La gouvernance mondiale

En l'espace de quelques années, le contrôle politique et économique du réseau a été à l'origine de nombreuses tensions internationales. Les révélations d'Edward Snowden ont aussi modifié en profondeur la perception internationale des rapports de forces sur Internet et pourraient être à l'origine de changements majeurs dans son architecture et sa gouvernance [1].

Bernard BENHAMOU, secrétaire général de l'Institut de la souveraineté numérique, ancien conseiller de la délégation française au Sommet des Nations unies sur la société de l'information


© DR

Les instruments fondamentaux de la souveraineté sont devenus indiscernables des outils de la puissance technologique. L'architecture et la gouvernance du réseau sont aujourd'hui le nouveau théâtre des conflits internationaux entre Etats, mais aussi entre acteurs industriels.

Qu'y a-t-il, en premier lieu, derrière la « gouvernance » de l'Internet ? Celle-ci a souvent été décrite comme la concertation des acteurs impliqués dans la gestion technique et politique du réseau mondial [2]. C'est l'ICANN [3], l'association de droit californien créée par l'administration Clinton en 1998 pour gérer les noms de domaine sur Internet, qui a cristallisé les tensions. En effet, les pouvoirs d'organisation de la cartographie mondiale de l'Internet conférés à l'ICANN incluent des prérogatives de souveraineté dont les Etats ne pouvaient être privés dans la durée, en particulier pour la gestion des extensions dédiées aux pays. C'est en partie pour tenter de faire évoluer le mode de gouvernance des noms de domaine que les Nations unies ont organisé le Sommet mondial sur la société de l'information (SMSI). Le texte adopté à l'issue du Sommet, l'Agenda de Tunis, n'a cependant pas permis de faire évoluer le statu quo. Récemment encore, lors de la Conférence mondiale sur les télécommunications (WCIT 2012), de nombreux pays émergents et en particulier la Chine, la Russie et les Emirats arabes unis ont souhaité que la gouvernance de l'Internet échappe aux seuls Etats-Unis et soit placée sous le contrôle exclusif des gouvernements. L'Union européenne a refusé de signer cette proposition, qui aurait pu avoir des conséquences politiques et économiques imprévisibles en raison de la « fragmentation » de l'Internet en une série d'îlots, et qui remettait en cause l'un des principes fondamentaux de l'architecture du réseau : la neutralité de l'Internet.

Les multiples conséquences de l'affaire Snowden

Ce n'est cependant qu'à l'issue des révélations d'Edward Snowden que les autorités américaines ont décidé de remettre en cause le contrat liant l'ICANN au Département du commerce des Etats-Unis [4].

Face à l'essor des usages numériques, les révélations d'Edward Snowden sur les pratiques de surveillance mises en place par la NSA ont permis à l'ensemble des opinions publiques de prendre conscience de la vulnérabilité des individus face aux services mis en place sur Internet et qui pouvaient, dans une logique inversée, devenir un risque pour eux-mêmes, pour leurs libertés, mais aussi pour la protection des données sensibles des entreprises.

Avec ces révélations, l'ensemble des acteurs de l'Internet ont découvert, tout comme les opinions publiques, que leurs infrastructures étaient devenues « transparentes », pour les agences gouvernementales. Ces révélations ont créé les conditions d'un « schisme » entre les industriels de l'Internet et le gouvernement américain. En effet, si l'affaire Snowden pose, à juste titre, des questions liées aux risques démocratiques issus de la surveillance

(1) « Architecture et gouvernance de l'Internet », B. Benhamou, revue *Esprit*, mai 2006.

(2) « *Par* "gouvernance de l'Internet", *il faut entendre l'élaboration et l'application par les Etats, le secteur privé et la société civile, dans le cadre de leurs rôles respectifs, de principes, normes, règles, procédures de prise de décisions et programmes communs propres à modeler l'évolution et l'utilisation de l'Internet* », extrait du rapport du Groupe de travail sur la gouvernance de l'Internet des Nations unies, juin 2005.

(3) L'Internet Corporation for Assigned Names and Numbers (ICANN) assure la gestion du Domain Name System (DNS) qui constitue l'« annuaire mondial » des ressources sur Internet et permet de convertir des adresses IP numériques en noms de domaine intelligibles.

(4) « U.S. to Cede Its Oversight of Addresses on Internet », *New York Times*, 14 mars 2014.

de l'Internet après Snowden

La fragilisation des dispositifs cryptographiques constitue une menace sur l'ensemble des dispositifs qui reposent sur la confidentialité des échanges.

de masse, c'est la remise en cause de la confidentialité des données des entreprises qui a constitué le volet le plus inquiétant pour l'ensemble des acteurs économiques. Ainsi, les géants de la Silicon Valley ont fait savoir à Barack Obama à quel point la NSA pouvait remettre en cause la clef de voûte de l'Internet : la confiance de ses usagers[5].

Par la suite, d'autres industriels des technologies ont été « pris en étau » entre leurs obligations vis-à-vis des autorités américaines (en particulier celles qui découlent du Patriot Act) et les conséquences des actions de la NSA sur les marchés émergents[6]. La Chine a ainsi exclu de ses marchés publics certains produits phares des industries américaines des technologies[7]. Cela touche aussi les marchés européens, ainsi l'Allemagne a fait savoir qu'elle comptait exclure de ses marchés publics les entreprises contractantes de la NSA[8].

Impact industriel, impacts socioculturels

Les révélations d'E. Snowden ont par ailleurs gravement ébranlé, auprès de l'opinion, certains préjugés :

- la volonté des acteurs technologiques de protéger les données de leurs usagers serait un invariant économique ;
- la surveillance ne concernerait que des enquêtes et des individus isolés et pas l'ensemble des citoyens d'un Etat ;
- seuls les contenus directement issus des usagers devraient être protégés (les métadonnées issues de la navigation des internautes seraient « moins sensibles » que le contenu des échanges eux-mêmes) ;
- les entreprises auraient les moyens de protéger leurs données sensibles des intrusions issues des Etats ou de hackers malveillants ;
- aucun Etat ne prendrait le risque de fragiliser à lui seul Internet.

Les conséquences sociales et politiques à long terme de cette affaire commencent à peine à être mesurées. Certains préjugés sur la nature des échanges sur les réseaux sociaux commencent aussi à être remis en cause. Les personnes contactées, dans le cadre de l'étude du Pew Research[9], déclarent être réticentes à discuter de l'affaire Snowden et de la surveillance de la NSA dans les médias sociaux. Celles qui hésitent à en parler autour d'elles ne se tourneront pas vers ces médias pour partager leur opinion sur ces sujets. Cette forme d'autocensure faisait même l'objet des inquiétudes du créateur du Web, Tim Berners-Lee[10] : « *C'est la méfiance infusée depuis le niveau politique, jusqu'à l'autocensure des citoyens ordinaires, qui menace l'ouverture du Web. C'est une plus grande menace que la censure elle-même. Savoir que la NSA peut casser les systèmes commerciaux de chiffrement pourrait avoir pour conséquence de créer des réseaux comme le* "grand Intranet chinois"… »

L'une des réponses proposées par E. Snowden consiste à rendre plus difficile l'action des agences

> ***« La mise en place, par les Etats-Unis, des programmes de surveillance de masse crée une opportunité pour l'Europe de devenir l'artisan d'un accord transatlantique qui établirait les principes fondamentaux du développement de l'Internet dans les démocraties. »***

(5) « Tech executives to Obama : NSA spying revelations are hurting business », *Washington Post*, 17 décembre 2013.

(6) « American and Chinese companies are getting caught in the crossfire of the brewing cyber war », *The Diplomat*, 25 août 2014.

(7) « Chinese government banned Microsoft Office 365 due to security concerns : Should American IT firms be worried ? », *Tech Times*, 2 juillet 2014 et « China Said to Exclude Apple From Procurement List », *Bloomberg News*, 8 août 2014.

(8) « Germany blocks NSA-linked IT firms from state contracts », *Wired UK*, 21 mai 2014.

(9) « Social Media and the "Spiral of Silence" », Etude Pew Research, août 2014.

(10) www.wired.co.uk/news/archive/2014-02/06/tim-berners-lee-reclaim-the-web.

de renseignement dans le monde, en utilisant massivement des technologies de chiffrement. Cet objectif se heurte pour l'instant à des difficultés d'ordre ergonomique, les outils de chiffrement n'étant maîtrisables que par les « technophiles » : de nouveaux outils accessibles à tous devront être développés mais ils ne pourront réellement se démocratiser que s'ils deviennent aussi ergonomiques que les services les plus utilisés sur Internet.

Le rôle clé des normes et standards

L'une des conséquences de l'affaire Snowden aura été de montrer qu'au-delà de la surveillance des citoyens mise en place auprès des grands acteurs industriels de l'Internet, les normes et les technologies de sécurité elles-mêmes avaient été altérées ou corrompues. Cela a par exemple été le cas avec le programme Bullrun[11] de la NSA, dont les ingénieurs ont volontairement altéré la confidentialité des échanges en introduisant, dans les dispositifs de chiffrement[12], des « *portes dérobées* » ou « *backdoors* »[13], qui permettaient aux services de la NSA de déchiffrer les messages. Cette fragilisation des dispositifs cryptographiques constitue une menace sur l'ensemble des dispositifs qui reposent sur la confidentialité des échanges (qu'il s'agisse du commerce électronique, des échanges de données sensibles pour les Etats ou de la protection des secrets industriels…). Dans un autre domaine crucial pour les démocraties, la suspicion née de ces révélations pourrait aussi être à l'origine de la remise en cause de la sincérité des scrutins menés grâce à des dispositifs de votes électroniques.

Les révélations d'Edward Snowden ont été à l'origine de la remise en question du fonctionnement des organismes chargés d'élaborer les normes et standards de l'Internet (en particulier dans le domaine de la sécurité). Il est ainsi apparu nécessaire de protéger d'interventions extérieures les technologies qui constituent les socles de la sécurité et de la confiance sur Internet. Ainsi, l'indépendance des organismes chargés des normes et standards de l'Internet devra être assurée, en particulier lorsqu'il est question des dispositifs qui assurent la sécurité des échanges. Des mesures internationales devront aussi être prises pour éviter que les organismes chargés d'élaborer les normes et standards de sécurité sur Internet ne soient couplés (ou dépendants) des agences de renseignement[14].

Si Internet a été à même de se développer sans connaître de « crises de croissance » et qu'il a montré sa résilience à de nombreuses attaques sur ses infrastructures, il ne pourrait pas résister une « crise de confiance » globale[15]. C'est pour lutter contre cette crise de confiance que les organismes chargés de la régulation technique de l'Internet ont souhaité intervenir dans ce débat hautement politique de la surveillance de masse[16]. Ainsi, l'Internet Engineering Task Force, groupe informel de l'ensemble des ingénieurs chargés d'élaborer les normes et standards de l'Internet, a émis une « loi technique » qui décrit la surveillance de masse comme une attaque contre le réseau[17]. Cependant, pour que cette « loi technique » puisse s'imposer auprès de l'ensemble des acteurs technologiques et surtout des agences de renseignement, il conviendra d'élaborer des mécanismes internationaux de contrôle et de limitation des actions des Etats en matière de surveillance sur Internet. En effet, comme l'ont démontré en France les débats sur la loi sur le renseignement, ainsi que les demandes récentes du gouvernement américain d'intégrer des « *portes dérobées* » dans les dispositifs mis à disposition du public, les conséquences des modifications qui portent sur l'architecture de l'Internet peuvent avoir des conséquences durables. Et des deux côtés de l'Atlantique, ces conséquences ont le plus souvent été ignorées par les législateurs eux-mêmes.

La situation nouvelle créée par la

© MIKE LEE, THE OPTE PROJECT, LICENCE CC

Si Internet a été à même de se développer sans connaître de « crises de croissance » et qu'il a montré sa résilience à de nombreuses attaques sur ses infrastructures, il ne pourrait pas résister une « crise de confiance » globale.

(11) www.theguardian.com/commentisfree/2013/sep/05/government-betrayed-internet-nsa-spying.

(12) Plus précisément dans les systèmes de génération des nombres aléatoires.

(13) « The internet after Snowden : New threat model army », *The Economist*, 11 novembre 2013.

(14) « Panel recommends NIST declare independence from NSA », FCW, 14 juillet 2014.

(15) « Architecture et Gouvernance de l'Internet », Bernard Benhamou, revue *Esprit*, mai 2006.

(16) « Montevideo Statement on the Future of Internet Cooperation », ICANN, 7 oct 2013.

(17) « Pervasive Monitoring Is an Attack », RFC 7258 IETF, mai 2014.

(18) « An online Magna Carta : Berners-Lee calls for bill of rights for web », *The Guardian*, 12 mars 2014.

(19) Des propositions similaires commencent à être évoquées à l'échelle des seuls Etats-Unis et pourraient être élargies dans le cadre d'un accord transatlantique. Voir « How to Save the Net : A CDC for Cybercrime », *Wired*, 19 août 2014.

mise en place, par les Etats-Unis, de leurs programmes de surveillance de masse crée une opportunité pour l'Europe de devenir l'artisan d'un accord transatlantique qui établirait les principes fondamentaux du développement de l'Internet dans les démocraties.

Vers un traité transatlantique ?

Dans cette perspective, Tim Berners-Lee a déjà réclamé que soit créée une Constitution mondiale pour l'Internet [18] qui pourrait placer les principes fondamentaux de l'Internet au-dessus des lois nationales, afin que les Etats ne puissent unilatéralement modifier Internet à des fins économiques ou politiques. Ces principes fondamentaux étant l'ouverture, l'interopérabilité et la neutralité de l'Internet, ainsi que l'interdiction pour les Etats de prendre des mesures portant atteinte au fonctionnement du réseau pour l'ensemble de ses utilisateurs. La création d'un accord transatlantique permettrait aussi de fonder une opposabilité juridique internationale aux actions technologiques des Etats qui mettraient en péril le bon fonctionnement et la sécurité du réseau. Il pourrait ainsi, dans un second temps, être élargi à d'autres régimes démocratiques. Ce traité pourrait être à l'origine de la mise en place d'un observatoire mondial chargé du contrôle et de la protection de l'Internet [19].

La gouvernance de l'Internet ne doit plus être uniquement envisagée comme une régulation « a posteriori » des édifices technologiques mis en place par les industriels, mais bien comme une co-élaboration des normes et standards qui devront être intégrés « a priori » au cœur même de ces technologies. La souveraineté du peuple doit s'exercer sur l'ensemble des technologies qui auront un impact sur les évolutions culturelles, sociales, économiques et politiques de nos sociétés. ●

Un paysage technologique en mutation

Dans un premier temps, les usagers des technologies ont bénéficié de la décentralisation de la puissance de traitement en passant d'ordinateurs centraux connectés à des terminaux, puis à des micro-ordinateurs, et désormais nous assistons à la « recentralisation » d'importantes masses de données via les technologies de l'informatique en « nuage » (*cloud*), et bientôt la montée en puissance de services associés aux objets connectés. C'est ainsi la nature même de la gouvernance du réseau qui sera amenée à évoluer. En effet, les informations qui transitent sur Internet sont aujourd'hui créées par les ordinateurs connectés (donc par des humains) ; dans un avenir proche, ce sont les capteurs et les objets connectés qui généreront la majorité du trafic sur les réseaux [1].

Vers un « droit au silence des puces »

Face à l'introduction de ces objets connectés dans l'environnement des citoyens, de nouvelles mesures devront être mises en place à l'échelle internationale pour éviter qu'ils ne deviennent à la fois de nouveaux vecteurs d'attaques informatiques sur les infrastructures critiques dans le domaine des transports, de la santé ou encore de l'énergie [2]. Le fonctionnement des objets connectés qui nous entourent devra aussi être examiné dans la durée, depuis leur conception jusqu'à leur destruction. En effet, à mesure que nos objets quotidiens seront connectés et qu'ils recueilleront des informations, ils constitueront aussi des cibles potentielles pour de nouvelles formes d'attaques informatiques. Or, pour la plupart, ces objets, à la différence des ordinateurs ou des terminaux mobiles, ne font pas encore systématiquement l'objet de mises à jour de sécurité. Qu'il s'agisse du recueil d'informations médicales personnelles voire de prise de contrôle à distance, la sécurité des objets devra faire l'objet d'une attention particulière. Parmi les mécanismes de sécurité des objets connectés, deux d'entre eux devront faire l'objet de mesures d'encadrement :

- l'obsolescence ou la mort programmée des objets, en particulier pour ceux liés à des fonctions critiques et qui ne seraient plus « supportés » en termes de sécurité par leurs constructeurs ;
- le droit au silence des puces : la possibilité qui devra être donnée à l'usager de faire « taire » les puces et autres dispositifs interrogeables à distance afin qu'ils ne puissent communiquer des informations sans son consentement.

Le concept de « droit au silence des puces » a été élaboré en 2006 [3] dans le but de permettre aux usagers de maîtriser les informations issues des puces à radiofréquences (RFID), pour éviter de nouvelles formes de captation frauduleuse d'informations (*skimming*) par des tiers. Ce principe a aussi pour objectif de placer le citoyen usager en situation de maîtrise des données. Il implique que soient inclus, dès la conception des objets, des dispositifs de désactivation/réactivation associés à des dispositifs de chiffrement pour les données les plus sensibles, comme les données médicales ou relatives à la sécurité des personnes.

Les nouvelles générations d'objets connectés devraient être à l'origine de changements majeurs dans les formes culturelles, sociales et politiques de nos sociétés. Ces mutations ne sauraient être induites par les seuls industriels des technologies. Les citoyens doivent participer à la construction des réseaux en tant que « co-architectes ». En plus de leur impact économique, les mesures qui permettront de rendre intelligibles et maîtrisables les données et les services de l'Internet revêtent un caractère politique et stratégique pour l'ensemble des sociétés démocratiques.

(1) « [...] *Le taux de croissance du trafic est encore de 40 % par an, ce qui équivaut à un quasi-doublement tous les deux ans. La montée en puissance de "l'Internet des objets" pourrait en outre donner un essor accru à cette expansion* [...] » ; étude annuelle 2014 du Conseil d'Etat, « Le numérique et les droits fondamentaux ».

(2) « The CIA Fears the Internet of Things », Defense One, 24 juillet 2014.

(3) Ce concept a été introduit dans le texte « Architecture et gouvernance de l'Internet » (revue *Esprit*, Bernard Benhamou, mai 2006), puis formalisé dans le texte « Les mutations économiques, sociales et politiques de l'Internet des objets » (Bernard Benhamou, « Cahiers de la Documentation française », décembre 2012).

B. B.