LES NOUVEAUX DÉFIS POLITIQUES ET ÉCONOMIQUES DE L'INTERNET

Bernard Benhamou
Secrétaire général de l'Institut de la souveraineté numérique

Les révélations d'Edward Snowden sur les programmes de surveillance des services de renseignement américains ont suscité de fortes inquiétudes sur la protection des libertés individuelles. Bernard Benhamou explique que les conséquences économiques de cette surveillance de masse sont également considérables, la confiance des utilisateurs conditionne en effet le développement des technologies numériques. La décision de la Cour de justice de l'Union européenne du 6 octobre 2015 qui a remis en cause la transmission des données personnelles de citoyens européens aux entreprises américaines et la récente opposition entre le FBI et Apple sur le chiffrement des iPhone illustrent les nouvelles dimensions de ce conflit. Dimensions qui pourraient être encore plus importantes avec l'essor des objets connectés. À l'opposé des demandes des services de sécurité qui souhaitent introduire des failles dans les dispositifs cryptographiques – failles que les groupes mafieux ou terroristes découvriront inévitablement –, c'est le chiffrement des données qui pourrait à l'avenir protéger les libertés individuelles mais aussi nos sociétés et leurs infrastructures économiques.

C. F.

En l'espace de quelques années, le paysage technologique et industriel de l'Internet a été profondément modifié avec la montée en puissance des terminaux mobiles et bientôt l'essor de l'Internet des objets. Dans le même temps, les révélations d'Edward Snowden sur les programmes de surveillance mis en place par la National Security Agency (NSA) ont permis aux opinions publiques de mesurer les nouveaux risques pour les libertés que ces technologies peuvent créer. Plus récemment, les débats qui se déroulent aux États-Unis et en Europe à propos des mesures technologiques et juridiques prises par les gouvernements pour faire face aux menaces terroristes, commencent à évoquer les conséquences de ces mesures sur l'architecture informationnelle de nos sociétés. En effet, en plus de remettre en cause la protection des données personnelles des citoyens, les actions des États pourraient aussi avoir des effets de bord imprévisibles sur l'ensemble du paysage industriel des technologies. Ces débats qui semblaient jusqu'alors réservés aux seuls experts relèvent d'enjeux politiques et économiques majeurs pour l'ensemble de nos sociétés et, à ce titre, devront faire l'objet d'un véritable débat démocratique.

L'après Snowden : vers une redéfinition de la géopolitique de l'Internet

Dans les deux décennies passées, la géopolitique de l'Internet[1] a été conditionnée par la maîtrise des infrastructures essentielles à la gestion de l'Internet.

(1) Benhamou B. et Sorbier L. (2006), « Internet et souveraineté : la gouvernance de la société de l'information », *Politique étrangère*, IFRI, automne.
http://www.netgouvernance.org/politiqueetrangere.pdf

C'est en particulier le cas du système de gestion des noms de domaines (aussi appelé DNS) qui détermine la cartographie fonctionnelle de l'Internet à l'échelle mondiale. La gestion du DNS est en grande partie à l'origine de la mise en place du premier sommet mondial des Nations unies sur la gouvernance de l'Internet en 2005.

Désormais, ce sont les flux d'information, leur traitement et la localisation des données qui deviennent de nouveaux enjeux de souveraineté pour les États. Comme le décrivait le sociologue des réseaux Manuel Castells[2], la montée en puissance de l'Internet consacre le passage d'un espace des lieux à un espace des flux. Or le contrôle de ces flux et leur surveillance par les agences de renseignement américaines ont été au cœur des révélations d'Edward Snowden. Ainsi, l'accord « *Safe Harbor* » qui permettait aux entreprises américaines de traiter les données personnelles des citoyens européens a été invalidé par la Cour de justice de l'Union européenne dans son arrêt du 6 octobre 2015, en raison des risques de surveillance de ces données par les agences de renseignement américaines. Cette invalidation et sa récente renégociation sous l'intitulé « *Privacy Shield* » ont marqué le début d'une prise en compte par l'Europe de la nouvelle donne créée par l'ère « post Snowden ». En effet, en revenant sur cet accord crucial pour plus de 4 000 sociétés américaines, les institutions européennes ont établi la première action de gouvernance des données à l'échelle européenne. Certains allant même jusqu'à décrire cet événement fondateur comme l'embryon d'un gouvernement européen.

En plus des écoutes mises en place par la NSA (comme celle du programme PRISM), Snowden a révélé que l'ensemble des couches qui constituent l'Internet, depuis les protocoles de sécurité en passant par les disques durs des ordinateurs ou plus récemment les terminaux mobiles, peuvent être criblées volontairement de failles de sécurité (avec les programmes Bullrun ou Equation). Le principe établi par le physicien Dennis Gabor[3] pour décrire les évolutions des technologies de l'armement pourrait ainsi être paraphrasé pour décrire les évolutions des technologies numériques liées à la souveraineté des États : « *Tout ce qui est technologiquement faisable pour faciliter le travail des agences de renseignement sera fait ou tenté, quelles qu'en soient les conséquences politiques ou morales…* ».

Comme l'ont fait remarquer les industriels des technologies, ces failles mettent aussi en péril l'un des piliers essentiels du développement économique de ces technologies : la confiance des utilisateurs. S'il a été souvent question des aspects liés à la protection des libertés individuelles dans les discussions suscitées par les révélations d'Edward Snowden, les aspects économiques pourraient *in fine* dominer le débat international sur les formes que prendront nos sociétés à mesure que se développeront des technologies de plus en plus mêlées à nos activités quotidiennes. Or, l'intrusion des acteurs du renseignement non seulement dans la collecte d'information mais dans la définition même des prochaines générations de technologies est désormais perçue comme un risque économique et politique majeur pour les acteurs industriels. En effet, comme le rappelait Maxime Chertoff, l'ancien responsable du département Homeland Security : « *Historiquement, nos sociétés n'ont pas été conçues pour faciliter le travail de collecte d'information des services de renseignement…*[4] ».

Des effets de bord imprévisibles

Le récent conflit entre le FBI et Apple à propos des mesures de contournement des dispositifs de chiffrement des iPhone correspond à une tentation ancienne des services de renseignement américains d'installer officiellement des portes dérobées (*backdoors*) dans l'ensemble des terminaux connectés. Déjà dans les années 1990, la NSA avait développé une puce cryptographique « *Clipper Chip* » dont les clés auraient été détenues par les autorités américaines qui au besoin auraient pu déchiffrer l'ensemble des échanges informatiques transitant par ces puces. Cette puce avait été abandonnée en 1996. Deux décennies plus tard, ces questions se posent avec une acuité d'autant plus grande qu'elles s'inscrivent dans un climat sécuritaire où les menaces d'attaques sont désormais perçues par l'ensemble des opinions publiques.

(2) Castells M. (1998), *La société en réseaux. L'ère de l'information*, Paris, Fayard.

(3) « Tout ce qui est techniquement faisable se fera, que sa réalisation soit jugée moralement bonne ou condamnable… ». Cf. Gabor D. (1963), *Inventing the Future*, Londres, Éd. Secker & Warburg.

(4) « Even the Former Director of the NSA Hates the FBI's New Surveillance Push », *The Daily Beast*, 27 juillet 2015.
http://www.thedailybeast.com/articles/2015/07/26/even-the-former-director-of-the-nsa-hates-the-fbi-s-push-for-new-surveillance-powers.html

Ainsi, la possibilité d'installer des portes dérobées dans les dispositifs destinés au grand public s'est progressivement imposée dans les débats politiques des deux côtés de l'Atlantique. La société Apple, au départ isolée dans son refus de se conformer aux demandes du FBI, a progressivement été rejointe par l'ensemble des acteurs économiques majeurs de l'Internet. En effet, le paysage industriel et politique a évolué et les sociétés qui s'opposent à ces mesures figurent parmi les plus importantes capitalisations boursières mondiales et, en plus de leur capacité d'influence à Washington, ces sociétés forment l'épine dorsale des technologies qui progressivement s'imposent dans tous les secteurs de l'activité économique et sociale.

Désormais, la protection juridique que réclament les industriels des technologies face aux demandes des services de renseignement correspond à la création d'un nouveau « moment constitutionnel » de l'Internet. Il s'agit en effet pour les technologies clés du fonctionnement et de la confiance de bénéficier des mêmes protections constitutionnelles que celles qui protègent la liberté d'expression. Comme le rappelle l'expert en cybersécurité Bruce Schneier[5], la plus grande erreur que pourraient commettre les pays développés serait en effet de créer des failles qui seront nécessairement découvertes par des groupes mafieux ou terroristes. Ainsi, la réponse des services de sécurité face aux menaces terroriste porterait en elle le risque de fragiliser nos édifices industriels voire nos institutions elles-mêmes. Ce qui fait dire à Mike McConnell, l'ancien patron de la NSA, que la position d'Apple sur la cryptographie relève du patriotisme[6].

Première fracture entre gouvernement américain et industries technologiques

Si dans le passé, les libertés individuelles et le développement de l'Internet semblaient aller de pair, le contexte international a depuis remis en cause les liens qui existaient entre les discours de l'administration américaine et ses acteurs industriels. Ainsi, lors de son mandat à la tête du Département d'État, Hillary Clinton décrivait les principes qui guidaient son action sur le développement international des technologies (en particulier au moment des printemps arabes) en ces termes : « *Je voulais avertir des pays comme la Chine, la Russie et l'Iran que les États-Unis allaient promouvoir et défendre un Internet où les droits individuels sont protégés et qui est ouvert à l'innovation, interopérable dans le monde entier, assez sûr pour mériter la confiance des gens et assez fiable pour les aider dans leur travail. Nous allons nous opposer à toute tentative visant à restreindre l'accès à Internet ou à réécrire les règles internationales qui régissent ses structures, et soutenir les militants et les innovateurs qui essaient de contourner les pare-feu répressifs*[7] ».

La politique extérieure des États-Unis et les industries technologiques fonctionnaient alors en pleine harmonie. Depuis, l'affaire Snowden et les tensions autour des objectifs sécuritaires des États-Unis ont créé une fracture durable entre les alliés indéfectibles d'hier. En effet, les intérêts des services de sécurité et les industriels des technologies apparaissent désormais comme divergents. Si dans un premier temps cette fracture concernait les industriels des technologies et le Gouvernement américain, elle s'est désormais étendue à l'intérieur même de l'appareil d'État américain[8].

Après ordinateurs et mobiles… les objets connectés

La prochaine étape du développement des technologies sera marquée par un mouvement de dissémination « centrifuge » de celles-ci dans notre environnement quotidien. En effet si nous avons connu jusqu'ici le développement de l'Internet sur des ordinateurs puis sur des terminaux mobiles, les prochaines générations d'objets connectés pourraient être radicalement différentes dans la mesure où elles seront associées à des objets « non informatiques » comme les vêtements, les denrées alimentaires ou des accessoires médicaux…

Actuellement la plupart des objets connectés sont conçus pour transmettre des données à des infrastructures distantes (le plus souvent « *cloud* ») et sont interrogeables *via* les terminaux mobiles. Cependant, en l'absence

(5) Schneier B. (2015), *Data and Goliath*, New York, Ed. Norton & Company.

(6) « Apple's Encryption Stance Patriotic, Says Ex-NSA Chief », *Tom's Guide*, 4 mars 2016. http://www.tomsguide.com/us/mcconnell-chertoff-apple-fbi-rsa, news-22346.html#sthash.Swn8ed0V. uxfs

(7) Clinton H. (2014), *Le Temps des Décisions. 2008-2013*, Paris, Éd. Fayard.

(8) « Apple Vs FBI : iPhone battle exposes rift in Obama administration », *Tech2*, 7 mars 2016 http://tech.firstpost.com/news-analysis/apple-vs-fbi-iphone-battle-exposes-rift-in-obama-administration-302762.html

de dispositifs de chiffrement efficaces, cette double connexion vers le mobile et vers le stockage distant peut se révéler fragile face aux attaques extérieures. D'autres architectures décentralisées et potentiellement plus sûres seraient possibles autour des objets connectés. Afin de prendre pied sur un marché crucial pour les économies européennes, les sociétés européennes pourraient ainsi développer de nouvelles générations d'objets connectés qui garantiraient à la fois la protection des données de leurs usagers et limiteraient les risques d'attaques extérieures. Là encore, la capacité des industriels des technologies à s'émanciper de l'influence des agences de renseignement pourrait conditionner le devenir économique de ce secteur. En effet, le directeur du renseignement américain reconnaît déjà s'intéresser aux objets connectés[9] qui représentent de nouveaux vecteurs d'attaques. Dans le même temps, la NSA finance même des projets visant à établir un cadre de protection pour le fonctionnement des objets connectés[10].

Il existe aussi des obstacles sociétaux à la montée en puissance de certains types d'objets connectés jugés particulièrement invasifs par les citoyens. Ce fut le cas pour le projet des Google Glass dont les possibilités d'enregistrement vidéo et audio permanentes ont suscité une levée de bouclier des associations de protection de la vie privée[11] et plus généralement des citoyens. Plus récemment, les projets d'objets connectés prenant la forme de mouchards automobiles proposés par les assureurs pour analyser la conduite et ainsi adapter le coût des primes d'assurances sur le principe du « *pay how you drive* » ont eux aussi suscité des interrogations sur leur acceptabilité auprès des conducteurs[12].

Sécurité et vie privée à l'heure des objets connectés

Les problèmes de cybersécurité déjà connus pourraient aussi prendre une ampleur nouvelle avec la montée en puissance des objets connectés et à mesure qu'ils accompagneront la quasi-totalité des activités quotidiennes des citoyens[13]. La fragilisation des dispositifs cryptographiques de protection des données de ces objets pourrait en effet avoir des conséquences graves pour l'utilisateur lorsqu'il est question de dispositifs médicaux ou de voiture sans pilote. À l'échelle des infrastructures vitales des États, les nouveaux dispositifs de gestion des réseaux électriques intelligents ou ceux des structures de santé pourraient eux aussi constituer de nouvelles cibles de choix pour des cyberattaquants, qu'il s'agisse de groupes mafieux susceptibles de vouloir rançonner des hôpitaux ou de groupes terroristes qui pourraient attaquer des infrastructures vitales dans le domaine des transports ou de l'énergie et qui verraient dans ces nouvelles formes d'attaques un substitut infiniment moins risqué et potentiellement plus dangereux que des attaques traditionnelles. Si les formes traditionnelles d'attaques terroristes visent les personnes et les lieux physiques, le rôle essentiel des infrastructures informationnelles dans nos sociétés et la capacité de mener des attaques à distance rendent ces nouvelles formes d'attaques terroristes à la fois plus probables et plus faciles à réaliser. En effet, au-delà de l'impact sur les opinions publiques, ces attaques pourraient

(9) « Le directeur du renseignement américain reconnaît s'intéresser aux objets connectés », *Le Monde*, 10 février 2016.
http://www.lemonde.fr/pixels/article/2016/02/10/le-directeur-du-renseignement-americain-reconnait-s-interesser-aux-objets-connectes_4862587_4408996.html

(10) https ://nakedsecurity.sophos.com/2015/08/12/the-nsa-is-funding-a-safer-internet-of-things/

(11) « A Retreat for Google Glass and a Case Study in the Perils of Making Hardware », *New York Times*, 18 janvier 2015.
http://bits.blogs.nytimes.com/2015/01/18/a-retreat-for-google-glass-and-a-case-study-in-the-perils-of-making-hardware/

(12) « Assurance automobile : la promesse d'économies en échange d'un mouchard », *Europe1*, 7 octobre 2015. http://www.europe1.fr/economie/assurance-automobile-la-promesse-deconomies-en-echange-dun-mouchard-2525971

(13) « Apple, the FBI, and the Internet of Things : Your whole house is open to attack », *Los Angeles Times*, 1er mars 2016.
http://www.latimes.com/business/hiltzik/la-fi-mh-apple-the-internet-of-things-vulnerable-to-attack-20160301-column.html

directement déstabiliser le fonctionnement même des sociétés attaquées par des groupes terroristes[14].

À terme, la sécurité des nations pourrait davantage reposer sur le renforcement de ces technologies de protection des données et donc sur une plus grande « opacité » des données. Ainsi, comme le fait remarquer le juriste Lawrence Lessig[15], les prochaines étapes de la régulation de la vie privée passeront davantage par le développement de nouvelles générations de technologies de chiffrement des données que par les seules mesures d'encadrement de l'utilisation des données. L'un des exemples de ces technologies est le projet Enigma[16] mené par le MIT qui se propose d'utiliser les technologies de chiffrement de la « *blockchain* » pour protéger l'utilisation des données personnelles. L'importance de la sécurité des infrastructures informationnelles est devenue telle qu'aucun pays désormais ne peut envisager que soit remis en cause leur fonctionnement. Ce qui semblait encore impensable il y a quelques années, un accord sino-américain sur la limitation du cyber-armement, semble désormais possible comme en témoignent les récentes négociations entre MM. Obama et Xi Jinping[17].

Une Europe encore fragmentée sur les questions de gouvernance des technologies

Face à la nécessité d'une meilleure coordination internationale sur les politiques technologiques, l'Europe apparaît encore fragmentée. Si le gouvernement néerlandais défend désormais le chiffrement des données[18], d'autres pays comme le Royaume-Uni, proposent de bannir les technologies de chiffrement « d'utilisateur à utilisateur » (*end-to-end encryption*)[19]. En France les débats sur les lois promulguées à l'issue des attaques terroristes en 2015 ont donné lieu à des propositions similaires en particulier pour forcer les constructeurs de terminaux mobiles à collaborer avec les autorités.

Plus encore que les seules menaces de cyberattaques, les États européens ont pris conscience de leur vulnérabilité face à des évolutions technologiques sur lesquelles ils n'ont que peu de prise. En effet, à défaut de participer activement à l'élaboration des normes et standards qui constituent l'épine dorsale de l'Internet, l'Europe ne pourra plus réclamer de souveraineté sur ses infrastructures informationnelles et donc sur nos sociétés entières. Comme le rappelait le vice-chancelier allemand Sigmar Gabriel, les acteurs européens de technologies devront aussi être en mesure de participer à l'élaboration des normes et standards de l'Internet. Cela s'avérera particulièrement nécessaire pour élaborer les nouvelles générations d'infrastructures de sécurité sur lesquelles un contrôle multilatéral du code (informatique) devra aussi être établi afin d'éviter que ces codes puissent à leur tour être porteurs de failles.

Plus qu'en agissant de manière « défensive » face aux menaces d'ubérisation massive de l'économie, les politiques publiques européennes devront établir des choix sur les secteurs stratégiques (comme la santé, l'énergie ou les transports…). Ces secteurs devront faire l'objet d'une véritable coordination industrielle, juridique et technologique afin d'investir des champs nouveaux dans le domaine des services et des objets connectés. Afin de bénéficier de l'effet d'entraînement des succès comme BlaBlaCar (qui correspond à une initiative européenne originale et « non réplicable » dans le domaine des transports) ou de Sigfox (autour de la création de nouvelles générations de réseaux d'objets connectés), les politiques publiques européennes devront aussi orienter la commande publique vers des entreprises innovantes de petite taille et de taille intermédiaire qui pourront à leur tour participer à la transformation de l'ensemble des secteurs industriels. En effet, comme l'ont démontré les acteurs américains des technologies, il est désormais impossible de concevoir le développement d'une souveraineté numérique européenne sous un angle uniquement juridique ou technique si elle ne s'appuie pas aussi sur un écosystème industriel diversifié et puissant.

(14) Benhamou B. (2014), « Les perspectives de la Gouvernance mondiale de l'Internet après Snowden », *Politique étrangère*, IFRI, hiver.

(15) Lessig L. (2015), « Technology Will Create New Models for Privacy Regulation », *Wall Street Journal*, 30 décembre.

(16) http://enigma.media.mit.edu

(17) « U.S. and China Seek Arms Deal for Cyberspace », *New York Times*, 20 septembre 2015.
http://www.nytimes.com/2015/09/20/world/asia/us-and-china-seek-arms-deal-for-cyberspace.html

(18) « Le gouvernement néerlandais défend le chiffrement des données », *Le Monde*, 7 janvier 2016./http://www.lemonde.fr/pixels/article/2016/01/07/le-gouvernement-neerlandais-defend-le-chiffrement-des-donnees_4842993_4408996.html

(19) « Internet firms to be banned from offering unbreakable encryption under new laws », *The Telegraph*, 2 novembre 2015. http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/11970391/Internet-firms-to-be-banned-from-offering-out-of-reach-communications-under-new-laws.html