Asymétrisation et barrières : évolutions d'architecture et reconfigurations de la « coopération » dans l'internet des origines

Cette contribution explore les manières dont la mutation de l'internet en un phénomène de culture de masse s'opère par des transformations radicales de l'architecture du réseau, passant par un double phénomène : l'asymétrisation des flux et l'érection de barrières à la libre circulation. On se propose de démontrer que cette mutation entraine une reconfiguration de ce que l'on appellera le « principe de coopération » de l'internet. Cette reconfiguration du réseau démultiplie les modalités organisationnelles de l'internet et remet en question son modèle. Le formatage technique ne repose pas sur la domination d'un principe organisationnel unique, mais sur la coexistence de différents niveaux de centralisation, hiérarchisation et coopération : des ressources, des pouvoirs et des internautes.

Introduction

Au milieu des années 1990, l'explosion commerciale de l'internet en change radicalement la forme, transformant une tranquille utopie de scientifiques passionnés en médium de masse agité et puissant (Abbate, 1999). Des millions de nouveaux utilisateurs font leur apparition sur le Net, avec de nouveaux profils d'internautes : les *ordinary people* intéressés par la facilité avec laquelle on peut entrer en contact, visiter des pages d'information, et acheter en ligne, plutôt que par les secrets et les détails de structuration de réseaux complexes. Dès lors, les modalités d'adoption du réseau de la part des utilisateurs (et des utilisateurs de la part du réseau) évoluent profondément. Si dès 1994, le public commence à rejoindre en masse la communauté d'ordinateurs qui composent l'Internet, posant problème pour la durabilité de la plus basique des ressources - la bande passante -, la confiance croissante dont les utilisateurs investissent le « réseau des réseaux », pour des usages et des applications à la fois fondamentaux et critiques, entraîne de nouveaux critères de sécurité, conduisant à la mise en place de pare-feu qui divisent fortement l'Internet en régions s'auto-alimentant et se suffisant à elles-mêmes.

Notre contribution vise à explorer les manières dont la mutation de l'internet en un phénomène de culture de masse s'opère par des transformations radicales de l'architecture du réseau, passant par un double phénomène : l'asymétrisation des flux et l'érection de barrières à la libre circulation. On se propose de démontrer que cette mutation entraine une reconfiguration de ce que l'on appellera le « principe de coopération » de l'internet : l'attribution de priorité à des questions d'efficacité et d'optimisation technique du dispositif. Si l'objectif initial de l' « intelligence collective » des hommes et des machines qui composaient l'internet pouvait assez aisément être identifié dans la construction d'un réseau fiable, efficace et puissant, l'entrée de l'internet dans sa phase commerciale change les équilibres, les avantages et les structures ; elle provoque nombre de points de stress et de faiblesse.

Cette reconfiguration du réseau démultiplie les modalités organisationnelles de l'internet, au même moment où elle remet en question son modèle (Musiani & Schafer, 2011). Cette contribution se propose de montrer comment le formatage technique ne repose pas sur la domination d'un principe organisationnel unique. Ce n'est pas plus le cas à l'origine, avec un supposé modèle absolument décentralisé, qu'aujourd'hui avec un prétendu omnipotent modèle hiérarchique. En revanche, le modèle internet repose sur la coexistence de (et les tensions entre)

différents niveaux de centralisation, hiérarchisation et coopération : des ressources, des pouvoirs et des internautes.

La coopération au centre du modèle internet

Le modèle initial de l'internet comporte une organisation décentralisée et symétrique – non seulement en termes de consommation de bande passante, mais aussi en termes de contact, relation et communication entre machines (Minar & Hedlund, 2001). Le but de l'ARPANET originel était de partager des ressources de calcul sur le territoire américain. Le défi principal auquel cet effort a dû faire face a été l'intégration de différents types de réseaux existants, mais aussi des futures technologies, dans un réseau commun, qui permettrait à chaque hôte d'être un participant égal dans le jeu. Les protocoles et les systèmes sont suffisamment obscurs – et suffisamment spécialisés – pour rendre les failles de sécurité rares et, pour la plupart, négligeables. Si les premières applications dominantes de l'internet, FTP et Telnet, sont client/serveur, les modèles d'usage dans leur ensemble sont symétriques : chaque hôte sur le Net peut se connecter au moyen de FTP ou Telnet à tout autre hôte, et dans ces débuts des mini-ordinateurs et des unités centrales, les serveurs se comportent souvent dans l'économie du réseau en tant que clients. Le système de forums Usenet, qui fait sa première apparition en 1979, influence par la suite certains des exemples les plus réussis de structures de contrôle décentralisées sur le Net (Pfaffenberger, 1996). Les premières visions du Web, depuis 1994, tracent quant à elles un portrait de grand « égalisateur de communications » – un système permettant à tout usager de publier son point de vue au lieu d'être purement et simplement un consommateur de médias (Flichy, 2001).

Le protocole TCP/IP (Transmission Control Protocol/Internet Protocol) illustre bien ce modèle coopératif, avec son principe fondamental de conception de l'internet par le *best effort*, le « meilleur effort » de livraison de paquets : cela signifie que la composition et la structure du réseau internet ne garantit pas qu'un paquet va rejoindre sa destination, mais tout simplement que le réseau « fera de son mieux » pour que cela arrive. Les protocoles de niveau supérieur, tel TCP, créent des connexions fiables en détectant quand un paquet est perdu et en le renvoyant. Le comportement collectif de nombre de connexions TCP individuelles, qui ralentissent de façon indépendante, entraîne une diminution de la saturation au niveau du routeur ; l'algorithme TCP est donc, en fait, une façon pour les différents pairs de gérer une ressource partagée, sans coordinateur central. L'efficacité du protocole TCP à l'échelle de l'internet dans son ensemble requiert, fondamentalement, de la coopération. À chaque utilisateur du réseau, il est demandé de jouer avec les mêmes règles ; toute personne travaillant sur l'internet partage la même motivation : maximiser l'efficacité et optimiser techniquement le dispositif pour construire un réseau fiable, efficace et puissant (Oram, 2001, 2004 ; Taylor & Harrison, 2009). Mais il serait tout à fait possible de « concevoir d'autres protocoles qui ne suivent pas cette équation, et qui vont rudement essayer de consommer plus de bande passante qu'ils ne devraient. Ces protocoles peuvent causer des ravages sur le Net, » explique un développeur (Entretien du 2 octobre 2009).

L'inquiétude croissante que les protocoles hostiles commencent à nuire à l'internet est bien illustrée par la controverse qui s'installe en 1996 autour de la fonctionnalité ajoutée par Netscape à son navigateur, qui donne la possibilité de télécharger plusieurs fichiers en même temps. Les ingénieurs de Netscape découvrent que si on télécharge des images intégrées en parallèle, plutôt qu'une seule à la fois, la page entière se télécharge plus rapidement, ce que les utilisateurs apprécient. Mais une question se pose alors : cette utilisation de bande passante est-elle équitable? Non seulement on force le serveur à envoyer plusieurs images simultané-

ment, mais on multiplie les canaux TCP, et on contourne les algorithmes TCP contre la saturation. La controverse s'apaisera une fois que, Netscape ayant rendu publiques les caractéristiques de son navigateur, on découvre dans la pratique que la stratégie de téléchargement en parallèle ne porte pas indûment préjudice à l'internet. Cependant, elle a révélé une fois de plus la centralité du modèle de coopération et sa fragilité face aux évolutions et à la massification des usages.

La forme d'organisation basée sur la coopération est mise en cause par les usages et leurs modèles économiques, car on assiste à un déplacement vers un modèle où le téléchargement de données acquiert plus d'importance (ne serait-ce que dans les flux de données qui circulent sur le réseau) que la publication d'informations ou leur téléchargement vers l'amont. Cela reflète les usages qui vont devenir dominants ; en particulier (mais pas exclusivement) avec les échanges de contenus culturels échappant aux droits d'auteur (Dauphin & Dagiral, 2005). L'explosion commerciale de l'internet va diriger rapidement une grande majorité du trafic vers le paradigme *downstream* propre à la télévision et aux médias traditionnels ; même si la fabrication de contenus *ad hoc*, liée à la spécificité de chaque requête et de chaque contribution des utilisateurs, reste une première évolution par rapport à ce modèle – une évolution destinée à s'inscrire dans la durée.

Une lente érosion

Le modèle initial de coopération, qui tient, en partie, du mythe, est remis en cause par ses propres limites : il exige un comportement actif de la part des internautes – de tous les internautes. Si dans le premier modèle coopératif, chacun assure la responsabilité de ses connections et de ses échanges, ce modèle révèle bientôt ses limites du point de vue du fonctionnement du réseau et de son « usabilité » pour les internautes. On procède donc à la construction de points de passage obligés, en particulier les fournisseurs d'accès à internet (FAI), et à une régulation et un bridage des transferts de données beaucoup plus strictes – ce qui pousse, à son tour, à l'asymétrisation des flux. Le principe selon lequel si un hôte peut accéder au réseau, tout le monde sur le réseau peut atteindre cet hôte, s'érode de plus en plus à partir du milieu des années 1990.

L'exemple le plus flagrant de cette tendance est le navigateur Web. Ce dernier, comme plusieurs autres applications qui naissent dans les premières phases de la commercialisation de l'internet, se base sur un simple protocole client/serveur : le client amorce une connexion à un serveur connu, en télécharge des données et se déconnecte. Le modèle de téléchargement à sens unique est à ce stade plus simple, bien que souvent moins transparent, et il fonctionne sans que l'utilisateur ait besoin de s'investir dans le processus de configuration. Ce modèle s'avère une façon simple et directe de mettre en place nombre d'applications qui impliquent un service à l'utilisateur, de la navigation du Web, au visionnage des vidéos en *streaming*, auxquelles se rajoutent bientôt des chariots de courses, des transactions de stocks, des jeux interactifs, et beaucoup d'autres « biens ». Les machines qui hébergent un client web ne nécessitent pas, elles, une adresse reconnue ni permanente. Elles n'ont pas besoin d'une connexion permanente à l'internet, ni de gérer les besoins de plusieurs usagers. Elles doivent juste « savoir comment poser une question, et comment écouter et comprendre la réponse » (Entretien du 19 mars 2009 avec un développeur P2P).

Pour maximiser l'efficacité du câblage disponible, les fournisseurs de services à large bande choisissent, quant à eux, de recourir à une bande passante asymétrique. L'installation domestique typique d'une ligne ADSL ou d'un modem câblé est conçue de façon à offrir trois à huit

fois plus de bande passante en téléchargeant des données depuis l'internet qu'en envoyant des données vers le réseau, favorisant ainsi des usages de type client plutôt que de type serveur. La raison pour laquelle ce déséquilibre entre téléchargements vers l'amont et vers l'aval est largement acceptée par le public est liée à la suprématie du World Wide Web parmi les applications Internet ; la plupart des utilisateurs Web n'ont que très rarement besoin d'être plus qu'un client. Même les usagers qui publient leurs propres pages Web ne le font pas, généralement, depuis leur connexion domestique à bande large, mais depuis des serveurs dédiés appartenant à des tiers, tels IT GeoCities ou Exodus. Si dans les premiers jours d'existence du Web la situation était moins claire – la possibilité que chaque usager se dote d'un serveur web personnel n'était pas écartée *a priori* – il devient bientôt clair que le Web commercial comporte en soi des éléments d'asymétrie (beaucoup de clients pour peu de serveurs) et que la plupart des usagers sont, dans ce contexte, bien servis par l'asymétrie de la bande passante. Mais les débuts des applications P2P destinées au partage de fichiers, qui explosent avec Napster en 1999 (Farchy, 2003), mettent à nouveau et radicalement en débat l'approche selon laquelle les usagers finaux exécutent presque exclusivement des opérations de téléchargement vers l'aval, et non vers l'amont.

La lutte contre les spammeurs, les *flamers* et les nouveaux-nés « vandales » du réseau des réseaux montre également la montée en puissance de cette tendance (Brunton, 2013). Au cours de la phase pré-commerciale du réseau, la publicité non sollicitée était généralement reçue avec surprise et indignation. La fin de l'innocence a lieu le 12 avril 1994, le jour où les avocats Laurence Canter et Martha Siegel postent individuellement une publicité sur tous les groupes de discussion Usenet. La messagerie électronique et Usenet comptaient sur la coopération active des individus, et sur leur volonté individuelle et collective de ne pas inonder les ressources communes avec des courriers publicitaires indésirables : c'est ce principe de coopération qui tombe en panne, et cela pose de nouvelles questions quant au manque d'attribution de responsabilité dans l'architecture de l'internet. Puisque n'importe quel hôte peut se connecter à tout autre hôte, et que les connexions sont presque anonymes, les usagers peuvent insérer du spam dans le réseau à tout moment. Commence alors une sorte de « course aux armements » pour essayer de responsabiliser les utilisateurs : la fermeture des relais ouverts pour l'envoi de messages, le suivi des sources de spam sur Usenet, les représailles contre les spammeurs (Everett-Church, 1999).

La diffusion du spam et le fonctionnement de l'algorithme TCP partagent une même caractéristique : ils démontrent la fragilité du fonctionnement durable de l'internet, et la nécessité de coopération que celui-ci implique. Dans le cas du protocole TCP, le système a résisté, et le réseau a été préservé. Dans le cas du spam, cependant, le comportement non coopératif a persisté.

Des clôtures puissantes et controversées

En même temps que la nature coopérative de l'internet se voit menacée, diverses mesures de « clôture » et de barrière se mettent en place : l'augmentation des adresses IP dynamiques, le déploiement toujours plus fréquent de pare-feu, et la popularité de la *Network Address Translation* (NAT ou traduction d'adresse réseau). Le développement de ces nouvelles modalités est entouré par des controverses – ce qui ne les empêche pas de se transformer.

Les utilisateurs lambda ne pouvant pas gérer de manière autonome les risques de sécurité pour leurs machines qui résultent d'une conception symétrique des réseaux, leurs gestionnaires se tournent vers diverses mesures de gestion, qui affectent notamment l'ouverture et la symétrie

du réseau, mais qui semblent être une nécessité structurante pour un internet plus mûr et aux usages plus variés. Les pare-feu se trouvent au point de contact entre le réseau interne et l'internet à l'extérieur. Ils filtrent les paquets, et choisissent quel trafic laisser passer et à qui refuser l'accès. Un hôte protégé de cette façon ne peut plus facilement fonctionner comme un serveur : il ne peut être qu'un client.

Permettre à un hôte sur l'internet de n'être qu'un client, et pas un serveur, est un thème transversal à beaucoup de changements de l'internet après son explosion commerciale. Avec l'augmentation du nombre d'utilisateurs dotés d'une connexion à l'internet par modem, la pratique de donner à chaque hôte une adresse IP fixe devient impraticable, le nombre d'adresses IP n'étant plus suffisant (DeNardis, 2009). L'affectation dynamique des adresses IP prend pied jusqu'à devenir la norme pour de nombreux hôtes sur l'internet, où l'adresse d'un ordinateur particulier peut maintenant changer même une fois par jour. Les fournisseurs de bande passante, de leur côté, trouvent les adresses IP dynamiques utiles pour le déploiement de services toujours disponibles. Le résultat final est que de nombreux hôtes sur l'internet, se déplaçant constamment, ne sont pas facilement accessibles, ce qui affecte, à nouveau, le principe de coopération. Ce phénomène est tout particulièrement un problème pour les applications en pair-à-pair servant des buts tels que la messagerie instantanée ou le partage de fichiers, qui, pour contourner ce problème, doivent désormais construire des répertoires dynamiques des hôtes.

Cette tendance s'accroît ultérieurement quand on commence à ne plus attribuer une adresse internet publique et valide à un hôte, mais à utiliser la NAT pour cacher cette adresse derrière un pare-feu. Un routeur fait du *Network Address Translation* (NAT) (« traduction d'adresse réseau ») lorsqu'il fait correspondre les adresses IP internes non uniques et souvent non routables d'un intranet à un ensemble d'adresses externes uniques et routables. Ce mécanisme permet notamment de faire correspondre une seule adresse externe publique visible sur internet à un ensemble d'adresses d'un réseau privé. Par rapport au type de trafic peer-to-peer, la NAT allie les problèmes des pare-feu et ceux des adresses IP dynamiques : la véritable adresse de l'hôte n'est pas seulement instable, elle n'est plus accessible. Toute communication doit parler un langage relativement simple, que le routeur NAT puisse comprendre, ce qui entraîne une grande perte de flexibilité dans les communications entre applications.

Les pare-feu, les adresses IP dynamiques et la NAT mettent à l'épreuve, chacun(e) avec ses spécificités, le modèle fondamental de l'internet : certaines parties du réseau ne peuvent plus parler de façon totalement libre à d'autres parties. Des outils de sécurité par ailleurs très utiles posent autant d'obstacles sérieux aux modèles de communication directs, symétriques, en peer-to-peer.

Conclusions

Les pare-feu, les IP dynamiques, et la NAT sont nés d'un besoin de sécuriser l'architecture internet et de faire évoluer les instruments de préservation du principe de coopération lui-même, au fur et à mesure que le réseau évoluait et se peuplait d'usagers ; la mise en opération de barrières a sans doute contribué de manière déterminante à amener des millions d'ordinateurs clients sur l'internet, de façon rapide et souple. Ces mêmes technologies ont, par ailleurs, profondément reconfiguré les équilibres de l'infrastructure internet dans son ensemble, en « reléguant » la plupart des ordinateurs au seul statut de clients.

Si la traduction de ce statut en des connexions asymétriques et un fort déséquilibre entre télé-

chargements vers l'amont et vers l'aval est largement tolérée par le public, la raison réside dans le rôle de « killer application » de l'internet que le Web a occupé pendant ces années : la plupart des usagers du Web n'ont que très rarement besoin d'être plus qu'un client. Et si les pratiques d'auto-publication deviennent plus populaires avec l'avènement de l'internet commercial, les usagers passent quand même, pour l'essentiel, la plupart de leur temps en ligne à lire (et télécharger) de l'information, et moins à en publier. Comme on l'a vu, les fournisseurs de services et d'accès internet construisent leur offre en s'appuyant sur cette asymétrie.

Cependant, les applications P2P (Musiani, 2013) mettront à nouveau et radicalement en débat cette approche – comme démontrent, pour ne citer que deux de ses applications les plus connues, le réseau Tor ou la monnaie électronique Bitcoin, où choix architecturaux et choix politiques se mêlent et se recouvrent. Les applications P2P qui jouissent d'un succès considérable depuis le début des années 2000 sont porteuses d'une réalité intermédiaire entre le supposé cas idéal des origines, « tout le monde publie », et l'apparente réalité de l'internet commercial, « tout le monde consomme ». Ces applications rendent très facile la publication de données dont on n'est pas l'auteur, tandis que les machines des utilisateurs sont utilisées comme répétiteurs pour la retransmission des données qu'elles reçoivent. Le design du réseau qui repose sur l'existence d'un nombre limité d'auteurs, et l'asymétrie de bande passante comme principe d'optimisation, se voient profondément remis en discussion par ce développement. Un nombre important de réseaux se trouve surchargé ; la dynamique de la « course aux armements » se répète ; dans la pratique, le P2P « pur » ou intégral – celui qui utilise une structure de réseau complètement décentralisée – n'est presque jamais utilisé, au profit de solutions hybrides ou de compromis.

La coexistence de différents niveaux de centralisation, hiérarchisation et coopération - dans un « ballet entre programmateurs, logiciels et utilisateurs » (Abbate, 2012) - est, une fois de plus, démontrée. Les tendances à la concentration, à la centralisation, et à la prédominance de données et de processus de plus en plus éloignés des *marges* du réseau (Moglen, 2010), ne peuvent aujourd'hui être mises en doute. Cependant, il reste remarquable - en dépit de la montée en puissance des modèles anti-coopératifs - que la capacité de l'internet (ou des internets, car le pluriel peut désormais sembler nécessaire) à servir un terrain fertile pour la production de modèles alternatifs reste forte. L'architecture actuelle du réseau des réseaux, bien que parsemée d'asymétries et de clôtures, peut encore être mise au service de projets qui cherchent à contourner ces barrières - pour proposer des alternatives aux infrastructures centralisées dominantes aujourd'hui (Egyedi & Mehos, 2012), sans pour autant exclure toute hiérarchie.

Références

Abbate, J. (2012). L'histoire de l'internet au prisme des STS. *Le temps des médias*, 18: 170-180.

Abbate, J. (1999). *Inventing the Internet*. Cambridge, MA, The MIT Press.

Brunton, F. (2013). *Spam: A Shadow History of the Internet*. Cambridge, MA, The MIT Press.

Dauphin, F. & E. Dagiral (2005). P2P: From File Sharing to Meta-information Pooling?, *Communications & Strategies*, 59 (3) : 35-51.

DeNardis, L. (2009). *Protocol Politics: The Globalization of Internet Governance*. Cambridge, MA: The MIT Press.

Egyedi, T. M. & D. C. Mehos (eds., 2012). *Inverse Infrastructures: Disrupting Networks From Below*. Cheltenham, UK : Edward Elgar Publishing.

Everett-Church, R. (1999). The Spam That Started It All, *Wired*, April 2009, http://www.wired.com/politics/law/news/1999/04/19098

Farchy, J. (2003), *Internet et le droit d'auteur : la culture Napster*. Paris : CNRS Editions.

Flichy, P. (2001). *L'imaginaire d'internet*. Paris: La Découverte.

Minar, N. et Hedlund, M. (2001). A network of peers – Peer-to-peer models through the history of the Internet. In A. Oram (Ed.), *Peer-to-peer: Harnessing the Power of Disruptive Technologies*, 9-20. Sebastopol, CA: O'Reilly.

Moglen, E. (2010). Freedom In The Cloud : Software Freedom, Privacy and Security for Web 2.0 and Cloud Computing. ISOC Meeting, New York Branch, 5 February 2010.

Musiani, F. (2013). *Nains sans géants. Architecture décentralisée et services internet*. Paris : Presses des Mines.

Musiani, F. & Schafer, V. (2011). Le modèle internet en question (années 1970-2010). *Flux*, 85-86 (3-4): 62-71.

Oram, A. (2004). From P2P to Web Services: Addressing and Coordination, *O'Reilly XML.com*, http://www.xml.com/pub/a/2004/04/07/p2p-ws.html

Oram, A. (Ed.) (2001). *Peer-to-peer: Harnessing the Power of Disruptive Technologies*. Sebastopol, CA: O'Reilly.

Pfaffenberger, B. (1996). If I Want It, It's OK: Usenet and the (Outer) Limits of Free Speech. *The Information Society*, 4(12) : 365-373. http://pfaff.sts.virginia.edu/bphome/docs/pdf/usenet.pdf

Taylor, I. & Harrison, A. (2009). *From P2P to Web Services and Grids: Evolving Distributed Communities. Second and Expanded Edition.* London: Springer-Verlag.