LES PERSPECTIVES DE LA GOUVERNANCE MONDIALE DE L'INTERNET APRES SNOWDEN

BERNARD BENHAMOU

Enseignant sur la gouvernance de l'Internet à l'Université Paris I – Panthéon Sorbonne.

Ancien délégué interministériel aux usages de l'Internet et conseiller de la délégation française au Sommet des Nations Unies sur la société de l'Information

---

En l'espace de quelques années, les instruments fondamentaux de la souveraineté sont devenus indiscernables des outils de la puissance technologique. L'architecture et la gouvernance du réseau sont devenues le nouveau théâtre des conflits internationaux entre États mais aussi entre les acteurs industriels. De nouvelles tensions internationales liées à la volonté de contrôle politique du réseau prennent appui sur l'architecture et la gouvernance de l'Internet. De plus, les révélations d'Edward Snowden sur l'étendue des programmes de surveillance de la NSA, si elles ont suscité de légitimes inquiétudes auprès des citoyens, et commencent à voir d'importantes conséquences industrielles pour l'ensemble des acteurs de l'Internet. En effet, en remettant en cause la confidentialité des échanges sur Internet, les pratiques de la NSA ont modifié profondément la perception de la sécurité et de la vie privée sur Internet. L'affaire Snowden pourrait aussi être à l'origine des changements majeurs dans l'architecture et dans la gouvernance mondiale de l'Internet[1]. En effet, le Gouvernance de l'Internet ne doit plus être uniquement envisagée comme une régulation « a posteriori » des

---

[1] *Architecture et Gouvernance de l'Internet* (B. Benhamou, Revue Esprit, mai 2006)
http://www.netgouvernance.org/ArchitectureEsprit.pdf

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. Ces évolutions devront aussi s'accompagner d'une meilleure prise en compte par les États des évolutions technologiques qui sous-tendent la Gouvernance mondiale de l'Internet afin de préserver les principes qui ont permis le développement de l'Internet.

UNE GOUVERNANCE MONDIALE SOUS HAUTE SURVEILLANCE

La gouvernance de l'Internet a souvent été décrite comme la concertation des acteurs impliqués dans la gestion technique et politique du réseau mondial[2]. Cependant, depuis la création de l'organisation chargée de la gestion des noms de domaines sur Internet, c'est essentiellement l'organisation des infrastructures critiques des noms de domaine sur Internet qui a donné lieu à des tensions internationales[3]. C'est l'ICANN[4], l'association de droit californien créée par l'administration Clinton en 1998 pour gérer les noms de domaine sur Internet, qui a cristallisé ces tensions entre les États. En effet, les pouvoirs d'organisation de la cartographie mondiale de l'Internet conférés à l'ICANN incluent des prérogatives de souveraineté dont les États ne pouvaient être privés dans la durée en particulier pour la gestion des extensions dédiées aux pays ou ccTLD (comme .fr , .de, .ru, .jp…). L'ICANN a en effet depuis sa création prôné un statu quo favorable aux États-Unis. La structure qui au sein de l'ICANN est chargée de valider l'ensemble des extensions de l'Internet (IANA) est jusqu'à ce jour liée par un contrat avec le Département du Commerce des États-Unis. De plus, le rôle politique mais aussi le fonctionnement économique de l'ICANN font encore l'objet de nombreuses controverses.

---

[2] *« Par "Gouvernance de l'Internet" il faut entendre l'élaboration et l'application par les États, 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 Nation unies, juin 2005) http://www.wgig.org/docs/WGIGREPORT.pdf

[3] *Internet et souveraineté : la gouvernance de la Société de l'Information* (B. Benhamou et L. Sorbier, Politique Étrangère - 2006) http://ifri.org/files/politique_etrangere/PE_3_2006_Benhamou.pdf

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

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 de 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 Émirats arabes unis, ont souhaité que la gouvernance de l'Internet échappe aux seuls États-Unis et soit placée sous le contrôle exclusif des gouvernements. L'Union européenne avait alors 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 remettait en cause l'un des principes fondamentaux de l'architecture du réseau : la Neutralité de l'Internet.

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 États-Unis[5]. Il est à noter que l'affaire Snowden et les nombreux programmes de surveillance de la NSA qu'elle a permis de mettre au jour, n'ont à aucun moment été liés aux prérogatives de l'ICANN. Ces révélations sur l'étendue des mesures de surveillance de la NSA ont été à l'origine de la plus importante crise de la gouvernance mondiale de l'Internet, et elles ont démontré que l'attention portée à l'ICANN ne devait pas occulter les autres sujets de gouvernance mondiale, en particulier les normes et standards de l'Internet (actuellement gérés par l'Internet Engineering Task Force) dont le rôle politique aura été mis en relief à l'issue de l'affaire Snowden.

UN PAYSAGE TECHNOLOGIQUE EN MUTATION

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 et pour leurs libertés. L'affaire Snowden est ainsi apparue comme un rappel à la lucidité pour les citoyens et les organisations dans la gestion des données personnelles et dans la protection des données sensibles des entreprises. Suivant les études du CRÉDOC[6], avant même l'affaire Snowden, le premier sujet

[5] *U.S. to Cede Its Oversight of Addresses on Internet* (New York Times, 14/03/2014) http://nyti.ms/1pib1Xg

[6] *La diffusion des technologies de l'information et de la communication dans la société française* (Rapport du CREDOC juin 2012 réalisé à la demande du Conseil Général de l'Economie, de l'Industrie, de l'Energie et des Technologies

d'inquiétudes des internautes reste le risque d'atteinte aux données personnelles. 86 % des mobinautes français souhaitent pouvoir interdire la transmission de leur géolocalisation à des entreprises commerciales.

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 » et bientôt la montée en puissance de services associés aux capteurs et aux objets. Avec ces changements de dispositifs technologiques c'est la nature même de la gouvernance du réseau qui sera amenée à évoluer. En effet, si pour l'essentiel, les informations qui transitent sur Internet sont aujourd'hui créées par les ordinateurs connectés (et donc par des opérateurs humains), dans un avenir proche ce sont les capteurs et les objets connectés qui généreront la majorité du trafic sur les réseaux[7]. La capacité qui sera donnée aux citoyens de maîtriser ces données pourrait devenir l'une des caractéristiques les plus cruciales de l'architecture informationnelle de nos sociétés et donc de sa gouvernance.

Comme l'ont déjà été les réseaux sociaux ou les moteurs de recherche, 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 sociales et politiques ne sauraient être induites par les seuls industriels des technologies. Les citoyens doivent en effet participer à la construction des réseaux non pas en tant qu'utilisateurs mais bien 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.

(CGEIET) et de L'Autorité de Régulation des Communications Electroniques et des Postes (ARCEP))*http://www.arcep.fr/uploads/tx_gspublication/rapport-credoc-diffusion-tic-2012.pdf*

[7] « *La croissance combinée du nombre d'utilisateurs d'internet et des débits de connexion a conduit à une explosion du volume des données transitant sur les réseaux. En 2012, le trafic mensuel a été de 43 exaoctets par mois, c'est-à-dire 43 milliards de milliards d'octets (1018) ; c'est 20 000 fois plus qu'en 1996. 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, les données transmises par les objets connectés s'ajoutant à celles issues des activités des internautes humains.* » étude annuelle 2014 du Conseil d'Etat *: Le numérique et les droits fondamentaux (http://www.ladocumentationfrancaise.fr/rapports-publics/144000541-etude-annuelle-2014-du-conseil-d-etat-le-numerique-et-les-droits-fondamentaux)*

Données, métadonnées… mégadonnées[8]

Les services numériques sont désormais « enchâssés » dans des architectures logicielles qui leur permettent de devenir intelligibles à l'ensemble des usagers de l'Internet. Ainsi, des données qui n'étaient accessibles qu'à un petit nombre de professionnels peuvent « prendre sens » auprès du grand public. C'est en particulier le cas des données liées à la géolocalisation et plus généralement des données géographiques. En l'espace de quelques années les systèmes d'information géographique qui étaient réservés aux seuls professionnels ont été progressivement remplacés par des systèmes de géolocalisation qui sont utilisés quotidiennement par plusieurs milliards d'individus… et permettent à leur tour de créer des services dans l'ensemble des secteurs de l'activité humaine.

Ces architectures, ces « cathédrales logicielles » reposent aussi sur des données de description des données (ou métadonnées) qui sont essentielles au traitement des informations et peuvent parfois représenter une valeur économique plus importante encore que la donnée dont elles sont issues. Ainsi, Kenneth Cukier[9] décrivait en ces termes l'importance du traitement des métadonnées pour l'ensemble des organisations : *« L'innovation et la création de valeur proviennent désormais de nouvelles formes de « re-structuration » des informations, liées au développement de « l'information sur les informations » ou « métadonnées ». Celles-ci permettent aux organisations de ré-organiser leurs réseaux plus facilement afin d'effectuer de nouvelles tâches, et cela signifie pour ces organisations accroître leur capacité d'apprendre en permanence et ainsi de s'adapter aux changements ».*

Cependant, l'un des enseignements de l'affaire Snowden aura été de montrer à quel point ces métadonnées générées par les plateformes de services sur Internet, peuvent être plus révélatrices des individus que le contenu même des messages échangés. En effet, la puissance de traitement dont disposent ces plateformes et les algorithmes en permanence améliorés pour tirer parti de ces vastes collections de données permettent d'interpréter les comportements des utilisateurs ainsi que leurs préférences au point de prédire certaines de leurs actions. Ces algorithmes deviendront d'autant plus

---

[8] *Ne dites plus "big data", mais "mégadonnées"* (Le Point, 22/08/2014) http://www.lepoint.fr/high-tech-internet/ni-dites-plus-big-data-mais-megadonnees-22-08-2014-1855721_47.php

[9] *Report of the 2007 Rueschlikon Conference on Information Policy* par Kenneth Cukier http://www.cukier.com/writings/Rueschlikon2007-infogov-cukier.pdf aussi coauteur de *Big data, la révolution des données est en marche* par Kenneth Cukier et Viktor Mayer-Schonberger (Lafont février 2014)

cruciaux qu'ils s'appliquent à des services intégrés à chacune de nos activités quotidiennes, via les terminaux mobiles qui deviennent en quelque sorte nos « exo-cerveaux » et cela avant même que de nouvelles générations d'objets connectés ne soient à même de transformer de nouveaux secteurs stratégiques de nos économies comme l'énergie, les transports ou encore la santé…

LES CONSEQUENCES DE L'AFFAIRE SNOWDEN SUR LA GOUVERNANCE DE L'INTERNET

La découverte de l'étendue des données collectées par la NSA auprès des géants de l'Internet via le programme PRISM a constitué un « séisme » pour les opinions publiques et aussi pour l'ensemble des acteurs de l'Internet. Ceux-ci ont en effet découvert que leurs infrastructures étaient devenues « transparentes » pour les agences gouvernementales. Pour la première fois depuis la création de l'Internet, 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 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[10]. Face aux risques industriels que les révélations des pratiques de surveillance mettaient en lumière, Mark Zuckerberg, le PDG de Facebook, déclarait même : « *Le gouvernement américain est devenu une menace pour l'Internet…*[11] ».

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[12]. La Chine a ainsi exclu de ses marchés publics

---

[10] *Tech executives to Obama: NSA spying revelations are hurting business* (Washington Post 17/12/2013) http://wapo.st/1kfMSAZ

[11] Editorial de Mark Zuckerberg posté sur Facebook le 13/03/2014 http://on.fb.me/1nVf2Cc

[12] American and Chinese companies are getting caught in the crossfire of the brewing cyber war (The Diplomat, 25 août 2014).
http://thediplomat.com/2014/08/casualties-of-cyber-warfare/

certains produits phares des industries américaines des technologies[13]. Les conséquences industrielles de l'affaire Snowden touchent aussi les marchés européens des technologies, ainsi l'Allemagne a fait savoir qu'elle comptait exclure de ses marchés publics les entreprises contractantes de la NSA[14].

Des conséquences industrielles… aux impacts socioculturels

La notion de surveillance de masse est devenue une réalité pour l'ensemble des opinions publiques mondiales. Au-delà de l'appropriation individuelle du fonctionnement des services et des technologies à des fins sociales, culturelles ou professionnelles, c'est aussi l'appropriation collective de ces technologies et donc la capacité de nos sociétés à édifier une architecture numérique conforme à leurs principes et à leurs valeurs qui sera déterminante pour l'évolution de nos sociétés, or c'est précisément cette capacité d'appropriation collective qui est remise en cause par l'affaire Snowden. Les révélations de l'ancien contractant de la NSA ont en effet démontré à l'ensemble des opinions publiques que certains préjugés avaient gravement été ébranlés ;

- 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 État,
- 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 États ou de hackers malveillants,
- Aucun État ne prendrait le risque de fragiliser à lui seul l'ensemble de l'Internet.

---

[13] *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)
http://www.techtimes.com/articles/9464/20140702/chinese-government-banned-microsoft-office-365-due-to-security-concerms-should-american-it-firms-be-worried.htm#ixzz3HIN9LrEZ
http://www.bloomberg.com/news/2014-08-06/china-said-to-exclude-apple-from-procurement-list.html

[14] *Germany blocks NSA-linked IT firms from state contracts* (Wired UK, 21 mai 2014)
http://www.wired.co.uk/news/archive/2014-05/21/german-contracts-nsa

Les conséquences sociales et politiques à long terme de l'affaire Snowden commencent à peine à être mesurées. Déjà, certains préjugés sur la nature des échanges sur les réseaux sociaux commencent à être remis en cause. Ainsi, contrairement à la perception commune, les médias sociaux semblent être moins à même de permettre l'échange d'opinions, surtout lorsque ces opinions paraissent être en désaccord avec celles des personnes proches. Ainsi, les personnes contactées, dans le cadre de la récente étude du Pew Research[15] déclarent être réticentes à discuter de l'affaire Snowden et de la surveillance de la NSA dans les médias sociaux, plutôt que d'en discuter en personne. Ainsi, les personnes qui hésitent à en parler autour d'elles ne se tourneront encore moins vers les médias sociaux pour partager leur opinion sur ces sujets qu'ils jugent sensibles. Cette forme d'autocensure faisait même l'objet des inquiétudes du créateur du web, Tim Berners-Lee[16] : *« 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'un des réponses proposées par Edward Snowden consiste à rendre plus difficiles les travaux de surveillance des agences de renseignement dans le monde en utilisant massivement des technologies de chiffrement dans le cadre des échanges des internautes. Il est à noter que cet objectif se heurte pour l'instant à des difficultés d'ordre ergonomique en effet jusqu'à une période récente, les outils nécessaires au chiffrement n'étaient maîtrisables que par la fraction la plus « technophile » des internautes. Or s'il s'avère nécessaire de diffuser plus largement cette culture de la sécurité renforcée des échanges, de nouvelles générations d'outils devront être développées pour permettre aux « néo-utilisateurs » de l'Internet de s'en emparer. Ainsi, ce marché qui était limité à certains usagers professionnels a connu un développement important depuis l'affaire Snowden[17]. Cependant, comme le rappelle Laura Poitras, la journaliste qui a reçu avec Glenn Greenwald les révélations d'Edward Snowden, ces technologies ne pourront réellement se démocratiser que si elles deviennent aussi ergonomiques que les services les plus utilisés sur Internet[18].

---

[15] *Social Media and the 'Spiral of Silence' (*Etude Pew Research - août 2014)
http://www.pewinternet.org/2014/08/26/social-media-and-the-spiral-of-silence/

[16] http://www.wired.co.uk/news/archive/2014-02/06/tim-berners-lee-reclaim-the-web

[17] *Snowden and NSA: A Boon to the Privacy Business* (The Fiscal Times, 14 juillet 2014)
http://www.thefiscaltimes.com/Articles/2014/07/14/Snowden-and-NSA-Boon-Privacy-Business

[18] *Snowden filmmaker Laura Poitras: 'Facebook is a gift to intelligence agencies'* (Washington Post, 23 octobre 2014).

Normes et standards au cœur de la Gouvernance de l'Internet

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[19] de la NSA dont les ingénieurs ont volontairement altéré la confidentialité des échanges en introduisant dans les dispositifs de chiffrement[20] des « portes dérobées » ou « backdoors[21] » qui permettaient aux services de la NSA de décrypter les messages.
Cette fragilisation des dispositifs cryptographiques constitue une menace sur l'ensemble des services qui reposent sur la confidentialité des échanges (qu'il s'agisse du commerce électronique, des échanges de données sensibles pour les États 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[22].

---

http://www.washingtonpost.com/blogs/the-switch/wp/2014/10/23/snowden-filmmaker-laura-poitras-facebook-is-a-gift-to-intelligence-agencies/

[19] http://www.theguardian.com/commentisfree/2013/sep/05/government-betrayed-internet-nsa-spying

[20] Plus précisément dans les systèmes de génération des nombres aléatoires (Dual Elliptic Curve Deterministic Random Bit Generator (Dual_EC_DRBG)).

[21] *The internet after Snowden : New threat model army* (The Economist, 11/11/2013) http://econ.st/1r5U71J

[22] *Panel recommends NIST declare independence from NSA* (FCW - 14 juillet 2014)
http://fcw.com/articles/2014/07/14/nist-panel-on-nsa.aspx

DES PERSPECTIVES TECHNOLOGIQUES ET JURIDIQUES

Un nouveau droit protecteur pour les citoyens : le « Droit au silence des puces »

Face aux évolutions technologiques de l'Internet et l'introduction de nouveaux objets connectés dans l'environnement des citoyens, de nouvelles mesures devront aussi être mises en place à l'échelle internationale pour éviter que ces objets ne deviennent de nouveaux vecteurs d'attaques informatiques sur les infrastructures critiques. 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 sur notre environnement, ils constitueront aussi des cibles potentielles pour de nouvelles formes d'attaques informatiques. Ces risques sont tels que les agences de renseignements envisagent désormais avec inquiétude le développement de ces technologies en particulier lorsqu'elles participeront à la gestion des infrastructures critiques dans le domaine des transports, de la santé ou encore de l'énergie[23]. 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 les objets 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[24] dans le but de permettre aux usagers

[23] The CIA Fears the Internet of Things (Defense One, 24 juillet 2014)
http://www.defenseone.com/technology/2014/07/cia-fears-internet-things/89660/

[24] Le concept de « *Droit au silence des puces* » a été introduit dans le texte *Architecture et Gouvernance de l'Internet* paru dans la revue Esprit, Bernard Benhamou mai 2006). http://www.netgouvernance.org/ArchitectureEsprit.pdf

de maîtriser les informations issues des puces à radiofréquences (RFID). En effet, la généralisation de dispositifs connectés dans l'environnement des usagers est à l'origine 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 qui seront échangées à partir de ces objets présents dans son environnement. Il implique en particulier que soient inclus dès la conception de ces dispositifs connectés des dispositifs de désactivation/réactivation associé à des dispositifs de chiffrement pour les données les plus sensibles, comme les données médicales ou les données relatives à la sécurité des personnes. Ce nouveau droit au « Silence des Puces » devra être codifié à la fois dans les textes et dans l'architecture de ces technologies (dans une démarche de « privacy by design ») afin qu'elles puissent rester sous le contrôle des citoyens. Les travaux sur le "Droit au Silence des Puces" ont été à l'origine de la première réunion ministérielle européenne sur l'Internet des Objets[25] et ont par la suite été repris par la Commission européenne[26] et le Parlement européen[27]. Ainsi, le Conseil des ministres des télécoms de l'UE a affirmé en 2008 la nécessité de reconnaître un « droit au silence des puces » pour les dispositifs basés sur les puces RFID. Plus récemment, le rapport du Conseil d'État : *"Le numérique et les droits fondamentaux[28]"* faisait état de ce droit comme l'une des pistes de réflexion pour l'avenir de l'Internet des Objets.

Il convient désormais d'étudier les perspectives issues des évolutions actuelles de l'Internet des Objets tant en termes de respect de la vie privée des personnes qu'en termes de sécurité de ces dispositifs. Au-delà de la protection des données, les questions de sécurité pourraient constituer un

---

Il a par la suite été détaillé et formalisé dans le texte « *Les Mutations Economiques, Sociales et Politiques de l'Internet des Objets* » (Bernard Benhamou dans les Cahiers de la Documentation Française, décembre 2012). http://www.netgouvernance.org/IOT%20Cahiers%20DOC%20FRANCAISE.PDF

[25] « *Internet des objets, Internet du futur* » Conférence Ministérielle Européenne organisée dans le cadre de la Présidence Française de l'Union Européenne (Nice 2008).

[26] *Europe prepares for the internet revolution* (European Action Plan 18 juin 2009) http://europa.eu/rapid/press-release_IP-09-952_en.htm?locale=en

[27] *Motion For A European Parliament Resolution On The Internet Of Things* (Committee on Industry, Research and Energy, Rapporteur: Maria Badia i Cutchet, 10 mai 2010). http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2010-0154&language=EN

[28] *Le numérique et les droits fondamentaux* (Etude annuelle 2014 du Conseil d'Etat, septembre 2014). http://www.ladocumentationfrancaise.fr/docfra/rapport_telechargement/var/storage/rapports-publics/144000541/0000.pdf

nouveau motif pour instaurer une désactivation (temporaire ou définitive) des puces de l'Internet des Objets. En effet, à mesure que ces objets seront présents, dans la durée, dans l'environnement des usagers, certains d'entre eux cesseront d'être supportés par les entreprises qui les auront conçus. Or, avec ce défaut de mise à jour de sécurité, ce sont de nouveaux risques d'attaques qui pourraient être diffusées à l'ensemble des objets ainsi « fragilisés ». Désormais, au droit au Silence des Puces pourrait être associée une obsolescence programmée des objets connectés[29] ainsi qu'à la nécessité d'utiliser des solutions logicielles libres « open source » pour les objets afin de permettre leurs évolutions en termes de sécurité. La complexité des objets connectés (qui pour beaucoup d'entre eux voient leurs données transmises sur des systèmes de « cloud computing »), nécessitera aussi que soient précisées les conditions technologiques et juridiques[30] dans lesquelles les données pourront être transmises[31].

Design et ergonomie : de nouveaux principes pour la démocratie à l'ère numérique

L'organisation des données numériques accessibles par les citoyens constitue un nouvel enjeu pour la puissance publique. En effet, s'il est toujours possible d'accéder au segment d'un ouvrage « papier », il en va tout autrement lorsque les mêmes informations sont disponibles en ligne. En effet, si les concepteurs d'un site ou d'une application n'ont pas pris en compte l'ergonomie de la navigation, ces informations peuvent devenir inaccessibles. Cela peut ainsi mener à une situation de « richesse paradoxale » où des informations et des services de plus en plus nombreux ne deviendraient accessibles qu'aux seules personnes ayant une maîtrise suffisante des technologies.

De manière plus générale une tension existe entre les objectifs de simplification (par le design et l'ergonomie) et les objectifs de contrôle démocratique des technologies par la transparence et l'appropriation du code par les citoyens. Les outils les plus ergonomiques étant actuellement souvent les plus « fermés » et les outils « ouverts » qui donnent aux citoyens la capacité d'intervenir sur les

---

[29] *Why Gadgets in the Internet of Things Must Be Programmed to Die* par Robert Mcmillan (Wired, le 23 mai 2014) http://www.wired.com/2014/05/iot-death/

[30] *When Everything Works Like Your Cell Phone* (The Atlantic, 28 septembre 2014) http://www.theatlantic.com/technology/archive/2014/09/when-everything-works-like-your-cell-phone/379820

[31] *The Internet Of Someone Else's Things* par Jon Evans (TechCrunch, le 11 octobre 2014) http://techcrunch.com/2014/10/11/the-internet-of-someone-elses-things

services numériques restent souvent plus complexes. Pour être en mesure de donner aux citoyens un véritable contrôle démocratique sur les architectures numériques qui détermineront leurs modes de vie et d'échange, il sera nécessaire que les outils soient à la fois plus transparents et plus ergonomiques.

En ce sens l'ergonomie et le design associés aux données numériques, loin d'être des variables d'ajustement deviennent des fonctions cruciales pour les architectes des systèmes d'information. À mesure que la quasi-totalité des mécanismes de transmission de l'information dans nos sociétés deviennent numériques, ces principes de simplicité et d'accessibilité des ressources numériques sont désormais devenus de véritables impératifs démocratiques.

Vers l'autolimitation des activités de surveillance des États sur Internet

Au-delà de l'encadrement juridique de la collecte des données et des pratiques liées à surveillance, des mesures devront être prises pour protéger l'architecture de l'Internet via les normes et standards qui lui ont permis jusqu'ici de fonctionner dans un cadre de confiance. En effet si l'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[32] comme celle qui pourrait naître à l'issue des révélations d'Edward Snowden. C'est précisément 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[33]. Ainsi, les organisations chargées de la régulation technique du réseau ont, pour la première fois depuis leur création, décidé de prendre part au débat politique sur la nécessité pour les États de ne pas remettre en cause l'architecture d'échange de l'Internet et en particulier de remettre en cause la confiance des usagers du réseau. Cette confiance qui a été la clé de voûte du fonctionnement de l'Internet pourrait si elle était durablement remise en cause induire une stagnation des échanges et avoir des conséquences sociales, économiques et politiques imprévisibles.

---

[32] *Architecture et Gouvernance de l'Internet* par Bernard Benhamou (Revue Esprit, mai 2006)
www.netgouvernance.org/ArchitectureEsprit.pdf

[33] *Montevideo Statement on the Future of Internet Cooperation* (ICANN, 7 oct 2013)
https://www.icann.org/resources/press-material/release-2013-10-07-en

Ainsi, l'Internet Engineering Task Force qui regroupe de manière informelle l'ensemble des ingénieurs chargés d'élaborer les normes et standards de l'Internet a émis une « loi technique » (aussi appelée *Request for Comment*) qui décrit la surveillance de masse comme une attaque contre l'Internet[34]. Cependant, pour que cette « loi technique » puisse s'imposer dans les faits 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 États en matière de surveillance sur Internet.

En effet comme le rappelait le rapport du groupe d'experts sur la cybersécurité remis à la Maison Blanche en décembre 2013[35], en plus d'une efficacité encore limitée, ces programmes de surveillance de masse pourraient avoir des "effets de bords" insoupçonnés sur les libertés et plus généralement sur le fonctionnement même de nos sociétés[36]. Cette « retenue » des activités des États vis-à-vis de leurs activités de surveillance ne doit donc pas se limiter à la seule remise en cause de la collecte des informations en masse (bulk collection) mais elle doit aussi être étendue aux activités qui ont pour objectif de modifier les technologies et les standards sur Internet à des fins de surveillance. Les attaques contre la sécurité et la confiance sur Internet doivent désormais plus être considérées comme des délits mais comme des atteintes graves au fonctionnement de nos sociétés. Que ces attaques soient issues d'entreprises, de particuliers ou d'agences gouvernementales.

Vers un traité transatlantique sur la Gouvernance de l'Internet

[34] *Pervasive Monitoring Is an Attack* (RFC 7258 IETF, mai 2014) http://tools.ietf.org/html/rfc7258

[35] « *Notre travail suggère que les métadonnées collectées dans le cadre de l'utilisation de la Section 215 n'ont pas été essentielles pour la prévention d'attaques. Ces données pouvaient de surcroît être obtenues de manière rapide via les procédures traditionnelles. De plus, la prudence exige de remettre en cause l'idée que ce programme est efficace dans la prévention des attaques terroristes étant donné que les métadonnées recueillies ne couvrent qu'une partie des enregistrements de certains opérateurs.* » extrait de *Liberty And Security In A Changing World*, Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies (décembre 2013) http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

[36] *"Les révélations de la NSA ont déclenché avec elles une incertitude existentielle : "tout ce que vous direz pourra et sera utilisé contre vous". Et les conséquences à long terme d'une telle destruction de l'échange informel sont encore inconnues."* Déclare Geert Lovink, directeur de l'Institut des cultures en réseaux. (*Comment le logiciel nous influence* – Hubert Guillaud InternetActu, le 29 août 2014) http://internetactu.blog.lemonde.fr/2014/08/29/comment-le-logiciel-nous-influence/.

La situation nouvelle créée par la mise en place par les États-Unis de leurs programmes de surveillance de masse sur Internet 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. Dans cette perspective, l'inventeur du web, le britannique Tim Berners-Lee, a déjà réclamé que soit créée une Constitution mondiale pour l'Internet[37]. Cet « Internet Bill of Rights » ou cette « Magna Carta » pourrait placer les principes fondamentaux de l'Internet au-dessus des lois nationales afin que les États ne puissent unilatéralement modifier l'Internet à des fins économiques ou politiques. C'est ce principe qu'avait aussi évoqué Viktor Mayer-Schoenberger, de la Harvard Kennedy School, dans son étude de la proposition européenne lors du Sommet des Nations unies. Dans cette étude, au titre évocateur « Jefferson Rebuffed[38] » (Jefferson repoussé), il notait qu'un « moment constitutionnel » avait été manqué par les États-Unis en 2005 en repoussant la proposition européenne qui prévoyait d'inscrire dans les textes internationaux les trois principes fondamentaux liés à l'architecture de l'Internet (l'ouverture, l'interopérabilité et la neutralité de l'Internet). À ces trois principes, il conviendrait aujourd'hui d'en ajouter un quatrième qui interdirait aux États de prendre des mesures à même de porter 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 États 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 afin de veiller à ce que de nouvelles crises liées à la confiance ne puissent fragiliser l'architecture mondiale de l'Internet.

Dans un premier temps, pourront être associés à ce traité les pays comme l'Allemagne et le Brésil qui partagent des préoccupations communes sur les libertés fondamentales et leur expression sur Internet avec pour objectif à moyen et long terme d'en favoriser l'adoption par l'ensemble des pays membres des Nations unies. 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[39]. Parmi les principes que cet organisme pourrait être amené à surveiller figureraient :

---

[37] *An online Magna Carta: Berners-Lee calls for bill of rights for web* (The Guardian, 12/03/2014) http://www.theguardian.com/technology/2014/mar/12/online-magna-carta-berners-lee-web

[38] *Jefferson Rebuffed - The United States and the Future of Internet Governance* - Viktor Mayer-Schoenberger et Malte Ziewitz – John F. Kennedy School of Government, Harvard University (mai 2006) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=902374

[39] Il est à noter que 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 sur ce point : *How to Save the Net: A CDC for Cybercrime* (Wired, 19 août 2014)

- La préservation des principes généraux de l'architecture du réseau : ouverture, interopérabilité et Neutralité de l'Internet,
- La protection des normes et standards qui sous-tendent le fonctionnement des infrastructures critiques de l'Internet (en particulier les systèmes de chiffrement),
- La protection des citoyens par des mesures d'encadrement des actions de surveillance des États ainsi que par la mise en place de dispositifs juridiques et technologiques de contrôle des données transmises par les objets connectés.

Comme le rappelait, le récent rapport du Sénat[40] sur la Gouvernance mondiale de l'Internet, la mise en place d'un traité transatlantique sur la gouvernance de l'Internet revêt en effet un caractère crucial pour les pays de l'Union européenne :

> *« L'Union européenne doit faire entendre sa voix dans le débat en cours sur la future gouvernance de l'Internet. Mais il est certain que sa crédibilité sera d'autant plus forte qu'elle aura, en interne, repris son avenir numérique en mains pour conquérir un poids réel dans le cyberespace. Il n'est assurément pas facile pour l'Union européenne d'intervenir dans une discussion que les États-Unis ont engagée mais qu'ils veulent voir menée par l'ICANN. Toutefois, le climat engendré par les révélations d'Edward Snowden lui offre une opportunité historique de se poser comme médiateur pour inventer une gouvernance de l'Internet fidèle à ses valeurs. »*

http://www.wired.com/2014/08/save-the-net-peter-singer/

[40] *L'Europe au secours de l'Internet : démocratiser la gouvernance de l'Internet en s'appuyant sur une ambition politique et industrielle européenne (*Rapport d'information n° 696 (2013-2014) de Mme la Sénatrice Catherine Morin-Desailly dans le cadre de la Mission Commune d'Information du Sénat sur la Gouvernance mondiale de l'Internet, 8 juillet 2014) http://www.senat.fr/rap/r13-696-1/r13-696-11.pdf