qui provoque un décalage entre infrastructure, les pays hébergeurs et connectés, et juridiction en vigueur
- Sa **nature** ou construction en réseau : éclatement qui provoque un décalage dans le temps et l'espace
- La **diversité des acteurs** qui le façonnent
- Le **rôle des gouvernements :** leurs prérogatives et leur pouvoir
- La **légitimité** des institutions ou organismes régulateurs
- Sa **valeur** : un outil dont tout le monde veut se saisir et maîtriser

I. Le modèle multi parties prenantes
   A. Point historique sur la constitution des acteurs
   B. Description du modèle et ses différents acteurs
   C. Son fonctionnement actuel
II. Enjeux de maîtrise des infrastructures internet
   A. Une mainmise américaine sur l'IANA et l'Icann
   B. La maîtrise des DNS
   C. Souveraineté numérique, penser le politique dans la technique
III. Repenser le terme de gouvernance / les défis actuels de la gouvernance
   A. Internet ou "des" Internet ?
   B. La co-construction/superposition des Internet
   C. Une place pour la société civile dans la gouvernance ?

I. Le modèle multi parties prenantes

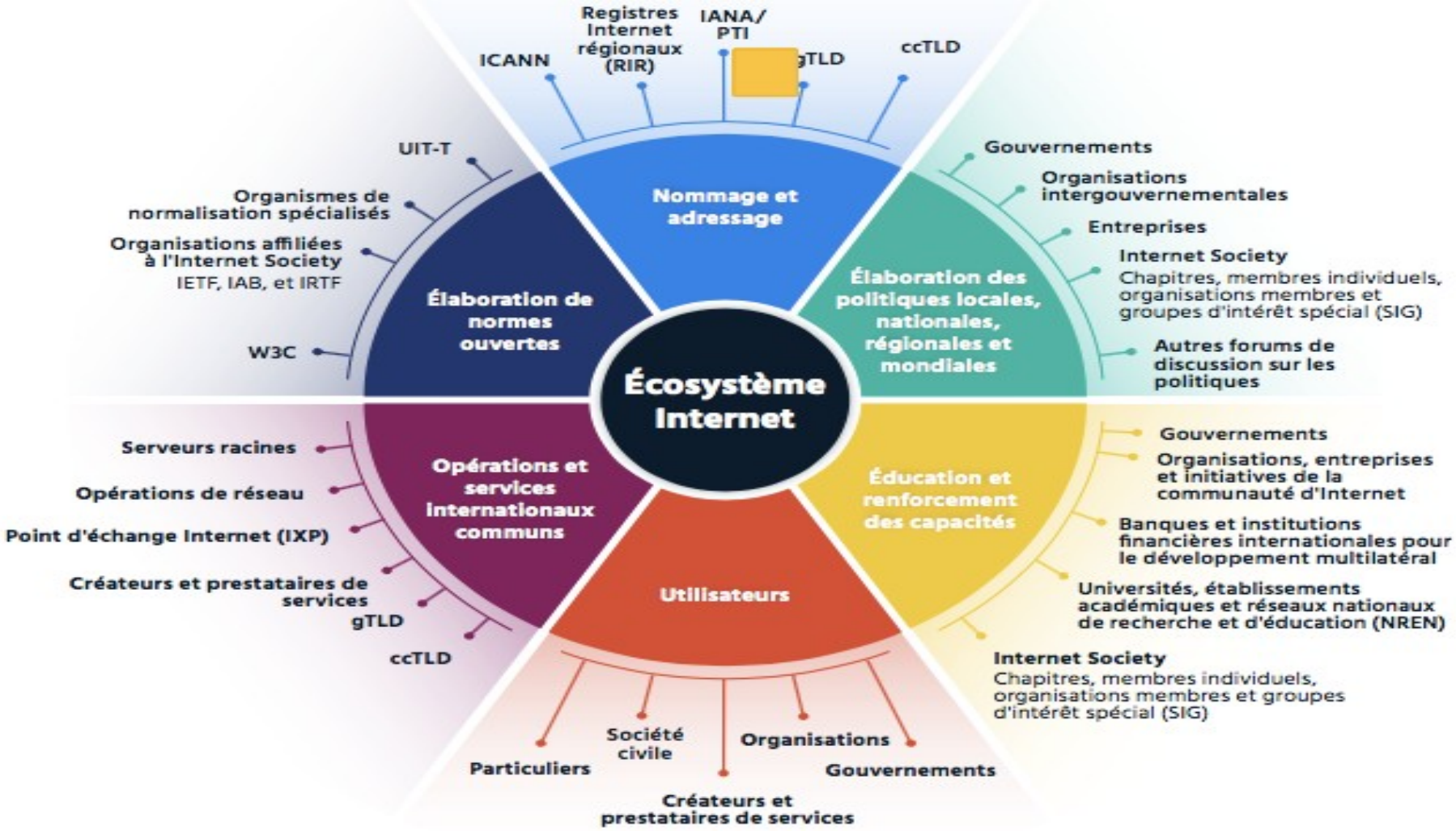
Penser le Net, c'est le fabriquer.
"Nous récusons rois, présidents et vote. Nous croyons au consensus et aux programmes qui tournent."

En réalité, dès les origines, des conceptions rivales se sont affrontées dans la conception d'Internet, liées aux désaccords entre les différentes « communautés » – militaire, scientifique, contre-culturelle – qui ont cherché à en définir la structure et les usages.

Années 60-70 : une tension entre ouverture et contrôle
- une origine militaire (ARPANET)
- un état d'esprit de laboratoire

Années 80 : une tension entre le marchand et le non marchand
Années 90 : création du Web (1992), espace de tous les possibles. John Perry Barlow *Déclaration d'indépendance du Cyberespace* 1996
Années 2000 : **le "Web 2.0"** tension entre liberté d'entreprendre et régulation étatique

→ Internet libéral vs libertaire vs commercial vs géopolitique …


Écosystème Internet
Nommage et adressage
ICANN
Registres Internet régionaux (RIR)
IANA/ PTI
gTLD
ccTLD
Élaboration de normes ouvertes
UIT-T
Organismes de normalisation spécialisés
Organisations affiliées à l'Internet Society
IETF, IAB, et IRTF
W3C
Élaboration des politiques locales, nationales, régionales et mondiales
Gouvernements
Organisations intergouvernementales
Entreprises
Internet Society
Chapitres, membres individuels, organisations membres et groupes d'intérêt spécial (SIG)
Autres forums de discussion sur les politiques
Opérations et services internationaux communs
Serveurs racines
Opérations de réseau
Point d'échange Internet (IXP)
Créateurs et prestataires de services
gTLD
ccTLD
Éducation et renforcement des capacités
Gouvernements
Organisations, entreprises et initiatives de la communauté d'Internet
Banques et institutions financières internationales pour le développement multilatéral
Universités, établissements académiques et réseaux nationaux de recherche et d'éducation (NREN)
Internet Society
Chapitres, membres individuels, organisations membres et groupes d'intérêt spécial (SIG)
Utilisateurs
Particuliers
Société civile
Organisations
Gouvernements
Créateurs et prestataires de services

Les principaux acteurs

- ❑ ICANN
- ❑ IANA
- ❑ IETF - IRTF
- ❑ gTLD et ccTLD
- ❑ Internet society et affiliés
- ❑ Les fournisseurs d’infrastructure
- ❑ Les entreprises privées
- ❑ La société civile
- ❑ Les gouvernements
- ❑ Forums internationaux

Mode d’action du modèle multi-acteurs

Depuis la création d’Internet, une majeure transformation a eu lieu dans la gouvernance d’Internet

- avant 2005 dominait le modèle « bas en haut » (coordination par le secteur privé)
- aujourd’hui s’est imposé le modèle multi acteurs (principe de subsidiarité et consenus)

2003-2005 : **Sommet Mondial International de l’Internet** (SMSI) et l’adoption de Agenda de Tunis met l’accent sur la collaboration

Chaque année, d’autres forums intergouvernementaux mettent en acte ce modèle et dessinent les contours de la gouvernance future. Par exemple, le **NETMundial** d’avril 2014

IGF 2023 - 8 thèmes
AI & Emerging Technologies - Avoiding Internet Fragmentation - Cybersecurity, Cybercrime and Online Safety - Data Governance and Trust - Digital Divides and Inclusion - Global Digital Governance and Cooperation – Human Rights and Freedoms - Sustainability & Environment

Programme général (ISOC 2020)

Renforcer Internet

- étendre le cryptage
- sécuriser le routage mondial
- partager les connaissances
- limiter la fracture numérique
- produire des lois

Développer Internet

- connecter les non-connectés
- favoriser une infrastructure durable pour le peering
- Mesurer internet

II. Enjeux de maîtrise des infrastructures internet

Point historique sur la constitution des acteurs

1968 : mise en place du réseau Arpanet par la Darpa (Pentagone)

La dissociation progressive entre l'usage militaire et civil du réseau internet pousse le gouvernement américain à la **création de l'Icann en 1998.**

Cette politique s'inscrit dans le développement de la stratégie américaine sur Internet. Lors du second mandat du Président Bill Clinton, les autorités américaines ont exprimé leur souhait d'avoir le leadership mondial sur le commerce de l'information privée, caractérisé par

- Les postures quasi monopolistiques acquises par les Gafa (Google, Apple, Facebook, Amazon).
- La stratégie d'investissement dominante dans le stockage des données (*cloud*).
- La maîtrise des nouveaux canaux de diffusion (exemple des MOOC, formation en ligne ouverte à tous).
- Le processus de valorisation de l'économie de la connaissance.

2000's - 2010's : **contestation de la mainmise américaine** par la communauté internationale

2016 : l'Icann devient indépendante

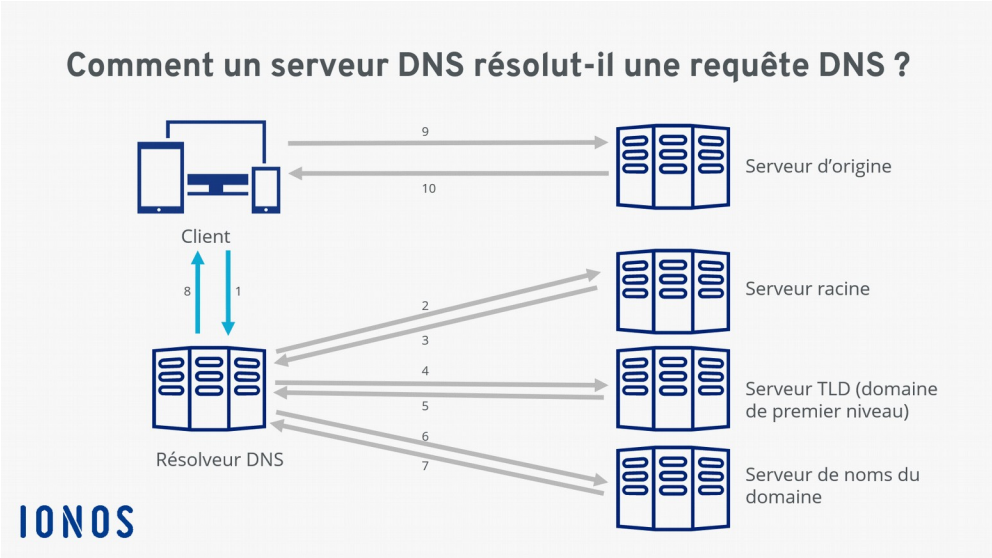
Comprendre les enjeux du DNS

Un serveur DNS **reconnaît quel domaine correspond à quelle adresse IP** ou sait à quel autre serveur DNS il doit transmettre la demande. Un serveur DNS, également appelé serveur de noms, est un logiciel serveur spécial : il s'appuie sur une base de données pour traiter les demandes du **Domain Name System (DNS)**.

2 types de DNS :

- les DNS qui "font autorité" appelés **DNS primaire ou secondaires** : ils sont responsables d'une zone DNS, c'est-à-dire d'un domaine ou d'un sous-domaine individuel. Les informations fournies par les serveurs de noms faisant autorité sont fiables.
- les **DNS "récursifs"**, qui ne font pas autorité car ils obtiennent leurs informations d'autres serveurs de noms faisant autorité. Ils utilisent les informations d'un DNS, non pas à partir de leur propre fichier de zone, mais à partir d'une deuxième ou d'une troisième source. Une telle situation se produit lorsqu'un serveur de noms **n'a pas les informations pour répondre à une requête** et qu'il doit **obtenir les informations auprès d'un autre serveur de noms**.

1. Le **client** cherche un nom de domaine ou une URL, ce qui envoie une requête au résolveur DNS.
2. Le **résolveur DNS** transmet la demande directement à un serveur racine.
3. Le **serveur racine** est un serveur de noms faisant autorité. Il répond au résolveur DNS avec l'adresse du domaine de premier niveau (TLD) concerné.
4. Le résolveur DNS envoie ensuite une requête au **serveur TLD** contenant les enregistrements DNS associés à son domaine de premier niveau.
5. En réponse, le résolveur DNS reçoit l'adresse IP du **serveur DNS faisant autorité sur le domaine recherché**.
6. Le résolveur DNS demande au serveur DNS faisant autorité l'adresse IP du serveur d'origine sur lequel le site Web est hébergé.



7. Le résolveur DNS obtient l'**adresse IP du serveur d'origine** auprès du serveur DNS faisant autorité.

8. Le résolveur DNS transmet l'adresse IP au client.

9. Le client peut alors interagir avec le **serveur d'origine du site Web demandé** via l'adresse IP.

10. Le serveur d'origine envoie les données du site Web demandé au client.

Il est souvent utilisé comme un moyen de collecte de données, car les requêtes DNS peuvent **fournir des informations précieuses** sur les comportements en ligne des utilisateurs :

- découvrir les sites web visités, les recherches effectuées ou les interactions avec les services en ligne. Ces données peuvent être exploitées pour des analyses comportementales, des études de marché ou encore des prévisions de tendance.
- La localisation géographique des serveurs DNS utilisés peut aussi **fournir des indications sur la distribution géographique des utilisateurs et des ressources en ligne**. C'est un précieux atout pour le ciblage des campagnes publicitaires ou le profilage démographique.
- L'utilisation du DNS pour résoudre les noms de domaine en adresse IP **permet de comprendre et d'analyser le trafic réseau**. Les enregistrements aident notamment à identifier les serveurs utilisés, les domaines visités, les temps de réponse ou les erreurs de résolution.

Conclusion : ces informations sont essentielles pour **la surveillance et l'optimisation des performances du réseau**, ainsi que pour la détection d'anomalies ou d'activités malveillantes.

Risques et débats liés aux DNS

Failles de sécurité :

- ➔ Les DNS leaks
- ➔ Contrôle et/ou censure via les DNS
- ➔ DNS Hijacking
- ➔ DNS Spoofing

Le système DNS est sans cesse convoqué dans la réglementation progressive du numérique.

- la loi sur le programme militaire votée par le Sénat en juin 2023, qui concerne l'extension des pouvoirs de l'Anssi dans la restriction des noms de domaine en cas de cyberattaque majeure
- le projet de loi pour la Sécurisation de l'espace numérique (SREN) en cours d'examen au Sénat, qui concerne l'enrayement de l'impunité en ligne et des contenus illégaux, ainsi que 'imposition de la limite d'âge sur les sites pornographiques

Les noms de domaines - ce que gère l'Icann

Qu'est ce qu'un nom de domaine ?

Un **nom de domaine** est la traduction d'une adresse IP en une suite de caractères facile à retenir ou mémorisables pour accéder à un site web ou retenir une adresse de courrier.

Il est unique dans un espace de nommage (comme le .fr) et attribué **au premier qui en fait la demande**, s'il satisfait aux conditions d'attribution de l'extension.

2 types

- Des **extensions nationales** (ccTLD, "Country Code Top Level Domain"), comme le .fr, le .re ou les autres noms de domaine ultramarins gérés par l'Afnic.
- Des **extensions génériques** (gTLD, "Generic Top Level Domain") dont les plus connues sont le .com, .net, .info, .biz. Depuis quelques années, de nombreuses nouvelles extensions génériques ont fait leur apparition,
  comme .paris, .bzh, .alsace, .corsica. 3 caractères ou plus.

- Les gTLD « *ouverts mais ne visant aucune cible spécifique* », le plus connu étant le .com. Il « *a été à l'origine créé pour désigner des organismes commerciaux ou à but lucratif* ». On retrouve aussi le .net des réseaux, le .org des organisations à but non lucratif, le .biz, le .info, etc.

- Les gTLD « *ouverts visant des cibles spécifiques en termes de type de titulaires, de positionnement marketing et d'usages* ». Ils doivent représenter un commanditaire, une communauté ou une entreprise. Par exemple, les .asia, .jobs et .mobi.

- Enfin, les gTLD semi-fermés, « *réservés à une cible particulière. C'est le cas du ".coop" réservé aux coopératives ou du ".museum"*

Depuis mars 2013, les extensions GTLDs ont été complétées par des nouveaux domaines de premier niveau. Il est aujourd'hui possible d'enregistrer des milliers de nouvelles extensions individuelles faisant référence à des régions, au sport voire au commerce (*paris*, *.music*, *.travail)*

Pourquoi ? **Car le nombre de sites Internet a considérablement augmenté** depuis les années 2000, provoquant l'allongement des adresses Internet.

Coûts des noms de domaine

Domaine	Coûts pour un an	Focus
.com	15–24 €	International
.fr	10–15 €	France
.org	15–24 €	International
.net	15–24 €	International
.eu	13–29 €	Europe
.io	60–100 €	Informatique
.mobi	25–32 €	Produits appareils mobiles
.app	24–30 €	Apps/Software
.beauty	18–20 €	Cosmétique
.shop	49–60 €	E-Commerce
.blog	39–48 €	Blogs
.paris	49–70 €	Régional/Touristique

Le marché des noms de domaines

La mise en ligne de nouveaux noms de domaine de premier niveau est encastré dans le **marché des noms de domaines** où s'exercent la loi de l'offre et de la demande.

2 controverses :

- le **.wine** et **.vin.** L'entreprise Donuts.Inc a cherché à posséder le nom de domaine afin de faire payer à des centaines de producteurs viticoles son utilisation.
- le **.psg** dont le club n'est pas propriétaire qu'il aimerait racheter… à prix d'or.

Afnic Association française pour le nommage Internet

Souveraineté numérique et cyberespace

Cyberespace : espace d'information généré par l'interconnexion globale des systèmes d'information et de communication dans lequel les données sont créées, stockées et partagées.

Il désigne à la fois :

- **l'infrastructure physique** à la source de cet environnement : câbles, serveurs, routeurs, satellites et tous les appareils connectés qui sont ancrés dans le territoire géographique physique et politique
- **l'espace virtuel** dans lequel circulent les données, l'information et les idées

Le cyberespace fait l'objet d'une gouvernance décentralisée et d'une souveraineté partagée.

Son enchevêtrement juridictionnel et l'application du droit parfois difficile laissent deviner des affrontements géopolitiques mondiaux

ex : RGPD, Runet, le cyberespace chinois

La territorialisation des données et l'ex territorialisation du droit

Frédérick Douzet et sa typologie

- **couche des infrastructures physiques**, fibres optiques, IXP, routeurs et commutateurs
- **couche protocolaire** contrôle et supervision, les tables de routage, le DNS, les logiciels qui en assurent le fonctionnement
- **couche logique**, les données visitées par l'internaute, son navigateur, les logiciels des serveurs ;
- **couche cognitive**, les interactions entre les humains et les couches inférieures, dont l'activité des ingénieurs qui assurent le fonctionnement et l'évolution de l'Internet, notamment au sein d'organismes de concertation, de coopération et de normalisation tel que l'IETF).

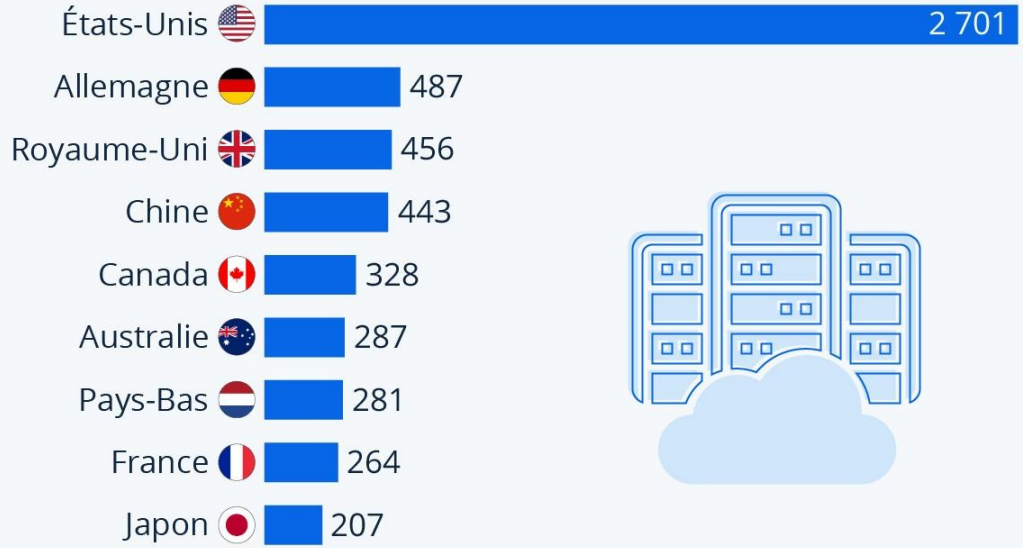
La localisation des centres de stockage de données (*Data Centers*) est souvent le résultat de conjonctures politiques et historiques particulières car constituent des infrastructures hautement stratégiques : ce sont les lieux où les données sont physiquement conservées et traitées.

"T**erritorialisation des flux de données**" *Le cyberespace, nouveau lieu de conflictualités géopolitiques* Amaël Cattaruzza

Cloud Act 2018 ; Loi russe sur la data-localisation des données 2014

Les pays qui hébergent le plus de data centers

Nombre de centres de données recensés par pays en septembre 2022 *



* Sélection des pays avec plus de 200 data centers répertoriés.

Source : Cloudscene

L’économie numérique des FAI : bras de fer entre régulation étatique et marché

Un Fournisseur d’accès à Internet (FAI ou ISP Internet service Provider) est un organisme (généralement une entreprise mais parfois aussi une association) offrant une connexion à Internet, le réseau informatique mondial.

Les FAI coopèrent afin d’assurer une connectivité globale pour leurs réseaux de clients respectifs. Ils garantissent l’accès à Internet pour les particuliers, pour de larges sous-réseaux qui représentent des entités commerciales ou des institutions publiques.

Laurent Bloch “*Si l’on compare l’Internet à un continent, les AS (autonomous system) en sont les pays, séparés par des frontières, avec chacun sa législation.* » Ex : AT&T, Verizon, les entreprises qui contrôlent ce secteur sont aussi en très grande majorité américaines.

Les plus grands FAI forment une aristocratie du Net nommée **Tier 1** : ils sont si importants que tous les autres opérateurs n’ont d’autre choix que de leur donner accès gratuitement à leurs réseaux, et d’ouvrir la porte à leurs paquets.

III. Les défis actuels des gouvernances

« il faudrait que les débats autour de la gouvernance de l'Internet échappent à l'idéologie. Lors du Sommet de Dubaï de l'UIT en décembre 2012, l'excessive polarisation entre les partisans auto-proclamés d'un Internet « libre et ouvert » et les tenants d'une gouvernance fondée sur la souveraineté territoriale avait suscité un discours anxiogène autour d'une possible « guerre froide numérique ». ***Or il n'y a pas une gouvernance, mais plusieurs, en fonction des enjeux et sujets abordés. Quel modèle unique de gouvernance pourrait traiter de sujets aussi divers que la cyber-sécurité, l'adoption de standards techniques, la liberté d'expression ou le statut des entreprises de contenus et de services ?*** *»*

Julien Nocetti, *Le Monde 2014*

→ gouvernance d'Internet ou "des" internets ?

La nécessité d'une co-construction par les lois du marché, les relations difficiles entre Etats et sociétés privées

Exemple de la neutralité du Net comme superposition de deux Internet (BtoB : les FAI et le BtoC : les utilisateurs)

La **neutralité du net** est l'un des principes fondateurs d'internet, qui exclut la création d'accès à internet « à plusieurs vitesses », par une gestion favorisant certains flux d'information au détriment d'autres (discrimination), ou la création d'accès à internet limités (à certains contenus ou certaines plateformes).
l'Arcep qui est chargée de veiller au respect de la neutralité du net.

Loi pour une République du Numérique 2016

- **le droit des utilisateurs** *« d'accéder aux informations et aux contenus et de les diffuser, d'utiliser et de fournir des applications et des services et d'utiliser les équipements terminaux de leur choix, quel que soit le lieu où se trouve l'utilisateur final ou le fournisseur, et quels que soient le lieu, l'origine ou la destination de l'information, du contenu, de l'application ou du service, par l'intermédiaire de leur service d'accès à l'internet* ».
- **le devoir des fournisseurs d'accès internet de traiter « *tout le trafic de façon égale et sans discrimination"***

La particularité européenne : une réglementation unique au monde

Article 8 de la **Charte des droits fondamentaux de l'Union Européenne** "Protection des données à caractère personnel"

Agit sur des domaines tels que

- réglementation de la propriété privée
- dumping fiscal
- cybersécurité
- libre concurrence
- RGPD (2018) qui définit les données à caractère personnel comme "des informations se rapportant à une personne physique identifiée ou identifiable"

Deux nouvelles lois appliquées cette année

- le Digital Services Act
- le Digital Market Act

La désillusion des pionniers

Constat un peu déprimant des fondateurs d'Internet : à partir des années 2010 l'ère du Big Data où **le numérique dépasse le Net.**

Internet et, par extension, le web, ne semblent plus constituer un espace de liberté mais un monde étroit où règne l'"homophilie" (chambres d'échos, bulles de filtres) gouvernée par des algorithmes.

La place au débat démocratique s'est vue décrédibiliser par les scandales de surveillance : la censure des gouvernements autoritaires et les disparités mondiales de connexion démentent l'idée d'un espace Internet mondial.

La **domination d'une poignée d'énormes acteurs** menace l'équilibre sur lequel Internet s'est construit – un réseau décentralisé qui maintenait un équilibre des forces.

Evgeny Morozov *The Net Delusion* « *cyberutopisme* » et l'« *Internet-centrisme* »

Une gouvernance qui nous échappe ?

Antoinette Rouvroy et Thomas Berns théorise une nouvelle forme de pouvoir : ***« gouvernementalité algorithmique »*** : “*un gouvernement qui s’exerce, qui structure le champ d’action possible, sans jamais contraindre les sujets, mais plutôt en façonnant* a priori *leurs environnements informationnels, comme les recommandations d’Amazon*”

Il faut continuer de **penser politiquement la technologie.**

Le futur du Net n’est pas écrit, il est en cours, cf Phillipe Aigrain : “*Il faut se garder de penser que l’histoire du numérique a couru son cours”*

Cela ne passe pas forcément par l’apprentissage du code, mais cela implique une **compréhension basique de ses principes** : comment fonctionne une base de données, ce que fait un algorithme. Cela passe aussi par une éthique personnelle et parfois des refus.