Repenser l'impact de la surveillance après l'affaire Snowden : sécurité nationale, droits de l'homme, démocratie, subjectivité et obéissance

Zygmunt Bauman, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, Robert Walker

▶ **To cite this version:**

Zygmunt Bauman, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, et al.. Repenser l'impact de la surveillance après l'affaire Snowden : sécurité nationale, droits de l'homme, démocratie, subjectivité et obéissance. Cultures & conflits, 2015, 2 (98), pp.133-166. 10.4000/conflits.19033 . hal-03414511

HAL Id: hal-03414511
https://sciencespo.hal.science/hal-03414511

Submitted on 15 Feb 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution - NonCommercial - NoDerivatives 4.0 International License

Cultures & Conflits

98 | été 2015
Élites transnationales

Repenser l'impact de la surveillance après l'affaire Snowden : sécurité nationale, droits de l'homme, démocratie, subjectivité et obéissance

After Snowden: Rethinking the Impact of Surveillance

Zygmunt Bauman, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon et R. B. J. (Rob) Walker

Édition électronique
URL : http://journals.openedition.org/conflits/19033
DOI : 10.4000/conflits.19033
ISSN : 1777-5345

Éditeur :
CECLS - Centre d'études sur les conflits - Liberté et sécurité, L'Harmattan

Édition imprimée
Date de publication : 15 octobre 2015
Pagination : 133-166
ISBN : 978-2-343-07829-8
ISSN : 1157-996X

Référence électronique
Zygmunt Bauman, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon et R. B. J. (Rob) Walker, « Repenser l'impact de la surveillance après l'affaire Snowden : sécurité nationale, droits de l'homme, démocratie, subjectivité et obéissance », *Cultures & Conflits* [En ligne], 98 | été 2015, mis en ligne le 15 octobre 2016, consulté le 02 avril 2021. URL : http://journals.openedition.org/conflits/19033 ; DOI : https://doi.org/10.4000/conflits.19033

Creative Commons License

Repenser l'impact de la surveillance après l'affaire Snowden : sécurité nationale, droits de l'homme, démocratie, subjectivité et obéissance [1]

Zygmunt BAUMAN, Didier BIGO, Paulo ESTEVES, Elspeth GUILD, Vivienne JABRI, David LYON, R. B. J. (Rob) WALKER

Techniques de surveillance de masse et portée mondiale de l'Internet : un fossé permanent ?

Edward Snowden a révélé de très nombreuses informations sur les pratiques de l'agence américaine de sécurité nationale (*National Security Agency*, NSA) liées aux programmes de surveillance PRISM, Xkeyscore, Upstream, Quantuminsert, Bullrun ou encore Dishfire, ainsi que la participation des services d'autres États – comme le Quartier général des communications du gouvernement (*Government Communications Headquarters*, GCHQ) au Royaume-Uni, avec son programme Tempora [2]. Une grande partie de ces informations, en particulier celles liées à l'ampleur, la portée et la sophistication technique de ces pratiques ont surpris les observateurs les plus avertis. Le sens de ces pratiques reste trouble. Cela peut en partie s'expliquer par le fait que les très nombreux détails sur les systèmes complexes qui ont été révélés sont difficiles à suivre, même si nombre d'entre eux semblent avoir des conséquences graves et immédiates. C'est également en partie parce que ces détails semblent impliquer des transgressions significatives des perceptions établies du caractère et de la légitimité des institutions impliquées dans des opérations de sécurité et de renseignement, et qu'ils stimulent ainsi des controverses politiques intenses. Enfin, cela peut aussi s'expliquer, et c'est sans doute ici l'interprétation la plus déstabilisante, par les transformations que ces révélations impliquent – des transformations de long terme des poli-

---

1 . Cet article est une traduction d'un article publié en anglais : "After Snowden: Rethinking the Impact of Surveillance", *International Political Sociology*, 8/2, 2014, pp. 121–144. Nous remercions la maison d'édition Wiley pour son accord sur la publication.

2 . Traduction de Miriam Perier, décembre 2014.

tiques des États, des relations entre les États et des institutions et des normes établies en matière de procédures démocratiques, d'État de droit, de relations entre État et société civile, de relations entre politiques publiques et intérêts économiques privés, d'acceptabilité des normes culturelles et même de concepts de subjectivité.

Il semble urgent de mettre en place une évaluation systématique de l'échelle, de la portée et du caractère des pratiques de surveillance contemporaines, tant du point de vue des justifications que des controverses qu'elles entraînent. L'enjeu est de savoir si ces pratiques procèdent d'une reconfiguration significative des relations entre, par exemple, la collecte de données d'une part et la surveillance de l'Internet et d'autres systèmes de télécommunications d'autre part, ou si elles relèvent d'atteintes durables aux droits fondamentaux des individus dans la sphère numérique. Il nous faut également faire particulièrement attention aux conséquences à plus long terme de ces pratiques qui ont pourtant déjà soulevé des questions très sérieuses sur les transgressions largement répandues des principes juridiques et des normes démocratiques, et ce d'une manière qui puisse également rendre compte des transformations historiques concernant l'autorité souveraine et la légitimité politique.

Les programmes de la NSA ont avant tout pour but de récolter des données des câbles Internet sous-marins (c'est le cas des programmes Upstream et Quantuminsert) et/ou d'intercepter des données pendant leur voyage (c'est le cas du programme Tempora). Ils impliquent l'installation d'intercepteurs sur les gros câbles de fibres optiques qui connectent les différentes plateformes (*hub*) Internet. Au Royaume-Uni, le programme Tempora aurait ainsi placé deux cent intercepteurs sur les câbles reliant les îles britanniques à l'Europe de l'Ouest et aux États-Unis. Côté français, la Direction générale de la sécurité exterieure (DGSE) aurait quant à elle placé des intercepteurs similaires sur des câbles sous-marins partant de sa base militaire de Djibouti. Entre autres activités, le service fédéral de renseignement allemand (*Bundesnachrichtendienst*, BND) se serait branché directement à la plateforme Internet européenne, la DE-CIX, à Frankfort. L'Institut national de défense radio de la Suède (*Försvarets radioanstalt*, FRA) intervient directement sur les câbles souterrains reliant les pays baltes à la Russie. Les différentes agences de renseignement collaborent plus ou moins afin de récolter les données et couvrir ainsi l'ensemble du réseau Internet au niveau mondial. Les relations entre les agences tendent à être asymétriques – il leur arrive d'être concurrentes et leur collaboration sur des sujets sensibles se réduit alors – mais elles estiment cette collaboration nécessaire à l'obtention d'une image fiable de l'Internet mondial. Ces agences n'ont de cesse d'affirmer que leurs ressources sont trop limitées, qu'elles ont besoin de plus de données et d'échanges et de moins de contrôle et de supervision afin de pouvoir accélérer le processus. Sans surprise, ce type de revendications leur valent d'être accusés de vouloir mettre en

œuvre des formes de surveillance de masse proches de celles pratiquées par la Stasi, et renverser le principe de la présomption d'innocence en instaurant une suspicion *a priori*, que l'individu doit dissiper par un comportement transparent [3].

Ces soupçons sont par ailleurs éveillés par une autre pratique d'interception, plus ciblée, la Xkeyscore. En lien avec la plateforme d'intégration de la NASA, le programme PRISM, elle fonctionne sur le même principe que ce qui avait été initié par le programme *Total Information Awareness* de l'amiral Poindexter. Il s'agit d'acquérir des données personnelles de consommateurs en forçant les entreprises privées récoltant régulièrement de grandes quantités d'information à des fins commerciales (par exemple, Google, Microsoft, Apple ou Skype) à transmettre leurs données aux services de renseignement à l'insu de leurs clients. La NSA et plusieurs services européens sont accusés d'avoir obtenu, par ce biais, de grandes quantités d'informations précises qui ne sont donc pas collectées à partir de données brutes en transit dans les câbles, mais grâce à l'utilisation de services dits de « *cloud* » offerts, par exemple, par des plateformes Microsoft ou Dropbox, sans que les internautes ne soient informés de cette collecte de données. Il en va de même pour les informations émanant de réseaux sociaux comme Facebook. Ces données et ces métadonnées permettent ainsi une cartographie des relations entre les individus, leurs adresses IP et le partage de contenus, de géolocalisation et de centres d'intérêts. Les réseaux de ces différents services sont donc non seulement transnationaux mais également des hybrides d'acteurs publics et privés.

Cette extension des acteurs et de la portée de leurs pratiques n'est pas un processus souple, elle exacerbe les luttes. Certains services de renseignement

3 . Pour une mise à jour régulière sur les révélations à propos des différents programmes de surveillance, voir les sites internet du *Guardian* (www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-filessurveillance-revelations-decoded) et du *Christian Science Monitor* (www.csmonitor.com/USA/2013/1016/NSA-revelations-A-timeline-of-what-s-come-out-since-Snowden-leaks-began/June-5-8-2013). Parmi les nombreux rapports disponibles, voir Clarke, R. A., Morell M. J., Stone G. R., Sunstein C. R., Swire P., *Liberty and Security in a Changing World. Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*, White House, 12 décembre 2013. Voir aussi le rapport du *US Independent Privacy Oversight Board* : Medine D., Brand R., Collins Cook E., Dempsey J., Wald P., *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court. Privacy and Civil Liberties Oversight Board*, 23 janvier 2014 (www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf) ; le rapport européen du Comité Libe du Parlement européen, dirigé par Claudio Moraes, 21 février 2014, *Sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures*, 2013/2188(INI) (www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2014-0139+0+DOC+XML+V0//FR) ; et l'étude pour le Parlement européen, du CCLS-CEPS : Bigo D., Carrera S., Hernanz N., Jeandesboz J., Parkin J., Ragazzi F., Scherrer A., *Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law*, 2013-PE 493.032. (www.ccls.eu et www.ceps.eu/book/mass-surveillance-personal-data-eu-member-states-and-its-compatibility-eu-law).

comme la NSA et le GCHQ travaillent à très grande échelle et s'appuient sur des collaborations volontaires ou forcées avec des fournisseurs privés (Microsoft, Google, Yahoo, Facebook, Paltalk, Youtube, Skype, AOL, Apple) et des entreprises de télécommunications (BT, Vodafone Cable, Verizon Business, Global Crossing, Level 3, Viatel et Interroute) afin d'identifier les différents points et de les relier grâce à des logiciels de profilage et de visualisation. Certains services désapprouvent cette stratégie et n'exigent pas des entreprises privées qu'elles leur fournissent des données, préférant se concentrer sur des cibles spécifiques, travailler à petite échelle, mais avec davantage de certitudes.

Un troisième type de pratiques implique l'écoute d'appels téléphoniques, la collecte de SMS, de communications Skype ainsi que les divers signaux audio et vidéo qui passent par des ordinateurs, des téléphones de type « *Smartphone* », des communications satellites et des lignes traditionnelles (c'est le cas du programme Dishfire pour les SMS). Ces pratiques mettent à jour et élargissent efficacement le type de surveillance des télécommunications qui avait mené aux scandales précédents impliquant le système Echelon pour la surveillance des communications personnelles et commerciales [4].

Ces différentes pratiques d'interception des communications sont à la fois complexes et interconnectées et sont conçues pour traiter secrètement des données personnelles. Ces dernières se composent à la fois de contenu (des enregistrements d'appels téléphoniques, des SMS, des emails, des contributions sur Facebook, l'historique des visites de sites d'un utilisateur, etc.) et de métacontenu (le moyen, l'heure, la date, le créateur et le lieu de création des données transmises). Une fois collectées, les données et les métadonnées sont conservées pendant une période précise (comme dans Tempora) puis elles sont organisées via des plateformes d'intégration (comme PRISM) afin de devenir intelligibles par la visualisation des réseaux (et en premier lieu les personnes et les adresses Internet) faisant déjà l'objet d'une suspicion.

La divulgation de plus amples informations sur ces pratiques a provoqué à juste titre de grandes polémiques, mais il est à craindre que les débats public et savant se limitent à des analyses rebattues sur les développements technologiques comme transformateurs des relations entre surveillés et surveillants, la réalisation des prédictions d'un George Orwell ou d'un Philip K. Dick, ou bien encore la transformation des démocraties représentatives en régimes totalitaires, au nom de la protection. Toutefois, l'information disponible et les nombreuses tentatives d'évaluation de son sens suggèrent que des questions plus profondes méritent d'être abordées. La première concerne la déconnec-

4 . Schmid G., *Sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception ECHELON)* (2001/2098(INI)), 11 juillet 2001 (www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A5-2001-0264+0+DOC+XML+V0//FR).

tion conceptuelle entre, d'une part, les dispositions et les aspirations d'un monde interétatique dans lequel chaque État a une vision claire de sa sécurité nationale et, d'autre part, les pratiques de surveillance qui sont mises en œuvre par un réseau de services de renseignement partageant de l'information tout en agissant les uns contre les autres, déstabilisant de ce fait nos conceptions traditionnelles d'alliance et de comportement étatique. Une autre question touche à l'utilisation de ces technologies et de la matérialité des câbles Internet comme sources d'information dont la géographie spécifique offre des avantages politiques à certains pays et peut ainsi reconfigurer les luttes de pouvoir à l'échelle planétaire. Une troisième question concerne les stratégies de nombreux acteurs visant à résister à ces politiques par des voies diplomatiques et stratégiques, tout comme par l'ajustement du comportement quotidien des utilisateurs d'Internet : à savoir, par exemple, s'ils vont continuer à contribuer à leur propre surveillance en s'exposant ou s'ils vont développer de nouvelles formes de subjectivité, plus réflexive, sur les conséquences de leurs actes. Enfin, une quatrième question porte sur l'origine et la légitimité des autorités dont les activités seraient justifiées par la nécessité politique et la sécurité.

Ce type de questionnements nous force à repenser les travaux des « études de la surveillance » et des « études critiques de la sécurité » qui ont déjà remis en question l'idée de la sécurité comme un outil au service des plus puissants – acteurs et intérêts. Certains chercheurs ont adopté des manières très encourageantes de penser le caractère complexe et rhizomatique de ces réseaux interconnectés d'outils de la surveillance, parmi lesquels l'auto-exposition est devenue chose banale. Toutefois, ces recherches doivent désormais poser la question du sens de l'extension de la collecte de renseignement.

Une partie de la difficulté d'une telle remise en question tient à cette idée omniprésente que tout ce qui peut se passer en relation à la NSA est formé par des dynamiques autres que la relation entre innovation technologique et possibilité politique, qui est elle-même abordée par peu de chercheurs et encore moins de dirigeants politiques. Ces dynamiques incluent des changements sociaux et culturels qui transforment l'acceptabilité des nouvelles pratiques de communication et des modalités de la connaissance, ainsi que des changements rapides dans l'expression de l'identité personnelle. Mais de manière plus significative encore, elles incluent le passage de la loi de l'État à celle du marché comme ultime mesure de la valeur politique et éthique. De manière peut-être plus troublante encore, il semble que nous prenions part à des phénomènes qui ne sont organisés ni horizontalement, à la manière d'une matrice internationale d'États plus ou moins autodéterminés et territorialisés, ni verticalement, à la manière d'une hiérarchie d'autorités plus ou moins hautes. Les relations, les lignes de conflits, les réseaux, les intégrations et les désintégrations, les contractions et les accélérations spatiotemporelles, les simultanéités, les inversions de limites internes, externes et de plus en plus élusives entre

inclusion et exclusion ou légitimité et illégitimité… la familiarité croissante avec ces notions et d'autres du même genre souligne la nécessité pressante de développer de nouvelles ressources conceptuelles et analytiques. Peut-être devrions-nous relire Leibnitz.

Un ruban de Moebius de la sécurité nationale et de la surveillance transnationale

Accès illimité aux données, sécurité nationale et renseignement étranger : la distribution inégale de la suspicion

On considère que le travail de renseignement commence par la suspicion d'actes dangereux commis par des groupes sous surveillance et se poursuit par l'identification d'individus inconnus connectés au groupe initial par trois degrés de séparations [5] ; c'est-à-dire que pour une personne suspecte qui a cent relations au premier degré, la personne responsable de sa surveillance à la NSA ou l'un de ses sous-contractants peut, sans mandat particulier, surveiller les 2 669 556 connections potentielles au troisième degré [6].

Étant donné la masse des données ainsi accumulées, les analystes ne lisent pas tout le contenu mais visualisent le graphique des relations qui ont été identifiées et se concentrent sur ce qui semble être les sections les plus importantes, là où apparaissent des nœuds de connections spécifiques entre données. On est loin d'une lecture exhaustive de tous les contenus recueillis dans ces données. On est loin également d'une procédure scientifique garantissant la certitude et la précision des résultats obtenus. Il s'agit plutôt d'un processus d'intuition et d'interprétation qui peut varier considérablement d'un analyste à un autre. Les craintes au sujet d'un *Big Brother* sont donc largement infondées. La prétention à la vérité qui accompagne cette visualisation n'a pas de fondement puisqu'elle ne vise qu'à transformer la suspicion en formes plus impressionnantes d'expertise par le biais de prédictions sur les actions d'individus, alors même que les prévisions plus générales à propos de tendances à venir s'avèrent déjà assez compliquées. Ce qui est ici en jeu n'est pas tant un mariage entre technologies et science de la société qu'une union entre technologie et croyance spéculative en des systèmes conçus pour « lire » le *big data*.

Le champ de suspicion potentielle est immense en ce qu'il n'a pas de fin et s'étend au travers de réseaux, mais il n'est pas immense en termes de portée

5 . Note de la traductrice : ou « saut », *hop*, en anglais.

6 . Suivant l'une des quarante-cinq recommandations du groupe de travail sur le renseignement et les technologies de communication publiées le 12 décembre 2013, Barak Obama semble prêt à limiter les recherches sans mandat à deux « sauts », soit 16 340 personnes, ce qui réduit en partie l'échelle de la recherche tout en maintenant le principe. Discours du 19 janvier 2014, lu sur le site du *Guardian*. Pour une recherche interactive sur les « sauts », voir www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillancerevelations-decoded#section/1.

globale ou de surveillance de tout un chacun. Tel est en effet l'argument principal des différents services de renseignement qui déclarent opérer selon des critères objectifs afin de limiter leurs recherches et de ne couvrir que les non-nationaux [7] ; et qu'ainsi les communications impliquant un « étranger » sont examinées en priorité via un canal spécial ; même s'il semble que le système puisse identifier des comportements suspicieux de ressortissants du pays (et devra, dans ce cas, obtenir un mandat, au Royaume-Uni et aux États-Unis). La collecte massive de données et la visualisation au travers de réseaux ne permettent pas de faire la différence, avec certitude, entre un étranger et un ressortissant national. Puisque les exigences de légalité menacent le fonctionnement du système, ce dernier exigerait à son tour que la loi s'ajuste, pas lui. Afin d'éviter ce type de « complications », un travail en réseau transnational entre les différents services de renseignement a permis de brouiller les limites et les frontières des juridictions nationales et étrangères. Il semble d'ailleurs que certains des services chargés de la sécurité nationale par le biais de la collecte et de l'échange d'information demandent en effet à d'autres services de sécurité de prendre en charge certaines de leurs tâches, et contournent ainsi les limites imposées en matière de renseignement extérieur en s'adonnant à un « *shopping* de vie privée » qui consiste à échanger la surveillance de leurs propres citoyens avec un autre service pour lequel ces derniers sont donc considérés comme des étrangers. En ce sens et pour toutes ces opérations transnationales, la distinction entre national et étranger perd sa pertinence.

La sécurité nationale et la numérisation de la raison d'État

Ces manières de collecter et de partager l'information ont des effets paradoxaux sur les exigences de sécurité nationale. Cette dernière n'est plus nationale lorsqu'elle achète ou analyse des données. Les différents impératifs de sécurité peuvent en effet diviser les alliés et la confiance initialement établie peut ainsi s'éroder. La numérisation crée du *big data* collecté à l'échelle transnationale, ce qui brouille les lignes du national ainsi que les limites entre le maintien de l'ordre et le renseignement. Ces tendances encouragent les acteurs à s'extraire du cadre juridique des services d'enquêtes criminelles pour adopter des approches préventives, préemptives et prédictives et favoriser un fort degré d'incertitude concernant de grandes masses de données, plutôt qu'un haut degré de certitude concernant une petite quantité de données. L'hybridation des acteurs publics et privés déstabilise la socialisation au travers d'intérêts et du secret des États nationaux, créant des opportunités de fuites de la part de personnes ayant des valeurs divergentes.

D'un point de vue plus théorique, les changements et l'incertitude qui entourent les catégories « d'étranger » et de « ressortissant national » disper-

7. C'est ce qui ressort du US-FISA et des FISC8, des exigences du GCHQ et des directives nationales françaises.

sent celles-ci dans les réseaux de connections et transforment la ligne souveraine les démarquant en un ruban de Moebius [8]. La collaboration transnationale des professionnels de la sécurité nationale et des données sensibles, publics comme privés, provoque un effet par lequel la dimension interne de la sécurité nationale s'externalise. En retour, cette externalisation s'insinue à l'intérieur par la suspicion qui pèse désormais sur tous les sujets de l'Internet. Ces « personnes concernées [9] » sont nombreuses à réagir et à rejeter une situation par laquelle tous les utilisateurs d'Internet sont traités, par principe, comme des suspects potentiels et non comme des innocents.

Il ne faut donc pas comprendre les révélations sur les pratiques de surveillance à grande échelle de la NSA et consorts comme une polémique alimentée par les médias vouée à s'essoufler, mais comme les indicateurs d'une transformation bien plus profonde affectant la manière dont les frontières de la sécurité nationale fonctionnent. Cette transformation procède de la conjonction de trois processus qui vont s'articuler : la transnationalisation, la numérisation et la privatisation.

Cette conjonction de processus crée un effet de dispersion global qui remet en question l'idée même d'une raison d'État conduite par un « État » au sein duquel le gouvernement détermine les intérêts nationaux et la sécurité nationale et demande à ses propres services d'agir en conséquence. Si le concept de la raison d'État a toujours reposé sur des revendications d'autonomie et d'autodétermination, il est à présent de moins en moins arrimé à l'idée d'une sécurité nationale assurée par des services de renseignement socialisés au secret et à la responsabilité publique, au patriotisme et à la suspicion envers les services des autres nations.

Au contraire, il nous est possible de voir la transformation de cette même raison d'État opérée par un ensemble complexe et hétérogène de professionnels de l'information sensible, un hybride composé d'acteurs privés comme publics. La nature transnationale de la collecte d'information, au-delà des frontières étatiques, dissocie la nature discursive homogène des intérêts nationaux en termes de sécurité, tout en reconstruisant un agrégat de professionnels échangeant des informations via des technologies numériques, produisant du renseignement en fonction de leurs intérêts propres et méprisant l'idée que les droits des internautes puissent limiter leurs projets.

8. Bigo D., "The Möbius Ribbon of Internal and External Security(ies)", in Mathias A., Jacobson D., Lapid Y. (eds.), *Identities, Borders, Orders. Rethinking International Relations Theory*, Minneapolis, University of Minnesota Press, 2001.

9. Note de la traductrice : s'il est difficile de se contenter de la traduction « personne concernée » (par les données) pour « *data subject* », nous avons tout de même opté pour cette expression car elle semble être communément utilisée dans l'ensemble des textes officiels se référant à cette question spécifique en français.

Par voie de conséquence, ces guildes transnationales de professionnels remettent directement en question l'autorité des professionnels de la politique qui, du moins en principe et dans les limites d'un ordre international, avaient la capacité et l'autorité de définir le contenu des intérêts et de la sécurité des nations [10]. Ils remettent également en question l'autorité des citoyens en refaçonnant les notions de vie privée, de secret des communications, de présomption d'innocence et l'idée même de démocratie. Est-ce aller trop loin que d'affirmer que ce que nous appelons encore sécurité nationale a été colonisé par une nouvelle aristocratie des services de renseignement opérant dans une arène transnationale de plus en plus autonome ?

Un champ d'échanges informatisés entre professionnels de l'information sensible et une guilde tentant de l'organiser

Étant donné le nombre d'agences, leurs forces vives et les capacités technologiques des différents services de renseignement, la notion de réseau, qui implique une relation de réciprocité et d'égalité, paraît inadaptée dans ce cas. Ces réseaux de relations sont asymétriques et hiérarchiques, comme l'étaient les guildes au Moyen Âge, avec leurs rituels, leurs codes, leurs règles d'obéissance et de solidarité. La NSA a huit fois plus d'employés que la DGSE ou la BND, et sept fois plus que le GCHQ. En outre, la NSA emploie des sous-traitants privés pour assurer une partie de son travail, de sorte qu'elle peut être amenée à employer douze à seize fois plus de personnes que toute autre agence. Le ratio est équivalent en termes de budget. La NSA a un budget de 7 milliards d'euros par an, tandis qu'en Europe, le GCHQ – avec 1,2 milliard d'euros – a un budget annuel plus de deux fois supérieur à celui de toute autre agence européenne, qu'il s'agisse de la BND, de la FRA ou de la DGSE. Plutôt que d'analyser le réseau comme une collaboration États-Unis-UE équilibrée, voire comme une collaboration transatlantique corrélée à l'OTAN, il serait sans doute plus exact de parler de guilde de professionnels anglo-américaine étendue à d'autres services de renseignement occidentaux. La force de cette guilde résiderait dans la forte solidarité née après la Seconde guerre mondiale entre des pays acceptant l'hégémonie américaine. Les fameux « Cinq yeux » (abrégé FVEY, incluant les États-Unis, le Royaume-Uni, le Canada, l'Australie, la Nouvelle-Zélande) constituent un réseau de services de renseignement, récemment étendu à la Suède, avec une ouverture possible à la France et à l'Allemagne. Ce réseau semble avoir été le principal moyen pour la NSA d'étendre sa surveillance au-delà de ses propres capacités techniques pour que sa portée soit globale (en particulier par le biais des câbles internet sous-marins). Ce réseau de professionnels de l'information sensible a fonctionné comme un nœud de collecte et de partage de données, donnant ainsi l'impression d'être engagé dans une collaboration réciproque forte et de par-

10. Bigo D., "The Transnational Field of Computerised Exchange of Information in Police Matters and Its European Guilds", in Kauppi N. et Madsen M. R. (eds.), *Transnational Power Elites: The New Professionals of Governance*, Londres, Routledge.

tager un objectif commun, l'antiterrorisme. Les révélations de Snowden montrent toutefois que cette relation est structurellement asymétrique en termes d'exploitation de données et de renseignement. Loin d'un flux homogène d'informations, les relations de pouvoir structurent le jeu.

De multiples sites de résistance

Certains partenaires de la NSA ont été choqués par la manière dont ils ont été dupés et transformés en simples instruments alors qu'ils se pensaient partenaires (l'Allemagne, la Pologne, la Suède, les Pays-Bas et même la France). La confiance entre les services, qui était certes limitée mais réelle au nom de la lutte contre le terrorisme a quasiment disparu lorsqu'il est devenu clair que les analystes de la NSA avaient eu recours à un espionnage « politique » et « industriel », à l'exploration des données personnelles de larges pans des populations d'autres pays dans le but de profiler l'évolution des choix de consommation et même les opinions politiques pour des élections à venir. Cela a aussi inclus un espionnage des populations des pays alliés et collaborant avec le réseau des « Cinq yeux + ». Ces pays ont compris que leur collaboration en vue de renforcer la sécurité nationale des États-Unis avait pu compromettre leur propre sécurité nationale et leurs intérêts, avec leur complicité « involontaire ».

La question de la loyauté a ainsi été soulevée car les services pourtant en charge de la sécurité nationale ont mis les nations en danger en communiquant des informations à la NSA. Le Royaume-Uni s'est retrouvé dans une situation particulièrement délicate lorsqu'il a été prouvé que le GCHQ s'était montré agressifs envers d'autres partenaires et des institutions européennes [11] alors même que le pays est membre de l'Union européenne (UE) et signataire de son traité qui requiert la loyauté des États membres.

De la même manière, les révélations selon lesquelles la NSA aurait mis en place des fichiers qui ne devaient pas être vus par des « yeux britanniques » du fait de leur importance et de leur rôle contre les intérêts britanniques ont provoqué un certain malaise au sein de services de police britanniques ainsi qu'un sentiment de trahison, de perte, comme si le Royaume-Uni ne jouissait plus d'une position privilégiée auprès des États-Unis.

De ce point de vue, par un effet boule de neige, les révélations d'Edward Snowden ont alimenté la méfiance à l'égard des effets soi-disant positifs de l'échange de données avec la NSA. Elles ont aussi poussé certains fournisseurs privés comme Orange à vérifier leurs infrastructures techniques, ce qui les a amenés à découvrir que les technologies utilisées par la NSA pour récolter les

11. Le GCHQ a été accusé de s'être introduit chez Belgacom afin d'espionner la Commission européenne et le Parlement, une opération dont le nom de code était « socialitst » et menée via la technique « *quantum insert* ».

données souhaitées (c'est-à-dire presque toutes) étaient doubles : dans un premier temps, en sollicitant une collaboration sur des questions raisonnablement légitimes (principalement du ressort de la lutte contre le terrorisme ou de la lutte contre le crime organisé), puis, en introduisant de manière frauduleuse des outils dans les systèmes de ses collaborateurs, en particulier ceux récemment agrégés au nœud principal (la France, l'Allemagne, la Suède, les Pays-Bas et potentiellement le Brésil).

Les hommes et les femmes politiques de ces pays ont été pris en tenaille entre d'une part leur soutien officiel au besoin de collecter des données contre le terrorisme, leur américanophilie, des arguments en faveur d'une alliance commune, et d'autre part le comportement agressif de la NSA. Si les dirigeants sont dans l'ensemble parvenus à réduire au silence les réserves exprimées par certains opérateurs au sein du réseau (certains juges enquêteurs, par exemple), ils n'ont pas convaincu l'ensemble des fournisseurs privés et encore moins la société civile et les différentes ONG. Des centaines de requêtes judiciaires ont ainsi été déposées par des acteurs très différents aux objectifs tout aussi différents et il paraît difficile d'empêcher leur multiplication, sauf à entreprendre une réforme de fond.

Les jeux des États autour du ruban de Moebius

La transformation des lignes territoriales en ruban de Moebius réarticule les jeux souverains habituels entre États. Si le *big data* brouille les catégories de « l'interne » et de « l'externe », la reconfiguration consécutive des frontières de l'État souverain en un ruban de Moebius est, à son tour, devenue un site en soi de luttes politiques, de résistance et de dissidence. Le ruban de Moebius permet à ses bords plusieurs types de jeux entre les États, les mouvements sociaux et les individus, autour du sens de la souveraineté et de la citoyenneté, de la sécurité et de la liberté. Dans le cas des États, les réactions à la surveillance de masse sont allées de revendications de respect des droits universels à la reconstitution des frontières territoriales souveraines, de la « numérisation » de la sécurité à la numérisation de la géopolitique. Plusieurs aspects de la réaction récente du gouvernement brésilien contre les techniques de surveillance de masse sont exemplaires de ces différents jeux étatiques le long du ruban de Moebius. La section qui suit abordera ces jeux et montrera comment ils façonnent les luttes politiques autour de la raison d'État adaptée aux nécessités de l'ère du numérique [12].

12. Note de la traductrice : ci-après « raison d'état numérique. » (« *digitized reason of state* » en anglais).

Comment ramener le ruban de Moebius vers les lignes souveraines ?

Les révélations d'Edward Snowden à propos des opérations de surveillance de la NSA au Brésil – y compris l'écoute du téléphone portable de la présidente Dilma Rousseff ou encore la collecte de données sur la compagnie pétrolière nationale et sur des citoyens brésiliens sans distinction – ont poussé à certaines actions et ce dans plusieurs domaines. Ainsi, en plus d'avoir reporté sa visite officielle aux États-Unis prévue en octobre 2013, la présidente Rousseff a consacré son discours d'ouverture devant l'Assemblée générale des Nations unies à la question de la surveillance de masse ou, comme elle l'a qualifiée, d'« un réseau d'espionnage électronique global ». Ce discours condamne les pratiques de la NSA pour deux raisons : violations des droits de l'homme et « non-respect de la souveraineté nationale ». Le résultat le plus remarquable de ce discours fut la reconnaissance de droits à la vie privée au sein du Comité pour les droits de l'homme de l'ONU et lors de l'Assemblée générale et ce avec le soutien du gouvernement allemand. Si la résolution ne mentionne pas les États-Unis de manière explicite, sa rédaction a permis de censurer les pratiques de surveillance de masse des agences américaines.

Toutefois, ce qui distingue cette réaction des accusations de violation des souverainetés nationales (exprimées par de nombreux gouvernements, y compris ceux du Brésil et de l'Allemagne), c'est la scène où elle a eu lieu et le vocabulaire employé. Aux Nations unis, les États sont censés employer un vocabulaire universel, permettant ainsi l'expression de revendications de reconnaissance de la vie privée comme un droit humain. L'adoption d'un vocabulaire universel déstabilise le cœur des pratiques de surveillance de masse, ramenant au premier plan les manières dont elles constituent leur principal objet d'attention : la « personne concernée ». La « personne concernée » a une forme d'existence conditionnelle au sein de réseaux numériques. L'observation et l'analyse de comportements spécifiques rendent possible la réalisation de profils génériques et l'identification de menaces et de cibles. De fait, le degré de séparation entre le sujet et une cible identifiée entraîne des techniques de surveillance spécifiques et définit les droits auxquels « la personne concernée » peut prétendre. Sous le régime de la raison d'État numérique, les droits individuels sont conditionnés par un ensemble spécifique de relations et par des positions particulières que le sujet occupe au sein de ces réseaux aux contours flous. Les « personnes concernées » sont identifiées et auscultées en fonction de leur position particulière. Leurs droits dépendent de la distance observée entre elles et les cibles. Cette articulation des positions est en désaccord avec les diverses hypothèses du cosmopolitisme qui sous-tendent la campagne en faveur des droits universels menée par les gouvernements brésilien et allemand. Leurs tentatives de rétablir des droits individuels et, *in fine*, l'idée régulatrice d'un sujet autonome – contre la raison d'État numérique – peuvent paraître datées, voire conservatrices. En ce sens, les débats

politiques qui ont eu lieu à l'Assemblée générale des Nations unies ont avant tout été une lutte entre deux modes d'existence : celui de la « personne concernée » et celui d'un sujet cosmopolite aux droits universels. Néanmoins, la tendance cosmopolite de la résolution des Nations unies était une manière de respecter les promesses de l'international moderne, non seulement par la sauvegarde de l'autonomie individuelle mais aussi par l'affirmation que les États sont responsables de sa protection. Des États comme le Brésil et l'Allemagne ont tenté de remettre le ruban de Moebius dans les lignes territoriales souveraines afin de lutter contre les pratiques de surveillance de masse.

Reste que la tendance cosmopolite n'a pas été promue au détriment de la souveraineté étatique, du moins pas dans le cas du gouvernement brésilien. Dans le cadre de ce jeu particulier, l'affirmation d'un vocabulaire cosmopolite autorise l'État à agir pour protéger les droits de ses citoyens, y compris le droit à la vie privée, et pour protéger les données, comme nous le verrons plus tard. À l'ONU, le jeu des autorités brésiliennes vise en réalité à tenter de réconcilier une certaine autonomie individuelle, la souveraineté de l'État et les droits universels. Si ce jeu stratégique peut remettre en cause les fondations de la raison d'État numérique, les techniques mobilisées et finalement déployées pour protéger les droits des citoyens risquent de la renforcer effectivement. Partant de l'idée que la vie privée est un droit humain, les autorités brésiliennes soutiennent la création d'un accord multilatéral et multipartite qui soit « capable de garantir la liberté d'expression, la vie privée des individus et le respect des droits humains [13] ». Cette même revendication autorise toutefois le gouvernement brésilien à « faire tout ce qui est en son pouvoir pour défendre les droits humains de tous les Brésiliens et de tous les citoyens du monde et protéger les fruits de l'ingéniosité de [ses] travailleurs et de [ses] entreprises ». Ce que la présidente Dilma Rousseff avait en tête était un ensemble de mesures nationales visant à renforcer les capacités du Brésil à protéger la vie privée de ses citoyens contre la menace de surveillance de masse américaine [14]. Si la régulation multilatérale du cyberespace et la capacité nationale à protéger la vie privée des citoyens peuvent se compléter, ce développement de techniques nationales de protection peut entraîner un nouveau jeu : la géopolitique numérique.

Raison d'État et géopolitique adaptées aux nécessités de l'ère du numérique

Parmi les politiques annoncées par le gouvernement brésilien pour se prémunir des menaces américaines liées aux techniques de surveillance de masse, on trouve l'amélioration de la connectivité internationale et la production de contenu national. Selon les autorités brésiliennes, la création de contenus

13. Discours de la présidente de la République du Brésil, Dilma Rousseff, à l'ouverture du débat général du Sommet de la 68e Assemblée générale des Nations unies, 24 septembre 2013.
14. Al Jazeera, "On Internet, Brazil is beating US at its own game", 20 septembre 2013 (http://america.aljazeera.com/articles/2013/9/20/brazil-internet-dilmarousseffnsa.html).

nationaux, comme un service de messagerie électronique ou un réseau social national permettrait aux citoyens brésiliens de garder leurs données sur le territoire national. Le débat autour de la création d'un « *cloud* » de données européen soulève le même type de questions car en effet, la réaction des autorités brésiliennes n'est pas isolée. Les autorités néerlandaises ont ainsi tenté de garder les données gouvernementales en dehors de la portée des entreprises américaines, tandis que l'Union européenne discute des possibilités d'isoler le stockage de données des techniques d'exploration américaines. De son côté, le gouvernement allemand tente de maintenir un trafic local en prévenant ses internautes lorsqu'ils quittent le cyberespace européen. Faut-il encore mentionner la grande muraille pare-feu de la Chine ou l'« Internet Halal » iranien ? Dans chacun de ces cas, les États renforcent leurs frontières numériques. S'il ne faut pas minimiser les différences entre ce que font les autorités brésiliennes, allemandes ou chinoises, dans chaque cas il est nécessaire de construire une infrastructure massive, sans compter le nécessaire déploiement de technologies, de législation, d'expertise pour protéger les données, contrôler le trafic ou encore surveiller. En plus de ces investissements visant à garantir les capacités des États en matière de protection ou de surveillance, les professionnels de la sécurité et du renseignement doivent être mobilisés pour gérer les systèmes nationaux.

En construisant leur forteresse dans les nuages, les États passent d'une tendance cosmopolite au jeu stratégique. Si le premier mouvement a consisté à revendiquer des droits universels, la partie stratégique implique des revendications de souveraineté d'État, ou, dans ce cas précis, d'une cyber-souveraineté. Toute référence aux droits universels tend à disparaitre dans ces jeux stratégiques et se voit remplacée par un raisonnement stratégique ancré dans l'incertitude et la peur. Ce sont les concepts d'intérêt national, de sécurité nationale ou étatique, d'espionnage et de guerre qui refont surface quand les représentants d'un État soutiennent publiquement les politiques et les techniques mises en oeuvre pour protéger leur société. Le cyberespace se voit décrit comme un espace américano-centré et le cyber-pouvoir américain doit donc être rééquilibré grâce au développement de cyber-capacités nationales ou de coalitions internationales.

Dans le cas du Brésil, les tentatives d'étendre la connectivité Internet internationale (au sein de l'espace régional mais aussi à l'échelle globale) sont compatibles avec l'idée de protéger les données nationales et de constituer un contrepoids à la position américaine au sein du cyberespace. Le programme comprend trois initiatives articulées : l'installation de câbles transatlantiques à fibre optique – dont un certain nombre entre États du Sud ; un programme satellite visant à lancer un « satellite géostationnaire de défense et de communications stratégiques » en 2016 ; et, finalement, un câble à fibre optique terrestre entre les pays d'Amérique du Sud. Un des premiers gestes de ce jeu stra-

tégique a été l'annonce d'un câble connectant les BRICS, indépendamment des États-Unis [15]. Chaque initiative brésilienne articule plusieurs services gouvernementaux et des entreprises brésiliennes ou transnationales ; chaque projet est transnational par nature [16]. Ce nouveau jeu donne lieu à l'expansion de cette raison d'État numérique ; au lieu de se soustraire au ruban de Moebius, les États y mènent un jeu géopolitique. La géopolitique numérique suppose que le cyberespace soit un champ de bataille et que les États doivent renforcer leurs propres cybercapacités pour se défendre et/ou s'engager dans des coalitions internationales pour faire face aux défis posés par la surveillance massive et l'espionnage numérique. L'effet paradoxal de ce jeu particulier semble être que la résistance des États à cette surveillance de masse renforce, *in fine*, le régime de la raison d'État numérique. Les États reproduisent l'opposition entre la sécurité et la liberté lorsqu'ils jouent ce jeu géopolitique numérique et, ce faisant, risquent d'inclure la citoyenneté et les droits dans la logique positionnelle de la personne concernée. En luttant contre la surveillance de masse, les États risquent de créer eux-mêmes les conditions appropriées à la conduite d'une surveillance de masse.

Droits de l'homme et vie privée à l'âge de la surveillance : le pouvoir du droit international

Les révélations d'Edward Snowden n'ont pas seulement eu des répercutions politiques substantielles en 2013 et 2014, elles ont aussi soulevé de profondes questions juridiques. Cette section examinera certaines de ces questions dans la perspective des actions politiques qui les entourent. Nous limiterons les détails juridiques au minimum en nous concentrant sur leurs effets par rapport aux relations internationales tempétueuses que ces révélations ont entraîné.

Deux questions liées aux droits de l'homme ressortent lorsqu'il est question de surveillance de masse. Elles sont interconnectées, mais séparées. La première, qui est la plus fondamentale mais la plus souvent ignorée, est celle du droit de chaque individu au respect de sa vie privée et de celle de sa famille. La seconde, qui fait généralement plus de bruit politique et médiatique, est celle du devoir des États de protéger les données personnelles.

Les acteurs politiques qui trouvent un intérêt à mettre en avant la légalité ou non de la surveillance de masse usent généralement de deux arguments : le

15. "Experts see potential perils in Brazil push to break with US-centric Internet over NSA spying", Associated Press, 17 septembre 2013.
16. Les entreprises de télécom brésiliennes construisent les câbles sous-marins grâce à des financements publics ou internationaux. C'est le cas du *South Atlantic Express cable* qui connecte le Brésil et l'Afrique du Sud grâce à des fonds de la Bank of China. Le satellite est un partenariat (*joint venture*) entre Telebras (entreprise publique brésilienne) et Embraer (entreprise publique brésilienne) avec une technologie franco-italienne (Thales Alenia). Voir Al Jazeera, "On Internet, Brazil is beating US at its own game", *art. cit.*

premier affirme que la sécurité nationale et internationale est toujours une exception faite au devoir de chaque État de respecter la vie privée des citoyens et de respecter les données personnelles. Il s'agit là de l'argument défendu avec le plus de force, car s'il tombe, les acteurs cherchant à justifier la surveillance de masse se trouvent sur des bases légales très fragiles. Le second argument énonce que les obligations des États à respecter les données personnelles sont sujettes à des règles et des exigences différentes selon les préférences politiques des différents États. Ainsi, puisqu'il n'y a pas d'harmonisation des règles spécifiques de ce qui est acceptable ou non en termes de protection des données, les États qui exercent leurs prérogatives de sécurité nationale et internationale ne respectent que leurs propres règles de protection des données.

Le droit à la vie privée et le droit à la protection des données

Avant d'aborder directement les arguments et la manière dont les acteurs politiques mécontents y ont répondu, il s'agira de clarifier très brièvement la relation entre le droit au respect de la vie privée et celui de la protection des données. Le droit au respect de la vie privée de la personne est le droit international ultime, énoncé dans la Déclaration universelle des droits de l'homme de 1948 [17]. Sa forme juridique se trouve dans le Pacte international relatif aux droits civils et politiques (PIDCP) signé aux Nations unies en 1966 [18]. Toute interférence dans la vie privée d'une personne doit avant tout faire l'objet de son consentement. Le droit au consentement ou au refus de l'utilisation de ses données personnelles appartient à la personne, non pas à l'État. Le consentement ne vaut d'ailleurs que si l'individu sait précisément ce à quoi il consent. Cet aspect du droit requiert qu'il y ait des limitations dans l'objectif de la collecte et de l'utilisation des données personnelles et interdit le dérapage, c'est-à-dire l'utilisation des données à d'autres fins que celles envisagées. Lorsque un État cherche à interférer avec le droit en collectant et en se servant de données personnelles – ce qui constitue donc une immixtion dans la vie privée de la personne concernée – il doit justifier son interférence. D'abord, cela doit être autorisé par la loi, qui doit elle-même être suffisamment claire et publique pour que tout le monde puisse la connaître et que chacun puisse modifier son comportement en fonction. Toute exception autorisée par la loi à l'un des droits de l'homme doit être interprétée strictement. Elle doit avoir un objectif légitime et être nécessaire pour atteindre cet objectif seulement. Il ne doit exister aucune autre option moins intrusive dans la vie privée de la personne concernée. Toute ingérence de l'État doit faire l'objet d'un contrôle judiciaire

17. Article 12 : Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes (www.un.org/fr/documents/udhr/#a12).
18. Article 17(1) : Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation (https://treaties.un.org/doc/Publication/UNTS/Volume%20999/volume-999-I-14668-French.pdf).

et toute personne affectée par une telle ingérence doit avoir accès au droit pour la contester. Par sa nature même, la surveillance de masse ne vise pas une personne en particulier, ce qui rend extrêmement difficile la justification d'une immixtion dans la vie privée d'un individu. Lorsque de telles techniques de surveillance de masse et sans cible précise ont été utilisées en Europe, la Cour européenne des droits de l'homme ne les a pas jugées non-conformes au droit au respect de la vie privée. Arbitraire, la surveillance de masse l'est par définition. Le devoir des États à protéger les données dérive du droit de la personne au respect de sa vie privée. Lorsque les États interfèrent dans la vie privée des individus, ils doivent respecter des règles strictes pour que ces immixtions puissent être justifiées. En outre, les États ont le devoir de garantir que les acteurs du secteur privé ne font pas intrusion dans la vie privée d'une personne et doivent donc réguler la collecte et l'utilisation des données personnelles par le secteur privé. Cela donne lieu à l'obligation de la protection des données.

Le devoir de protéger des données personnelles apparaît lorsque des données personnelles sont utilisées par des acteurs étatiques ou du secteur privé et vise à garantir que cette utilisation respecte le droit de l'individu au respect de sa vie privée. Ceci explique pourquoi il y a plusieurs types de régimes de protection des données, en fonction du pays. Peu importe la manière – ce sont les États qui décident de comment ils vont protéger les données – l'essentiel est que les données soient protégées puisque l'individu a droit au respect de sa vie privée. Le contenu du droit humain à la vie privée est invariable.

La position américaine au regard du droit international relatif aux droits de l'homme et l'initiative germano-brésilienne

Se démarquant de plus en plus d'une acceptation universelle des droits de l'homme et sommées de répondre à la crise politique autour de la surveillance de masse opérée par leurs agences, les autorités américaines font face à un véritable dilemme en droit international des droits de l'homme, un domaine où elles se sont toujours montrées plutôt méfiantes. L'approche promue dans les années 1950 revenait à dire que les instruments ne faisaient rien de plus qu'établir des principes, qu'ils n'instituaient pas de « vraies » règles de droit et qu'ils n'étaient en aucun cas des outils coercitifs dont les individus pouvaient se saisir. Cette posture politique a été minée par le développement d'obligations internationales très précises et l'établissement d'organes conventionnels dont la mission est de recevoir et de traiter les plaintes déposées par des individus concernant des violations présumés de leurs droits humains et de faire appliquer le droit international des droits de l'homme par les juridictions nationales. Le droit international des droits de l'homme ne peut plus être considéré comme un simple recueil de principes ; cet argumentaire n'est qu'un voile de pudeur jeté occasionnellement par des États cherchant à agir de manière arbitraire.

Les révélations d'Edward Snowden ont contribué à porter la question de la surveillance de masse à l'échelle internationale, et un certain nombre d'États, menés par le Brésil et l'Allemagne, ont commencé à s'interroger sur la manière d'aborder l'interception des communications par les États-Unis. Il a alors beaucoup été question de négociations bilatérales et d'actions unilatérales (comme celle, susmentionnée, consistant à installer de nouveaux câbles évitant le territoire américain). Toutefois, on s'est rapidement rendu compte que ces approches bilatérales ou unilatérales ne pouvaient être satisfaisantes. Le fait que les autorités britanniques aient mené des actions de surveillance de masse pour leurs partenaires américains et consorts (les « Cinq yeux ») tout en étant membres du Conseil de l'Europe et de l'UE ne représente qu'un exemple parmi d'autres du problème posé par ce type d'approche. Pour la plupart des acteurs, il est apparu clairement que seuls des efforts multilatéraux pouvaient s'avérer payants là où le poids des États-Unis et de certains de leurs partenaires pouvait être contrebalancé par une alliance souple entre d'autres États. Posée en ces termes, l'équation semble évidente : toute action doit être initiée au sein de l'Assemblée générale des Nations unies, et le terrain dans lequel elle doit s'ancrer est celui des obligations internationales liées aux droits de l'homme – l'interdiction d'une immixtion arbitraire dans la vie privée des individus.

Tel est le chemin choisi et suivi par les autorités brésiliennes et allemandes. Dès le mois d'août 2013, une résolution de l'Assemblée générale était en préparation, avec la participation de cinq organisations non gouvernementales (Access, Amnesty International, Electronic Frontier Foundation, Human Rights Watch and Privacy International) qui œuvraient en faveur d'un texte ferme. De nombreux petits États comme l'Autriche, la Hongrie, le Lichtenchtein, la Norvège ou encore la Suisse ont soutenu cette entreprise avec force, parfois même en détachant du personnel pour faire face à la charge de travail. La question fut assignée au Troisième comité de l'Assemblée générale, et c'est dans ce cadre que ce sont déroulées les négociations tendues sur les termes utilisés dans la résolution. Le texte a été adopté le 26 novembre par le Troisième Comité, puis le 18 décembre 2013, sans vote, par l'Assemblée générale des Nations unies.

La résolution est fondée sur le droit au respect de la vie privée de la Déclaration universelle et du PIDCP, avec référence spéciale à l'interdiction de toute immixtion arbitraire. Elle lie droit à la vie privée et liberté d'expression – si les individus sont soumis à une surveillance de masse, ils ne sont plus libres de s'exprimer (autrement qualifié d'« effet paralysant », *chilling effect*). Son préambule insiste sur les effets négatifs de la surveillance et de l'interception des communications, y compris de la surveillance et des interceptions extraterritoriales, lorsqu'elles sont massives, sur l'exercice et le bénéfice des droits humains. La résolution appelle les États à respecter le droit à la vie pri-

vée et à éviter toute violation ; à évaluer et revoir leur procédures, leurs pratiques et leurs lois sur la surveillance des télécommunications, leurs interceptions et les collectes de données, à faire respecter le droit à la vie privée et à garantir la mise en œuvre pleine et effective de toutes leurs obligations liées au droit international des droits de l'homme, ainsi qu'à établir ou maintenir des mécanismes de contrôle nationaux indépendants et capables de garantir la transparence et l'action responsable des États.

La résolution – et c'est peut-être ce qu'il faudra retenir en priorité – ordonne au Haut Commissaire aux droits de l'homme de présenter un rapport sur la protection et la promotion du droit à la vie privée dans le contexte d'une surveillance nationale et extraterritoriale et/ou d'interception de communications numériques et de collecte de données personnelles, y compris à grande échelle. Ce rapport sera présenté au Conseil des droits de l'homme, à l'occasion de sa 27e session (septembre 2014) [19]. À cette période, et jusqu'en septembre 2014, la Haute Commissaire aux droits de l'homme était Navi Pillay, une juriste sud-africaine dont la carrière a toujours été fortement marquée par la question des droits de l'homme et pour qui la question du droit à la vie privée face à la surveillance de masse n'est pas inconnue. Le Conseil des droits de l'homme de l'ONU (composé de quarante-sept États élus par l'Assemblée générale) avait mis la question au programme de la 24e session du Conseil, en septembre 2013. C'est en effet à l'occasion de cette rencontre que le Haut Commissaire avait noté que la surveillance était l'une des menaces les plus préoccupantes en termes de respect des droits de l'homme dans le monde. Lors de cette session, de nombreux représentants des États avaient alors porté un intérêt certain au rapport annuel présenté par Frank La Rue, le rapporteur spécial des Nations unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression à l'âge de l'Internet [20]. À l'époque, ce rapport avait déjà souligné les nombreux dangers de la surveillance étatique et ses conséquences négatives sur la liberté d'expression. Ce qui est surprenant, en revanche, c'est le peu de couverture médiatique que les rencontres du Conseil des droits de l'homme de septembre et décembre 2013 ont suscité. De fait, les représentants étatiques ont été nombreux à assister aux réunions et les discussions autour de la condamnation de la surveillance de masse et de l'interception des communications ont été enflammées. Nombre des déclarations sanctionnant ces pratiques avaient été préparées à l'avance et validées par les États voisins au nom desquels ces représentants avaient été habilités à parler. S'il peut sembler naturel que l'Allemagne ait été choisie pour représenter l'Autriche, la Hongrie, le Lichtenstein, la Norvège et la Suisse, il est plus surprenant que le Pakistan, parlant au nom de Cuba, du Venezuela, du Zimbabwe, de l'Ouganda, de l'Équateur, de la Russie, de l'Indonésie, de la

19. Note de la traductrice : le rapport, publié depuis la rédaction de cet article, est disponible à l'adresse suivante : www.un.org/french/documents/view_doc.asp?symbol=A/HRC/27/37
20. Rapport du 16 mai 2011, accessible sur http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

Bolivie, de l'Iran et de la Chine présente également un texte collectif condamnant ces pratiques. Si la réponse aux condamnations, en particulier à l'égard de ce second groupe d'États, a généralement consisté à dénoncer leurs pratiques nationales et à les soupçonner, pour ne pas dire les accuser d'hypocrisie, le fait qu'un groupe de pays connaissant habituellement de profonds désaccords ait pu trouver un terrain d'entente sur ce sujet et qu'ils soient intervenus mérite d'être souligné. L'étape suivante sera la présentation d'un rapport par le Haut Commissariat, en septembre 2014. Il va sans dire que l'équipe de la Commissaire recevra de nombreuses informations, de nombreuses preuves et de nombreux arguments juridiques lui permettant de rédiger le rapport [21].

Renseignement, démocratie, souveraineté : quel *demos* pour quelle société ?

La documentation rendue disponible par Edward Snowden et d'autres nous a permis d'en savoir plus sur le caractère et l'étendue des pratiques de collecte de renseignement des différentes agences en charge de l'amélioration de notre sécurité. Nous n'avons pas de certitudes sur ce que nous savons ou ne savons pas, et ce que représente notre connaissance limitée. Cela bouscule tant les analyses scientifiques que notre idée de la manière dont nous devrions réagir par la mise en œuvre de politiques, de procédures, d'institutions et d'actions collectives. On peut être gêné, ou non, par ce qui a été rendu public, mais ces révélations bousculent sans nul doute les perceptions conventionnelles de ce que cela veut dire de penser les pratiques de la sécurité, au-delà de la sécurité elle-même. D'un autre côté, l'éternelle suspicion selon laquelle les agences prétendant agir pour notre sécurité et notre bien-être sont en fait extrêmement dangereuses porte en elle une grande sagesse.

C'est dans ce contexte précis que nous pouvons apprécier les premières réactions aux conséquences immédiates des pratiques identifiées. En dépit de leur application imparfaite, les principes de vie privée, de droits de l'homme et d'État de droit sont profondément ancrés dans nos sociétés modernes, en particulier lorsqu'ils affirment une forme de libéralisme. Snowden a prouvé à maintes reprises que de telles avancées étaient méprisées, que ce soit par des actions volontaires voire même complotistes, par ignorance ou naïveté, ou encore au travers de processus structurels que personne ne comprend vraiment. En outre, ce mépris s'est étendu aux amis comme aux ennemis, aux citoyens d'un État comme aux étrangers, par des biais qui généralisent le soupçon et remettent en cause tout ce que nous pensions savoir sur le rôle de la conscience individuelle, la liberté d'expression, l'innocence et la culpabilité, la liberté et la responsabilité, le public et le privé. Les apôtres de formes de sécurité plus intrusives et secrètes invoquent souvent des récits extrêmes sur les menaces qui pèseraient sur nous, mais il semble tout aussi facile d'imaginer

21. Voir note 19.

des récits tout aussi extrêmes sur l'éviscération des formes de subjectivité moderne et d'autodétermination qui donnent aux agences de sécurité une grande partie de leur légitimité. Après tout, que sont-elles censées sécuriser ? Il est peu probable que la réponse spontanée des professionnels de la sécurité à cette question soit la « démocratie », en dépit de la rhétorique d'un certain nombre de dirigeants politiques. L'État ou la nation serait alors préféré : la condition de possibilité d'une collectivité de citoyens ancrée dans une localisation géographique spécifique qui parvient ou non à instaurer des formes démocratiques de gouvernance ; ou, peut-être, le système international qui serait la condition de possibilité de cette condition de possibilité ; ou sans doute plus précisément les interactions délicates ou maladroites des États dans un système d'États qui nous offre la possibilité de réconcilier nos revendications de citoyennetés ou de nationalités particulières avec notre statut universel d'êtres humains.

Des perceptions traditionnelles de la sécurité peuvent se trouver tiraillées entre les camps nationalistes et internationalistes, entre la sécurité nationale et la sécurité collective, comme dans la Charte des Nations unies. Cependant, les faiblesses évidentes des deux camps ne servent qu'à souligner leur interdépendance comme expression des principes concurrents d'autodétermination et d'universalité qui façonnent la vie politique moderne. Ici, l'une des principales difficultés vient du fait que certains États – un seul État dans le cas présent – agissent comme s'ils étaient à la fois particuliers et universels, de simple États ayant un problème de sécurité nationale mais aussi des puissances hégémoniques mondiales responsables de quelque chose de plus global. Reste que les processus économiques ne sont pas simplement subsidiaires à l'ordre politique international des États, ce qui peut par ailleurs compliquer la donne.

Ce qui est particulièrement intéressant à propos des modèles qui ressortent des informations révélées par Snowden est la possible confirmation d'affirmations selon lesquelles nous vivons dans un monde qui n'est organisé ni au sein d'États agissant dans un système d'États, ni selon une hiérarchie embryonnaire telle qu'envisagée par les théoriciens de la mondialisation, de la gouvernance mondiale, etc., ni sur le modèle d'un nouveau type d'empire ou de concert de grandes puissances. De plus, il semble imprudent de présupposer que ces modèles puissent être compris sans qu'on ait appréhendé d'une manière ou d'une autre les transformations contemporaines faisant des marchés mondiaux et de la santé des entreprises les mesures premières de la valeur économique et politique. Certaines réponses aux révélations d'Edward Snowden suggèrent que l'ancien modèle national/international est toujours vivace, même si nombre d'entre elles laissent entendre que quelque chose de moins prévisible est en cours. On peut voir des signes de cette imprévisibilité dans la manière dont les pratiques des agences de renseignement comme la NSA altèrent notre vision de la démocratie. Il est donc important dans ce

contexte de rappeler que la démocratie, comme d'autres formes de pluralisme politique, est quelque chose qui peut être limité, voire même sacrifié pour garantir l'ordre premier des États-nations dans un système d'États de ce type. Si nombre de récits apologétiques reproduisent cette tradition, ce qui ressort des récentes révélations n'est pas simplement la question traditionnelle de savoir quand il est possible de suspendre les normes démocratiques pour mettre en œuvre des opérations de sécurité plus efficaces ou d'opérer une stricte distinction entre un domaine civil où des normes démocratiques sont appropriées et un domaine sécuritaire où la démocratie doit céder la place. Ce qui ressort, c'est plutôt la réarticulation apparente des frontières entre les États d'une part, et entre l'État comme lieu de la nécessité politique et la société civile comme domaine de liberté politique et personnelle d'autre part ; ainsi, dans les deux cas, une limite entre des demandes de sécurité d'une part et les possibilités de liberté et d'autodétermination d'autre part. Si cela fait en effet partie du modèle qui émerge, le sens de la sécurité comme de la démocratie – et la relation entre les deux – se trouvera radicalement déstabilisée et pas forcément pour le mieux.

Quatre autres pistes d'analyses devraient venir s'ajouter aux questions que nous avons déjà soulevées sur la vie privée, l'État de droit et les tentatives de résistance aux prétentions impérialistes. Toutes concernent les limites des dichotomies qui sont reproduites, invariablement, dans les analyses conventionnelles et les débats publics, entre le national et l'international, l'État et la société civile, la liberté et la sécurité, la démocratie et le savoir. Le statut instable de la souveraineté est visible dans les quatre cas [22].

Premièrement, bien que cette conviction fonde encore des idéaux politiques largement partagés, notre monde politique n'est ni national ni international. La documentation révélée par Edward Snowden confirme que les incertitudes liées à la manière dont nous devrions comprendre la démocratie, du fait des dynamiques qui modifient les relations entre les États et entre État et société civile, fusionnent rapidement avec celles liées à la manière dont nous devrions localiser les ordres politiques qui se structurent en relation aux nouveau réseaux des agences de renseignement et de sécurité. Nous sommes loin de l'image classique des États de la sécurité nationale car ces réseaux sont diversement internationaux et transnationaux, et leurs cartographies ressemblent plus à des circuits électriques qu'à des propriétés territoriales. Les frontières sont devenues des phénomènes insaisissables, exigeant dès lors des manières différentes de comprendre les formes de subordination au sein de différents sous-systèmes, qu'il s'agisse des conflits d'allégeance et de citoyennetés divisées, ou de la dislocation du cadre spatiotemporel au sein duquel nous savons où nous sommes, quand nous sommes et qui nous sommes.

22. Pour des raisons déjà évoquées dans Walker R. B. J., *After the Globe, Before the World*, Londres, Routledge, 2010.

Pourtant, aussi insaisissables ou furtives soient-elles, elles ne s'effacent pas. Il est possible que la NSA et d'autres agences de renseignement travaillent dans le cadre de réseaux qui échappent à de nombreuses frontières, mais leur raison d'être est justement d'affirmer les limites de l'inclusion et de l'exclusion, qu'elles nous soient familières ou étrangères. L'ensemble des preuves des nouveaux schémas d'inégalité dans le monde devrait nous pousser à nous méfier sérieusement des perspectives de formes d'inclusion et d'exclusion inédites et déterminées par les nouvelles technologies de contrôle des populations.

Ensuite, l'un des éléments-clé de la démocratie dans le monde et au XXe siècle a été la distinction entre État et société civile et la distinction qui en découle entre privé et public. Ces distinctions ont souvent été troubles. De récentes révélations montrent toutefois une érosion encore plus soutenue de ces distinctions et le droit présumé des agences étatiques de pénétrer en profondeur dans le quotidien des vies privées et de la société civile. Cela ne prend pas la forme des États policiers totalisants que nous gardons en mémoire. Il est toutefois clair que les nouvelles procédures relatives aux opérations du renseignement, à la collecte de données, à la pratique de la suspicion et à l'identification des menaces potentielles – en particulier lorsqu'elles reposent principalement sur la manipulation informatique de preuves à la crédibilité empirique discutable et qu'elles se fondent sur des probabilités statistiques relatives à des populations abstraites pour identifier des individus particuliers – représentent un danger pour les libertés et les droits acquis qui est analogue aux régimes que nous nous plaisons à penser qu'ils sont révolus, enterrés par des révolutions, des démocratisations, des modernisations. Une partie de la difficulté analytique provient d'une double dynamique : d'un côté nous observons une interaction complexe entre les agences publiques et privées ; et de l'autre, nous avons la preuve de l'existence de réseaux d'agences de renseignement et de sécurité qui semblent avoir atteint un certain degré d'autonomie tant vis-à-vis de l'État que de la société civile ou, pour le dire en d'autres termes, tant vis-à-vis de la souveraineté étatique que de la souveraineté populaire.

Troisièmement, beaucoup trop d'analyses politiques ou de débats commencent aujourd'hui par la sécurité, comme si celle-ci était à la fois un problème et un principe qui existe en soi, voire même le principe premier qui prendrait le dessus sur tout le reste ; la tendance est fréquente, même au sein de la littérature dite « critique ». Et si certains ont insisté sur le fait que cette primauté était un fait simple (donc socio-darwinien), aucune discussion portant sur la démocratie moderne ou sur d'autres principes du politique moderne peut se permettre une telle erreur. Pour de nombreux auteurs canoniques que les études de la sécurité actuelles se sont appropriés (de Machiavel à Hobbes en passant par Kant, Clausewitz, Schmitt et même sur certaines versions du concept de sécurité nationale), les appels à la sécurité impliquent qu'il y ait quelque chose à sécuriser. Ce quelque chose se réfère généralement à une

communauté politique spécifique attachée aux principes de liberté et d'égalité au sein du territoire national et dotée d'une capacité d'autodétermination par rapport à d'autres communautés semblables. Mais ce qui est flagrant dans le contexte actuel est que cela a généré cette tension à long terme entre les appels à la liberté et les appels à la sécurité. Cette tension a été occultée par la division du travail intellectuel qui a transformé la sécurité en une spécialisation autonome à suivre sans grande considération, voire avec un mépris certain des « populations » au nom desquelles la sécurité est brandie comme un atout. Le caractère précis de cette tension s'est en outre vu dépolitisé par ces exigences répétées d'un « équilibre » à trouver entre les deux valeurs.

Reste que la relation entre liberté et sécurité ne peut se comprendre comme un équilibre ou une balance, au sens commun du terme. La sécurité nomme les conditions dans lesquelles la valeur première de la liberté doit trouver ses limites, les conditions dans lesquelles les hypothèses normales, les injonctions éthiques et les lois doivent être suspendues. Toute suspension de ce type est généralement du ressort de l'État souverain et en contradiction avec les responsabilités d'un peuple souverain. Par voie de conséquence, la relation entre ces visions antagonistes de la souveraineté doit être négociée. Selon certaines lectures influentes (autoritaire, totalitaire, fasciste), la négociation implique simplement une décision souveraine de suspendre la norme au nom d'un peuple ou d'une nation : la souveraineté de l'État doit l'emporter sur la souveraineté populaire. Les sociétés à tradition démocratique ont été contraintes de trouver certains arrangements avec les demandes en faveur de la sécurité comme condition limite, en insistant généralement sur un contrôle strict des décisions, une division du pouvoir institutionnel et une importance particulière accordée aux conditions juridiques dans lesquelles certaines lois peuvent être suspendues. Il n'est pas question ici de choisir entre plusieurs biens disponibles sur un marché. Les invocations rhétoriques relatives à l'équilibre obscurcissent et menacent ce qui se passe sur le lieu sans doute le plus important, le plus intense mais aussi le plus négligé de la pratique démocratique moderne. La voie est donc ouverte aux affirmations selon lesquelles les responsabilités de la souveraineté reviennent à ceux qui sont chargés de notre sécurité, et qu'il faut réduire l'espace de négociation ouvert à ceux qui doivent soi-disant être sécurisés. Étant donné l'éventail des menaces plausibles auxquelles les sociétés contemporaines sont confrontées, mais aussi et surtout la capacité d'un grand nombre d'agences de sécurité à mettre en avant certaines menaces plus que d'autres et à encourager l'idée d'un besoin de sécurité comme principe premier gouvernant nos vies, ce que l'on pouvait comprendre dans le passé comme des options autoritaires est aujourd'hui élaboré pour paraître désirable ou même naturel.

Enfin, et c'est là un point essentiel, les agences de renseignement et de sécurité font des demandes de « secret » dévastatrices. La démocratie a tou-

jours été liée à la qualité de la connaissance au sein du *demos* : de la *polis* grecque aux Lumières européennes, en passant par la valeur plus récemment octroyée à l'éducation, au journalisme d'investigation et à l'opinion publique, la plupart des conceptions de la démocratie reposent sur l'idée que les populations sont capables de penser et d'établir des jugements par elles-mêmes. Le culte du secret nous renvoie à de trop nombreux cas historiques à l'occasion desquels « le peuple » était jugé incapable de savoir ce qui était bon pour lui tandis que son souverain devait savoir autant de choses que possible sur la population dont il affirmait représenter la souveraineté. Mais alors, de quelle autorité parlons-nous ici ? Ou, pour reprendre la rhétorique hobbesienne, comment l'autorité est-elle autorisée à présent ?

Subjectivité et surveillance du cyberespace

La transformation du citoyen en suspect n'est pas un phénomène nouveau, comme nous le rappelle le discours de Hobbes sur la subversion et le pouvoir souverain. Si le monde de Hobbes est confiné à des territoires, celui des agences de sécurité de la modernité tardive est global et transnational. La différenciation qui est opérée entre le citoyen et le non-citoyen est visible à tout point de passage de frontière, lorsque le non-citoyen est soumis à une identification biométrique, une pleine exposition de son corps et à d'autres modes d'examens approfondis par lesquels le voyageur doit se résigner à de nombreuses subjectivations humiliantes. Il y a, dans ce régime de pratiques de sécurité, ce terrain du passage de la frontière, un certain processus d'apprentissage qui gouverne les comportements, nos seuils de tolérance face à ce type d'interventions et notre indifférence acquise, voire notre complicité, face au malaise de l'autre.

C'est cette indifférence que questionnent les révélations de Snowden ; le fait que les citoyens d'un État, dirigeants comme dirigés, tout être communiquant, tout utilisateur des technologies de notre modernité tardive soient désormais considérés suspects. Le concept de suspect s'est toutefois largement transformé car nous ne sommes plus en mesure de le limiter à son entendement juridique, c'est-à-dire en référence à un acte criminel, pas plus que nous ne sommes en mesure de le limiter à son itération socio-politique qui renvoie à l'idée d'inimitié ou de subversion potentielle.

Ce qui est clair, c'est que le sujet de la surveillance est à présent un sujet dont les pratiques de communication sont perçues par les agences comme ayant potentiellement une valeur ou une utilité informationnelles, lorsqu'en effet cette valeur peut être liée à la sécurité ou à l'économie. Nous ne sommes donc pas tous suspects, mais nos contributions en termes de données et de réseaux pourraient être jugées valables ou utiles, dans le futur. Dès lors que le sujet communique dans le cyberespace, il peut être conscient du fait que le

réseau de communication qu'il utilise est plus ou moins surveillé, enregistré, stocké. Reste qu'on ne connaît pas assez l'utilité informationnelle que ces agences de surveillance attribuent à nos communications. La question de savoir comment la surveillance de masse des communications influe sur nos comportements est certes pertinente, toutefois, tout comme le voyageur s'adapte et se conforme aux exigences liées aux déplacements, il y aura ici une certaine adaptabilité et une créativité qui s'exprimeront au travers de cette gouvernementalité de soi qui prévaut face à l'intensification des pratiques de surveillance de notre modernité tardive.

C'est dans le cyberespace que cette intersection complexe entre le public et le privé est la plus visible. Il y a là tant l'intimité que la présence publique. L'intime prévaut pourtant et en dépit du fait que le sujet des pratiques de cybercommunication soit pleinement conscient de l'ouverture de cet espace au monde, il est vulnérable face au regard de l'étranger, pourquoi pas du pirate, du publicitaire ou même de l'État. L'« être numérique [23] » est un être connecté et rhizomique présent dans ce terrain distinctif d'interaction sociale, un espace dessiné et permis par des codes en réseau qui ne reconnaissent aucune limite en tant que telle, si ce n'est la limite technique. Le cybersujet est pensé et configuré comme un être qui émerge et qui est produit par des formes de performativité désincarnées qui viennent à constituer le cyberespace [24]. Luke suggère ainsi que le cyberespace peut s'entendre comme une « structure sociale » où se produisent de « nouvelles subjectivités » et des nouvelles formes d'action (*forms of agency*). Il pourrait toutefois être plus opportun d'analyser ce terrain comme la manifestation d'un espace dont la cartographie montre un ensemble multiple de lignes et de nœuds se recouvrant et se croisant, reflets des milliards de communications dans le monde. Or au sein de cette complexité rhizomatique, la « conscience pratique » de l'être numérique suppose une intimité en dépit de tout.

Ce qui est souvent présenté comme un changement générationnel indique un soi-individu qui révèle tout, et pas uniquement à ses amis ou sa famille, mais potentiellement à tous les « clients » des réseaux sociaux. L'hypothèse dominante de ceux qui communiquent de la sorte – en particulier, mais pas que, dans les sociétés libérales démocratiques – est celle d'un contrôle souverain, une souveraineté du soi comprise comme une liberté de s'exprimer, de communiquer et de se mobiliser sur des terrains déterritorialisés qui peuvent potentiellement défier des structures de pouvoir et de domination. La défiance de la distance se trouve ici quelque part équivalante à la défiance d'une autorité associée à un territoire, de sorte que même lorsque cette autorité cherche à assoir sa présence, l'imaginaire est celui de la possibilité, et même de la trans-

23. Negroponte N., *Being Digital*, New York, Vintage, 1995.
24. Luke T. W., "Simulated Sovereignty, Telematic Territoriality: The Political Economy of Cyberspace", in Lash S. et Featherstone M. (eds.), *Spaces of Culture: City-Nation-World*, Londres, Sage, 1999.

gression. C'est ce récit qui a nourri les interprétations du « Printemps arabe », mais aussi des émeutes de Londres en 2011, du mouvement altermondialiste, et d'autres expressions de protestation et de résistance dans le monde [25]. Il y a eu là, et il y a peut-être encore, la preuve de l'existence d'une sphère publique globale [26] au sein de laquelle les pratiques de communication ont l'autorité nécessaire pour tenir ensemble l'hétérogène quand elles mobilisent au sein et par-delà les frontières et constituent dès lors un espace entièrement autre : un monde interconnecté, où le cosmopolite est à la fois fait de différences et d'homogénéité.

C'est toutefois précisément ce brouillage des frontières, ce terrain illimité des possibles, où la différence peut habiter le familier ou l'homogène, qui invoque, qui défie un dispositif qui, nous dit Foucault, ne fonctionne pas suivant le modèle de la répression mais suivant celui de la production, de la permission et de l'autorisation [27]. Tel est le triomphe du libéralisme, car ici toute pratique répressive est aussi une pratique régressive. C'est une manière d'abandonner, avec toute la sophistication possible, les distinctions qui font qu'il n'y a plus ici un Zimbabwe de Mugabe ou une Chine communiste. Le modèle libéral est celui de la sécurité par la liberté et non pas de la sécurité au prix de la liberté. Le cyberespace en est venu à représenter la manifestation technologique d'une liberté transformative où les pratiques communicatives pourraient avoir lieu ; qu'elles soient de type politique, socioculturel, pédagogique et économique. La question, pour l'autorité politique – et il s'agit ici d'interroger l'autorité politique libérale – est de savoir comment réguler ce terrain de communication débridée, quelles sont les technologies de contrôle mobilisables sans qu'elles soient elles-mêmes sujettes aux limites des États et de l'autorité souveraine définie par l'État. Si de telles technologies pouvaient être créées, elles devraient également être numériques, prendre la forme de réseaux ou de logiciels et non de matériel, elles devraient être invisibles, transnationales et de portée mondiale.

L'informatique est devenue la discipline de choix des puissances libérales mais, en dépit de l'attention portée au logiciel, à la codification comme expertise rendue sous sa forme numérique, le « dur » compte beaucoup dans, justement, la matérialité des technologies conçues pour contrôler cet espace de l'illimité. Des disques durs aux câbles sous-marins, il s'agit là d'éléments technologiques et d'ingénierie d'une machine au service de la liberté de communiquer et de la capacité de surveiller et contrôler. Au sein de ces cadres de savoir disciplinaire, comme pour tous les systèmes de savoir et les formations discur-

25. Voir par exemple Gerbaudo P., *Tweets and Streets: Social Media and Contemporary Activism*, Londres, Pluto Press, 2012.
26. Castells M., "The New Public Sphere: Global Civil Society. Communication Networks, and Global Governance", *The Annals of the American Academy of Political and Social Science*, 616/1, 2008, pp. 78-93.
27. Foucault M., *Sécurité, territoire, population. Cours au Collège de France (1977-1978)*, Paris, Gallimard/Seuil, 2004.

sives qui assurent leur reproduction, le sujet épistémique gouverne un espace délicat entre politique et gouvernement, résistance (et on pense ici aux groupes comme Anonymous ou Hacked-Off [28]) et emploi pour entretenir le marché numérique ou l'État. La difficulté c'est qu'il n'y a ni dualisme ni opposition entre ces pôles, car chacun mobilise l'autre de sorte que, par exemple, le monde du *hacker* résistant est mobilisé par et peut-être même amélioré par les ressources disponibles aux fournisseurs d'accès ou à l'État. Il est rare que le mouvement parte de l'État vers le résistant individuel. Le pouvoir en vient à imprégner le savoir et le sujet produit dans cette matrice complexe est toujours déjà complice, impliqué, d'une certaine manière, dans sa reproduction. Le traçage de ces connections, la cartographie des réseaux, des nœuds mais aussi de ces imbrications complexes du pouvoir, du savoir et des subjectivités sont les tâches de toute intervention critique sur le cyberespace, sa constitution quotidienne dans des pratiques et des cadres de la connaissance, et son pouvoir constitutif dans la subjectivation.

D'aucuns peuvent estimer que les communications virtuelles entrainent la « fin de la vie privée [29] ». Tel est le contexte dans lequel les révélations d'Edward Snowden interviennent, car indépendamment de la connaissance que nous, habitants du cyberespace, pouvons avoir de la possibilité et même, en réalité, du profil – rêve du publicitaire du marché numérique mondial –, le jeu prend une direction tout autre lorsque le profileur est l'État et, de manière peut-être encore plus significative, lorsque le profilé peut être n'importe où dans le monde. Cet espace au sein duquel toute défiance des obstacles techniques à la communication se traduisait souvent par une défiance au pouvoir a été, grâce à Edward Snowden, subitement dénudé : un espace sujet à la pénétration la plus interventionniste qui soit du sujet communiquant par une puissance souveraine qui considère le monde comme son théâtre d'opération. Dans cette articulation déterritorialisée du pouvoir, les limites semblent futiles et les distinctions entre ami et ennemi, national et international, public et privé se disloquent. Dans cette rafle de la surveillance, chaque communication est enregistrée numériquement et stockée et le triomphe, qui s'exprime souvent par le biais de l'avatar du « *smiley* » dans les documents de la NSA rendus disponibles par les révélations (voir les dossiers NSA du *Guardian* pour les documents publiés récemment sous le label « Dishfire ») est défini comme la capacité à capturer des centaines de millions de communications SMS par jour.

Sur le plan politique, le langage en vient à être le terrain sur lequel et par lequel les modes de légitimation et de délégitimation opèrent. La terminologie employée par les défenseurs de la NSA et de la GCHQ est « l'accès en bloc » par opposition à la « surveillance de masse » [30]. Cette dernière dénomination

28. Coleman G., "Hacker Politics and Publics", *Public Culture*, 23/3, 2011, pp. 511-516.
29. Comme annoncé dans Whitaker R., *The End of Privacy: How Total Surveillance is Becoming a Reality*, New York, New Press, 1998.
30. L'expression « *bulk access* » (accès en bloc) a été utilisée par Sir David Omand, ancien chef de

nous évoque la Stasi de l'ancienne Allemagne de l'Est, un parallèle immédiatement réfuté. L'expression « accès en bloc » suggère des opérations qui visent à retrouver « une aiguille dans une botte de foin », cet individu ou cette cellule terroriste déterminé à commettre une atrocité quelque part et sans préavis. C'est en effet ce qu'a sous-entendu le ministre des Affaires étrangères britannique, William Hague, en déclarant « si vous n'avez rien à cacher, vous n'avez pas à vous inquiéter ». L'opération de surveillance est ici pensée comme un tamisage, une opération par laquelle les « masses » passent au travers sans être observées ou bloquées tandis que l'unique communication anormale est interceptée et par là, l'auteur potentiel d'un acte de violence terroriste. Et lorsque les communications des dirigeants mondiaux et des groupes pétroliers sont prises dans les mailles du filet, il s'agit de cas malencontreux et collatéraux.

Toutefois, si nous insistons sur le terme « surveillance de masse », l'attention est sur la « surveillance » de la « masse » et la masse peut ne pas vouloir signifier le terrain biopolitique de la population, mais bien plus radicalement la « multitude » de communications singulières et rhizomiques sujettes à la surveillance, même si les « données » en tant que telles peuvent apparaître numériquement dans un profil en réseau révélé par des « métadonnées » ou même du « contenu ». Le sujet de la surveillance est donc non pas simplement la population, bien que le « profil » soit dit pouvoir porter en lui des populations spécifiques, mais le sujet individuel de la communication. C'est en ce sens, et nous le savons maintenant, que l'espace de l'intime est totalement pénétré par ces agences, de sorte qu'un profil est construit à partir de la trace numérique faite par le sujet communiquant et interactif.

La trace est laissée dans toute son intimité et avec la pleine conscience qu'elle n'est plus privée, que les agences impliquées dans les activités de surveillance y ont accès. Si nous la comprenons normativement, la formule « liberté par la sécurité » ne prévoit aucune limite à cet accès. Toutefois, la conception positive des droits en prévoit une, lorsque la vie privée ne se voit pas conférer qu'une valeur culturelle, mais aussi légale, comme nous l'avons vu plus tôt dans cet article.

Vivre avec la surveillance : résignation, perplexité et résistance

Quelles qu'aient été les réponses particulières aux révélations de Snowden sur la surveillance de masse et la NSA, il est clair que l'opinion publique a été ébranlée et que les discussions sont nombreuses dans le monde sur ce que nous découvrons progressivement à propos des agences de sécurité et des services de renseignement nationaux. Il est tout aussi évident que les membres de

---

la GCHQ, suggérant ainsi qu'elle était plus appropriée pour décrire les activités de la NSA et de la GCHQ. Voir "Mass Electronic Surveillance and Liberal Democracy", Research Centre in International Relations, Department of War Studies, King's College Londres, 21 janvier 2014.

l'*establishment* se sont rapidement mobilisés pour promouvoir la nécessité de cette surveillance dans l'intérêt de la « sécurité nationale » ou de « l'ordre public ». En janvier 2014, la réponse officielle du président Obama aux révélations Snowden a été de renforcer l'idée que la surveillance de masse gouvernementale était nécessaire et qu'il valait mieux contrôler la surveillance opérée par le secteur économique privé [31].

Qu'en est-il, toutefois, des citoyens et des consommateurs ordinaires qui, dans leurs vies quotidiennes, ont le sentiment grandissant que leurs activités et leurs communications sont traquées et surveillées bien plus que ce qu'ils n'imaginaient ? Il n'y a bien entendu rien d'aussi évident, rien qui nous saute au visage comme un *Big Brother* sur un écran de télévision, mais plutôt un malaise kafkaïen quant au fait que les métadonnées ostensiblement innocentes (la localisation, la durée ou le destinataire d'un appel par exemple) ont en réalité des conséquences. Mais tout paraît fluide, glissant et difficile à saisir. Cela semble en effet correspondre à la qualité même des relations qui caractérisent une culture de la consommation, se divisant, mutant, se déversant sur des canaux et des conduits en changement perpétuel. C'est ce que nous avons pu appeler la « surveillance liquide [32] ».

La compréhension de l'opinion publique est notoirement difficile, mais si l'on aborde la question par plusieurs points d'entrée, on doit pouvoir la lire, sentir ce qui se passe à mesure que les gens réagissent aux révélations. Il existe des mesures directes telles que les sondages ou des entretiens plus approfondis, voire des ethnographies, et des approches indirectes consistant à placer la question dans un contexte culturel et historique et tenter d'y discerner les signes d'une époque. Elles ont toutes une place et il faut au moins commencer par admettre à quel point cet effort de compréhension est difficile car peu de temps a passé depuis les premières révélations de Snowden en juin 2013 et les expériences varient énormément selon les régions et les pays touchés par la surveillance américaine.

Un sondage mondial de l'institut Angus Reid publié en fin d'année 2013 [33] a montré que ce que l'on pense de Snowden dépend en partie du lieu où l'on se trouve. Les Américains sont 51 % à penser qu'il est un héros car il a « permis au public de savoir que nos gouvernement opèrent des programmes de surveillance électronique menaçant la vie privée des individus », contre 49 % qui le considèrent comme un traitre qui « menace les opérations de renseignement occidentales ». Reste que 60 % déclarent considérer que la surveillance gouvernementale de masse est inacceptable. Dans d'autres pays, Snowden est

31. Podesta J., "Big Data and the Future of Privacy", 2014 (www.whitehouse.gov/blog/2014/01/23/big-data-and-future-privacy/).
32. Bauman Z., Lyon D., *Liquid Surveillance: A Conversation*, Cambridge UK, Polity, 2013.
33. Edwards-Levy A., Freeman S., "Americans Still Can't Decide Whether Edward Snowden Is A 'Traitor' Or A 'Hero,' Poll Finds", *The Huffington Post*, 30 octobre 2013 (www.huffingtonpost.com/2013/10/30/edward-snowden-poll_n_4175089.html/).

plus soutenu : 67 % des Canadiens et 60 % des Britanniques considèrent que ses alertes sont positives. Seuls 5 % des sondés au Canada pensent que le gouvernement peut garder leurs données et ce taux ne s'élève qu'à 7 % aux États-Unis. Que ce soit aux États-Unis, au Canada ou au Royaume-Uni, il est clair d'après ces résultats qu'une grande part de la population s'inquiète de cette surveillance d'État et exprime un certain cynisme à propos de ce que les gouvernements font des données récoltées.

Les révélations de Snowden sont encore trop récentes pour qu'il soit possible d'analyser en profondeur ce que les populations pensent de la surveillance de masse opérée par les gouvernements, sans parler de possibles ethnographies des adaptations de comportement des individus par rapport à leurs données sur Internet. Nous devons donc nous rabattre sur des enquêtes plus larges et de plus long terme sur les attitudes. Le travail d'Edward Snowden nous a montré à quel point la NSA et consorts dépendent des fournisseurs d'accès Internet et des plateformes de réseaux sociaux comme Facebook pour accéder à des données transactionnelles et interactionnelles. Cependant, pour la plupart des utilisateurs de médias sociaux, la surveillance comme pouvoir hiérarchique semble avoir peu de pertinence à moins qu'ils ne vivent dans des zones de conflits ou dans des pays où la répression politique est manifeste. Il est bien plus probable qu'ils prennent part à la surveillance sociale [34] là où, dans la « capillarité du pouvoir » de Foucault, les différentiels de pouvoir des interactions quotidiennes sont bien plus immédiatement significatifs que ce que peut faire la NSA ou ses consœurs. Cela ne veut pas dire que la prise de conscience ne peut avoir lieu, en particulier lorsqu'on évoque des évènements mondiaux comme l'action de résistance en ligne « *The-Day-We-fight-back* » organisée le 11 février 2014.

Le contexte plus large des révélations d'Edward Snowden n'est pas seulement le déclin de la participation politique au sein des États libéraux démocratiques mais aussi, pour suivre Agamben [35], la fin du politique. Agamben insiste sur le fait que sous le signe de la sécurité, les États contemporains sont passés de la politique à la police, du gouvernement au *management* – usant de systèmes de surveillance électroniques – et ébranlent ainsi la possibilité même du politique. Il est de mauvaise augure pour un éventuel retour du politique que cette tendance émerge en même temps que la croissance de toutes sortes de surveillances au-delà de celles qui sont associées aux communications et aux transactions, et ce, en particulier lorsque ces cultures de la surveillance paraissent inoffensives au quotidien.

---

34. Marwick A. E., "The Public Domain: Surveillance in Everyday Life", *Surveillance and Society*, 94/4, 2012, pp. 378-393 (http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/viewFile/pub_dom/pub_dom/).
35. Agamben G.. "From the state of control to the *praxis* of destituent power", Présentation publique, Athènes, 16 novembre, 2013 (http://roarmag.org/2014/02/agamben-destituent-power-democracy/).

Trois types de facteurs – qui peuvent toutefois se chevaucher pour se renforcer ou s'affaiblir mutuellement selon le contexte – nous aident à essayer de comprendre pourquoi ces surveillances multiples sont encore acceptables pour une part importante de la population.

Le premier est la familiarité. La surveillance est si répandue et comporte tant de dimensions qu'elle fait dorénavant partie du quotidien. Elle nous entoure dans de nombreux contextes, au-delà des signes les plus évidents (même si leur miniaturisation les rend moins ostensibles aujourd'hui) comme les caméras de vidéosurveillance dans la rue, les centres commerciaux ou les écoles, ou encore les procédures de sécurité dans les aéroports mais aussi dans les bâtiments, les véhicules, les appareils dont nous nous servons au quotidien. La surveillance est intégrée dans les voitures (GPS, Internet, enregistreurs de données ou caméras haute-définition) et les bâtiments (systèmes d'accès par badges, senseurs). Beaucoup les prennent pour acquis ; ils sont domestiqués, normaux, ils passent inaperçus. Beaucoup de personnes ne les remarquent plus et ne pensent pas à leurs capacités de surveillance [36].

Le deuxième facteur est la peur, qui serait devenue plus forte depuis le 11 Septembre [37]. Les gouvernements, les sociétés de sécurité et les médias jouent un jeu cynique avec ce facteur peur dont les effets peuvent être paralysants ou directs. La peur sert aux entreprises qui tentent de vendre de nouveaux équipements, pour les gouvernements qui estiment que leur tâche est de libérer les forces du marché et d'assurer la sécurité et pour les médias qui ont besoin de cette polarisation des « bons contre les méchants », en particulier si le « méchant » peut être pensé en termes « musulmans » [38]. L'effet paralysant peut se produire par exemple lorsque des hommes et des femmes politiques ou des journalistes ne font pas clairement la distinction entre ceux qui sont réellement des terroristes et d'autres qui peuvent être des opposants licites (contre la pollution, les atteintes aux droits de l'homme ou l'exploitation des aborigènes) ou encore des migrants sans papiers. Les niveaux de peur surpassent largement les statistiques effectives des actes terroristes et encouragent probablement cette acceptation de l'intensification de la surveillance.

L'amusement, les loisirs représentent le troisième facteur critique qui encourage l'intensification de la surveillance. Si cela peut apparaître trivial dans le contexte des peurs post 11 Septembre, il est important de noter que les médias sociaux se sont également beaucoup développés et mutuellement encouragés au cours de la dernière décennie. La clé pour comprendre ce nou-

36. New Transparency, *Transparent Lives: Surveillance in Canada/Vivre à nu: La surveillance au Canada*, Edmonton, Athabasca University Press, 2014.
37. Voir Bauman Z., *Liquid Fear*, Cambridge, Polity, 2005 et Lyon D., *Surveillance After September 11*, Cambridge, Polity, 2003.
38. Kurzman C., "Where Are All the Islamic Terrorists?", *Chronicle of Higher Education*, 31 juillet 2011 (https://chronicle.com/article/Where-Are-All-the-Islamic/128443/).

veau type de média est son postulat de départ : du « contenu généré par les utilisateurs ». Dans ce Web 2.0, l'information n'est plus uniquement fournie par de grandes organisations, mais par tous. Wikipédia est sans doute le premier média de ce type à avoir eu du succès. Les médias sociaux ne fonctionnent pas uniquement par les contenus apportés mais aussi, et cela est central, par les relations entre les différents utilisateurs. Les « amis » Facebook sont les plus évidents et les plus répandus. De plus, les individus participent à Facebook et aux autres réseaux sociaux en se servant de leur vraie identité et se connectent avec d'autres personnes aux apparences proches. Cette « surveillance sociale [39] » (que l'on appelle aussi surveillance « par les pairs » ou « latérale ») est appréciée par les participants. Le regroupement avec des personnes qui aiment le même type de musique, de films ou de sport est réalisé par les utilisateurs eux-mêmes avant que le travail de répartition en algorithmes ne commence (par les agences de *marketing* électronique). Les médias sociaux sont encore très populaires et s'ils sont en effet un puissant moyen d'organiser les opinions publiques et les protestations, ils fournissent aussi les données brutes dont se serviront les entreprises privées ainsi que les agences de renseignement de police, comme l'a montré Edward Snowden.

Cela semble si fluide, si glissant et si difficile à attraper pour les citoyens et les consommateurs ordinaires. On sent, on sait qu'on est observé, mais on ne sait pas (et on ne s'en préoccupe guère) par qui ni pourquoi. Les caméras vidéo sont aujourd'hui peut-être ce que nous voyons de plus banal dans les rues peuplées ou vides de nos villes ; si communes que nous ne les remarquons plus – elles se « cachent en pleine lumière », ou plutôt dans leur familiarité. De fait, elles ne se cachent pas, elles publicisent leur présence, ouvertement et avec fierté. Et il y a quelque chose qui les distingue des caméras vidéos cachées dans la chambre d'étudiant de Winston Smith [40] : elles ne nous surveillent pas pour nous maintenir dans les rangs et nous forcer à respecter des horaires routiniers, elles ne nous donnent pas d'ordre, elles ne nous enlèvent pas notre liberté de choisir, elles n'établissent pas nos préférences. Elles sont là où elles sont, c'est-à-dire partout, pour garantir notre sécurité et les libertés que nous chérissons…

En dépit de la pleine conscience que nous avons de l'ubiquité de cet espionnage (requalifié de « collecte de données » par souci du politiquement correct) et de l'énormité des « bases de données » générées (loin devant tout ce que la CIA, le KGB, la STASI du passé avaient réussi à amasser avec leurs légions incalculables d'informateurs payés), on ne peut qu'être surpris de la sérénité avec laquelle les révélations de Snowden ont été reçues par « les citoyens et les consommateurs ». S'ils avaient espéré voir leurs audiences ou

39. Marwick A. E., *Status Update: Celebrity, Publicity and Branding in the Social Media Age*, New Haven, Yale University Press, 2013.
40. Note de la traductrice : personnage de *1984* de George Orwell.

leurs ventes de journaux grimper, les professionnels des médias s'étaient cruellement trompés. Qu'importe leurs efforts, les révélations d'Edward Snowden n'ont entraîné que quelques frémissements légers, presque imperceptibles, là où des ondes de choc étaient attendues.

On peut imaginer que ce qui a fortement contribué à cette (non-)réaction, c'est la satisfaction consciente et subconsciente ressentie par les milliards d'utilisateurs d'Internet s'abandonnant dans cette auto-surveillance 24h/24. L'une des principales attractions de l'Internet est la liberté d'accès permanent et à la demande à la (version en ligne de la) « sphère publique » qui n'était dans le passé ouverte qu'à quelques privilégiés et dont l'entrée était sévèrement gardée par les grands groupes de radio, de télévision ou de presse. Pour des millions d'individus effrayés par le spectre de la solitude et de l'abandon, Internet offre une chance sans précédant de sortir de l'anonymat, de la négligence et de l'oubli. Un des effets collatéraux des révélations de Snowden a été de montrer à quel point cette « sphère publique » était grande et remplie de gens importants, de « gens qui comptent vraiment ». Leur espoir semi-conscient est devenu bien plus réaliste et a offert la preuve retentissante – s'il y en avait le besoin – de la justesse et la valeur de leur investissement en termes de temps et d'énergie dans ces amis et cette arène publique virtuels. L'effet le plus profond et le plus durable, s'il y en a un, de toute cette affaire sera un autre bond en avant dans le dévouement et l'enthousiasme de l'espionnage « fait maison » (*do it yourself*) – bénévole et gratuit – pour la plus grande joie des marchés de consommation et de sécurité.

Si nous partons du principe que les facteurs que nous venons d'énoncer sont corrects, le danger pour toute recherche de transparence et de responsabilité des grandes agences et de la participation démocratique aux nouveaux protocoles d'information est que du point de vue des utilisateurs quotidiens d'Internet et des médias sociaux, ce ne sera qu'une routine de plus. Les révélations au compte goutte permettent de contrer cela efficacement. Il semble que chaque révélation soit calculée pour pouvoir toucher des dimensions différentes de cette surveillance orchestrée par les gouvernements et permises grâce à la coopération des entreprises de l'Internet. Cette méthode de dénonciation très rusée a permis d'entretenir l'attention du public bien au-delà de l'intérêt médiatique habituellement très bref. Reste à savoir ce qui pourrait produire un engagement public plus sérieux.