«La République sur écoute»: enquête sur une surveillance de masse

PAR JÉRÔME HOURDEAUX
ARTICLE PUBLIÉ LE JEUDI 8 OCTOBRE 2015

Manifestation du 4 mai 2015 contre la loi renseignement. © *Reuters*

Fadettes, métadonnées, algorithme, boîte noire, imsi-catchers, signal faible… Ces termes racontent bien plus qu'une révolution technologique : un projet politique de mise sous surveillance des citoyens ou de monitoring de toute une population. Pour l'expliquer, Mediapart publie *La République sur écoute, chroniques d'une France sous surveillance*, un livre d'enquêtes et d'analyses.

Ce combat pour nos libertés n'est pas terminé. L'adoption, en juin dernier, de la loi sur le renseignement a certes été une défaite pour les nombreuses associations et autorités administratives indépendantes qui en avaient dénoncé les multiples dangers (**voir ici notre émission spéciale «Six heures contre la surveillance»**). La mise en place d'une surveillance de masse, au nom d'une lutte globale contre le terrorisme, n'aura provoqué que tardivement un sursaut citoyen. L'extraordinaire rapidité de la révolution numérique en cours, la complexité des dispositifs et des termes techniques ont permis aux services de renseignement d'avancer en partie masqués et d'imposer à des parlementaires peu experts en la matière une série de mesures liberticides.

En prolongement de cette loi, un nouveau texte est actuellement examiné au Parlement dans une indifférence quasi-générale. Il vise à étendre encore les dispositifs de surveillance à l'international: il s'agit de mettre en place un système d'espionnage de masse des câbles transatlantiques acheminant le trafic internet (**lire notre article ici**).

Mais ces atteintes à nos libertés individuelles ne sont pas irréversibles. En témoigne la décision rendue cette semaine par la Cour de justice de l'Union européenne d'annuler le *Safe Harbor*, l'accord sur le transfert de données collectées par des entreprises américaines sur des internautes européens, en raison du peu de protection face aux services de renseignement (**lire notre article ici**). A l'origine de cette décision, une procédure lancée par un simple citoyen européen devant la justice irlandaise.

C'est pour expliquer les enjeux fondamentaux de ces combats que Mediapart publie ce 8 octobre, aux éditions Don Quichotte, *La République sur écoute, chroniques d'une France sous surveillance*. C'est un livre d'enquêtes et d'analyses qui vient prolonger et compléter le travail de notre rédaction effectué ces derniers mois sur la surveillance de masse. Il rappelle également nos révélations, avec Julian Assange et WikiLeaks, de la mise sur écoute d'une partie du personnel politique français (les présidents de la République en premier) par la NSA américaine.

Coordonné par Fabrice Arfi, ce livre dresse un état des lieux minutieux et pédagogique de ce vaste système d'écoute et de surveillance. Fadettes, métadonnées,

algorithme, boîte noire, imsi-catchers, signal faible… Ces nouvelles expressions racontent davantage qu'une révolution technologique : un projet politique assumé par le gouvernement, la mise sous surveillance, ou un monitoring généralisé, de la population française. Ci-dessous, nous reproduisons l'un des chapitres du livre.

Surveillance de masse:
dans quelle sorte de monde nous vivons

Le vote, au mois de juin 2015, par le Parlement français de la loi relative au renseignement, quasiment deux ans après la publication des premières révélations d'Edward Snowden, avait quelque chose de symbolique. Alors que l'ex-employé de la NSA avait mis au jour un dispositif mondial de surveillance, la France, elle, comme si de rien n'était, adoptait peu ou prou les mêmes mesures qui avaient conduit les États-Unis à ces dérapages. Comme si ces deux dernières années, l'avalanche d'articles, souvent accompagnés de documents secrets émanant du cœur même de l'appareil de surveillance américain, n'avait pas permis d'éveiller les consciences. Comme si le débat n'avait pas pris.

Certes, les informations fournies par Edward Snowden ont eu un impact indéniable. Les journalistes ayant eu accès à ces documents, notamment les premiers d'entre eux, Glenn Greenwald et Laura Poitras, ont mené un impressionnant travail d'enquête et de pédagogie toujours en cours. Celui-ci a ouvert de véritables débats dans des pays comme le Brésil ou l'Allemagne, mobilisé le milieu de l'hacktivisme et popularisé certains outils de sécurisation de la vie privée, tels le navigateur **Tor Browser** ou le **logiciel de chiffrement PGP**, dont la diffusion a grimpé en flèche. Edward Snowden, lui, qui vit toujours réfugié en Russie, n'est sans doute pas pour rien dans la décision, annoncée au mois de juillet par Barack Obama, de ne pas renouveler une partie substantielle du Patriot Act, limitant ainsi sérieusement les pouvoirs de la NSA.

Néanmoins, malgré ces avancées incontestables, on ne peut que constater la léthargie d'une bonne partie de la société. Comme l'expliquait **au mois de mars 2015** à Mediapart Sarah Harrison, journaliste à WikiLeaks et compagnon de fuite d'Edward Snowden, ce dernier avait à la fois un *« but »* et des *« espoirs »*. *« Son but était que les illégalités commises par la NSA soient connues par le peuple américain »*, expliquait-elle. Ses espoirs : *« que la réaction du public à ces informations serait de changer les choses »*. *« Son but a été incontestablement atteint. Est-ce que ses espoirs se sont réalisés ? Pas encore. »*

Glenn Greenwald, Edward Snowden et Laura Poitras © Reuters

En France, les révélations d'Edward Snowden n'ont suscité chez nos dirigeants que des indignations de principe – et encore. Aucune mesure de rétorsion, aucune enquête parlementaire… Pas de vaste mouvement d'opinion publique non plus. Au contraire, quelques mois après la publication des premiers articles sur la NSA, le Parlement français adoptait la loi de programmation militaire (LPM), puis, un an plus tard, la loi antiterroriste et, enfin, il y a quelques mois, la loi renseignement. Et ce, malgré l'opposition d'une grande partie de la société civile, d'associations, de syndicats et d'autorités administratives indépendantes.

L'une des raisons de ce décalage entre l'indignation réelle suscitée par les révélations d'Edward Snowden et l'absence de réaction des opinions publiques s'explique en partie par un manque de recul. En deux ans, c'est une avalanche d'informations, de nouveaux termes, de nouveaux concepts qui a déferlé dans la conversation publique. Chacun des nombreux programmes de surveillance révélés aurait mérité à lui seul plusieurs mois d'enquête. Et peut-être que le rythme effréné des publications et des réformes sécuritaires lancées par cette majorité n'a pas permis de prendre le temps nécessaire pour expliquer le contexte global.

Peut-être n'avons-nous pas non plus réussi à expliquer les enjeux d'une révolution déjà en cours. Lorsque, **le 5 juin 2013**, le quotidien britannique *The Guardian* publie le premier article tiré des documents fournis par Edward Snowden, le dispositif de surveillance qu'il dévoile est en effet en place depuis plusieurs années. Profitant du manque d'intérêt du grand public pour les questions de surveillance – et du manque d'intérêt des politiques pour les questions numériques – le monde du renseignement a silencieusement opéré ces deux dernières décennies une mue dont il est aujourd'hui difficile d'apprécier l'ampleur et les conséquences sur nos libertés.

Parallèlement, le débat s'est porté sur les figures classiques de la surveillance et sur de vieilles problématiques rendues obsolètes par les changements de paradigmes. Pour beaucoup, le système de surveillance global mis en place par la NSA, et que la France a commencé à reproduire, se résume à Big Brother de *1984*, le célèbre roman d'anticipation de George Orwell. Un surveillant, émanation d'un État tout-puissant et centralisé, omniprésent et exerçant une surveillance directe, permanente des citoyens via un système de contrôles, de caméras, de *« télécrans »* installés dans les foyers. Les espions et leurs gadgets, micros, balises de géolocalisation et « IMSI-catchers » demeurent toujours dans les esprits comme les symboles de la surveillance.

Ces formes classiques de surveillance conservent leur importance. Cependant, elles dissimulent le nouveau terrain d'activité des services de renseignement : le monde des données, et plus précisément du big data, des données de masse. Ce que dévoilent les documents d'Edward Snowden, ce n'est pas tant un dispositif intrusif, pénétrant nos maisons et nos ordinateurs, mais un mode de surveillance plus discret, reposant sur une collecte massive et indiscriminée de toutes sortes de données. Celles-ci sont ensuite stockées le plus longtemps possible afin d'être croisées, recoupées, analysées et traitées par des algorithmes.

La chasse aux « signaux faibles »

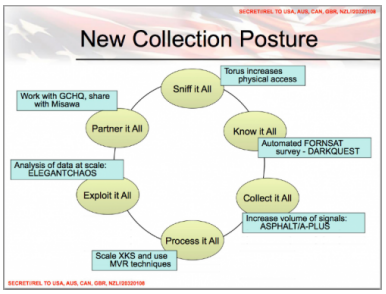
Le but du big data est d'identifier des patterns, c'est-à- dire des modèles se répétant à l'identique et permettant de systématiser un comportement. Ces modèles sont ensuite utilisés pour repérer, par déduction, des comportements similaires. Pour schématiser, si les données collectées sur un terroriste montrent qu'il a visité tel site, effectué tel achat ou tel voyage, on pourra présumer que toutes les personnes visitant le même site, effectuant les mêmes achats et le même voyage seront de potentiels suspects. L'idée est de détecter des « signaux faibles », des petites informations qui, sans l'aide du big data, seraient passées inaperçues. Les Américains emploient également l'expression connecting the dots (« connecter les points ») en référence à ce jeu pour enfants où l'on relie des points numérotés afin de faire apparaître un dessin.

L'un des problèmes avec les signaux faibles est le critère de « faiblesse » des données nécessaires à l'analyse. Jusqu'à quel niveau de sensibilité, et donc d'intrusion dans la vie privée, les algorithmes auront- ils besoin de descendre ? Le fait d'acheter des falafels, par exemple, peut-il transformer une personne en possible terroriste ? L'idée peut sembler ridicule. **Elle a pourtant germé** dans le cerveau de quelques responsables du FBI qui, en 2005 et 2006, avaient mis en place dans la région de San Francisco un programme de collecte des données des magasins d'alimentation moyen-orientaux. En épluchant les listes de ventes, les agents espéraient pouvoir repérer des « pics » pour certains produits et, en combinant ces données avec d'autres, remonter jusqu'à des agents secrets iraniens vivant dans la région. Alertée, la direction du FBI avait d'elle-même interrompu ce programme. Mais il reste révélateur des besoins intrinsèques de la surveillance algorithmique.

C'est l'une des caractéristiques du big data : les données appellent les données. Afin de faire émerger des modèles suffisamment précis, les algorithmes ont besoin d'une base de données considérable qui doit être régulièrement alimentée pour les affiner. Cette dépendance explique la boulimie des agences

américaines dévoilée dans de nombreux documents d'Edward Snowden. Au mois de mars 2013, l'officier en chef responsable de la technologie à la CIA, Gus Hunt, **expliquait sans détour lors d'une conférence** sur le big data qui se tenait à New York : *« La valeur de tout morceau d'information n'est connue que lorsque vous pouvez le connecter avec quelque chose d'autre qui se produira à un moment donné dans le futur. »« Comme vous ne pouvez pas connecter les points que vous n'avez pas […], en vérité nous essayons de tout collecter et de le retenir pour toujours. »*

« Tout collecter. » Collect it all. Un slogan et fil rouge des révélations d'Edward Snowden. Selon un portrait publié **en juillet 2013 par le *Washington Post***, cette phrase était un leitmotiv pour le général Keith B. Alexander, directeur de la NSA de 2005 à 2014 et l'un des artisans du système mondial d'espionnage mis en place par l'agence. Le journaliste Glenn Greenwald lui consacre un chapitre entier dans son livre *Nulle part où se cacher*, qui décrit les dessous de sa collaboration avec l'ex-employé de la NSA. On retrouve cette phrase dans plusieurs documents, et notamment dans **un PowerPoint projeté en 2011** lors d'une réunion de représentants des Five Eyes, l'alliance réunissant les services de renseignement des États-Unis, du Royaume-Uni, du Canada, de la Nouvelle-Zélande et de l'Australie. Le schéma en question illustrait *« la nouvelle posture de collecte »* que les agences devaient adopter. Résumée à six slogans, elle renvoyait chacun à des programmes bien réels : *« Tout aspirer »*, *« Tout savoir »*, *« Tout collecter »*, *« Tout traiter »*, *« Tout exploiter »*, *« Tout associer »* (c'est-à-dire partager avec les autres Five Eyes).



Le document de la NSA projeté en 2011

La captation de données est devenue une obsession pour les services de renseignement qui explique de nombreux aspects des réformes adoptées ces dernières années, aux États-Unis ou en France. Jusqu'au début des années deux mille, la surveillance se limitait en effet à l'interception de communications, de textes et de paroles par la pose de micros ou le placement sur écoute de lignes téléphoniques. Ces contenus, parfois difficiles à collecter et à analyser, sont en outre souvent protégés par des législations sur la vie privée relativement contraignantes. De plus, ils ne sont que de peu d'utilité dans le cadre du big data. Celui-ci a besoin de données « brutes » facilement manipulables, intégrables à des catégories statistiques et sur lesquelles les algorithmes peuvent travailler.

Pour le big data, ce n'est pas le contenu mais le contexte – les « métadonnées » – qui importe. Ces données correspondent à toutes les informations émises par un fichier ou une action sur un réseau. Dans le cadre d'une communication téléphonique ou d'un mail, elles correspondent aux noms de l'expéditeur et du destinataire, à la durée de communication ou à la taille du texte, son objet s'il est indiqué… Dans le cadre d'une connexion Internet, elles se rapportent à l'historique de navigation, à la durée de visite de chaque page. Pour des achats par carte bancaire, c'est le montant de la transaction, l'identité du vendeur, la date…

Le but des différentes réformes législatives a donc été, en grande partie, d'accorder à ces métadonnées un statut à part et surtout moins protecteur que pour les contenus. Aux États-Unis, cela s'est traduit par

la section 215 du Patriot Act autorisant la collecte de masse de métadonnées. **Le premier article** écrit à partir des documents d'Edward Snowden, publié le 5 juin 2013 dans *The Guardian*, révélait justement comment les autorités américaines avaient contraint l'opérateur téléphonique Verizon à lui fournir *« sur une base quotidienne »* les métadonnées téléphoniques de millions d'utilisateurs. Le lendemain, le quotidien britannique dévoilait l'existence du programme Prism autorisant la NSA à accéder directement aux données stockées par la plupart des grands noms du net : Google, Facebook, Skype, Microsoft, Apple…

Pour exploiter cette masse considérable de données, les agences utilisent toute une série d'outils et de logiciels qui permettent par exemple de retracer, sous forme de graphiques, les cercles relationnels d'une personne. Également démontré par Edward Snowden, le système XKeyscore peut effectuer des recherches dans l'immense base de données chaque jour constituée. Et, pour stocker toutes ces informations, les autorités américaines ont inauguré au mois de mai 2014, dans l'État de l'Utah, **un méga data center** de plus de cent mille mètres carrés ultra-sécurisé et ayant coûté plus de 1,5 milliard de dollars.

À la fin du mois de mai 2015, un rapport de l'inspecteur général du département de la Justice américain, Michael E. Horowitz, annonçait que la collecte de masse de données par le FBI sous le régime de **la section 215 du Patriot Act** avait été multipliée par trois entre 2004 et 2009. Toutefois, **ce rapport était surtout extrêmement critique** sur l'efficacité de cette surveillance. Selon les agents interrogés, les données collectées n'avaient permis d'arrêter aucun terroriste ni de déjouer aucune attaque. Au contraire, le rapport soulignait que cette extension de la collecte avait conduit à placer sous surveillance un nombre croissant d'Américains sans lien avec le terrorisme.

« Métadonnées égalent surveillance »

Sans doute grâce aux révélations d'Edward Snowden, les États-Unis semblent prendre conscience des dérapages de leurs agences de renseignement depuis le 11-Septembre. Au mois de juin 2015, les parlementaires américains ont refusé de renouveler toute une partie du Patriot Act, dont la section 215. Dans le même temps, ils adoptaient l'« USA Freedom Act », un texte mettant fin à la collecte directe de métadonnées chez les opérateurs téléphoniques.

En France,**c'est le chemin inverse** que nous suivons. Alors que les métadonnées sont de plus en plus intrusives, le législateur fait tout, lui, pour les inscrire dans un régime dérogatoire de plus en plus défavorable aux citoyens. Il y a eu tout d'abord la loi relative à la lutte contre le terrorisme du 23 janvier 2006, qui allégeait le contrôle effectué par la Commission nationale de contrôle des interceptions de sécurité (CNCIS). Ce texte, temporaire, a finalement été pérennisé par la loi de programmation militaire (LPM) du 18 décembre 2013. Il a également étendu les possibilités de collecte. Celle-ci n'est plus limitée au seul cas de « terrorisme » mais peut être justifiée par *« la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, [la lutte contre] la criminalité et la délinquance organisées et [contre] la reconstitution ou le maintien de groupements dissous »*.

En outre, ce ne sont plus seulement les agences dépendant du ministère de la Défense et de l'Intérieur qui peuvent demander la collecte de données, mais aussi le ministère de l'Économie et toutes ses administrations, comme l'organisme de lutte contre le blanchiment Tracfin ou les Douanes. Plus inquiétant, la loi permet d'obliger les hébergeurs et les fournisseurs d'accès à livrer les données *« en temps réel »* et sur *« sollicitation du réseau »*.

Les métadonnées étaient également au cœur de plusieurs dispositions de la récente loi renseignement. Celle-ci étend, entre autres, à cinq années la durée de conservation des *« données de connexion »* (contre trente jours pour les correspondances). Elle autorise également la pose, directement chez les fournisseurs d'accès ou de services, de boîtes noires, des algorithmes censés repérer les apprentis terroristes grâce à la détection des fameux signaux faibles.

[[lire_aussi]]

Et la frénésie législative du gouvernement ne semble pas prête de se calmer. A peine adoptée la loi renseignement, la majorité a déposé à l'Assemblée une nouvelle loi *« relative aux mesures de surveillances électroniques internationales »*. Ce texte répond à une censure partielle de la loi renseignement par la Conseil constitutionnel d'un article sur la collecte des communications internationales. Les Sages avaient jugé cette partie du texte trop succincte car renvoyant pour la plupart des détails d'application à des décrets. La nouvelle loi a donc obligé le gouvernement à dévoiler ses intentions. Or, celle-ci offre des pouvoirs considérables aux services comme celui de se brancher directement sur les câbles transatlantiques par lesquels transitent les flux internationaux. Le texte autorise notamment l'installation de « boîtes noires » semblables à celles prévues pour la France dans la loi renseignement. Placé au cœur du dispositif, le premier ministre aura la possibilité d'autoriser *« l'exploitation non individualisée des données de connexion interceptées. Ces autorisations déterminent la ou les finalités poursuivies ainsi que les types de traitements automatisés pouvant être mis en œuvre en précisant leur objet »*.

L'argument avancé, en France comme aux États-Unis, pour justifier ce régime dérogatoire est toujours le même : les métadonnées ne seraient pas des données privées. Elles ne seraient que *« des données sur les données »* et auraient donc un caractère intrusif limité. Or, cette interprétation est largement contredite. Que ce soit par le président de la Commission nationale de contrôle des interceptions de sécurité (CNCIS), Jean-Marie Delarue (le « Monsieur Écoutes » de l'État), la Commission nationale de l'informatique et des libertés (Cnil) ou par la quasi-totalité des chercheurs et experts sur le sujet.

L'un des exemples les plus parlants pour expliquer l'utilité des métadonnées et leur caractère intrusif est sans doute celui pris par l'un des spécialistes les plus réputés en matière de sécurité informatique, l'Américain Bruce Schneier, dans **une note de blog publiée en septembre 2013**. Imaginez que vous deviez placer sous surveillance une personne et que vous n'ayez le choix qu'entre deux méthodes. Dans l'une, vous pourriez intercepter les conversations, sonoriser les lieux… mais vous n'auriez accès qu'à ces contenus, sans le contexte. Dans l'autre, vous auriez accès uniquement aux « métadonnées » qu'elle a pu émettre. Vous sauriez à qui elle a parlé, téléphoné, écrit, combien de temps cela lui a pris, où elle s'est rendue, quels magasins elle a visités, les achats qu'elle a pu y faire… Laquelle vous semble la plus efficace, et donc la plus intrusive ? Pour Bruce Schneier, la réponse est claire. *« Quand le gouvernement collecte des métadonnées sur des personnes, le gouvernement les place sous surveillance. Quand le gouvernement collecte des métadonnées sur un pays entier, il place tout le monde sous surveillance. Quand Google le fait, il fait la même chose. Métadonnées égalent surveillance ; c'est aussi simple que cela »*, conclut-il.

Si ce refus obstiné de reconnaître les métadonnées semble nier l'évidence, il correspond en fait à une logique, celle du big data. Ce concept, venu du monde de l'entreprise, n'est pas nouveau. Dès les années quatre-vingt-dix se sont développées des techniques de management des risques visant à tenter de « prédire » le futur par l'analyse de données. Aujourd'hui, ce rêve économique, dans lequel on pourrait prévoir les fluctuations des cours d'une action, connaître la date de décès d'un assuré ou encore prédire le comportement d'un consommateur sur Internet, semble à portée de main en raison de deux facteurs.

Algorithmes et police prédictive

Tout d'abord, l'explosion du « web 2.0 » et de ses réseaux sociaux a offert au big data la masse critique de données dont il avait besoin. Avec l'émergence de services participatifs tels que YouTube, Facebook, Google ou Twitter, la quantité de données mises en ligne a été démultipliée. Et, pour faciliter les choses, ce sont les internautes eux-mêmes qui alimentent volontairement ces ogres numériques d'informations aussi nombreuses que variées. Une fois constitué, le big data avait besoin de machines assez puissantes pour pouvoir être exploité. Grâce à la progression exponentielle de la puissance des composants électroniques, c'est le cas depuis déjà quelques années. Ces nouveaux moyens ont remis

au goût du jour certaines théories mathématiques en sommeil dans le domaine de la statistique et des probabilités. De nombreux laboratoires ont ainsi développé, parfois dans le cadre de partenariats avec des entreprises privées, des programmes visant à mettre sur pied des « algorithmes prédictifs » reposant sur le big data. Les premiers « partenaires » des chercheurs ont été les banques, les assurances, les publicitaires.

La surveillance étatique n'a fait que suivre la nature de l'économie numérique actuelle qui permet une collecte, une analyse et un tracking en temps réel des données et des utilisateurs. Ce choix du big data s'inscrit dans une logique économique de rationalisation des coûts. Les solutions techniques sont d'ailleurs très attractives en raison de la prolifération de logiciels, de solutions « clefs en main » à la compétitivité imbattable. Selon une étude de Kevin Bankston et Ashkan Soltani **publiée par The Yale Law Journal Online** en janvier 2014, la surveillance physique d'une personne coûte en moyenne 275 dollars de l'heure, la géolocalisation 10 dollars, et la surveillance d'un téléphone seulement 5,21 dollars de l'heure.

© Reuters

Mais la technologie n'est pas neutre. Les informations collectées et soumises aux algorithmes sont souvent présentées comme une matière première anonyme, des « données brutes ». Pourtant, comme l'explique la chercheuse américaine Lisa Gitelman dans son livre *Donnée brute est un oxymore* (***Raw Data Is an Oxymoron***), les informations que nous émettons chaque jour sont des produits culturels qui seront interprétés et traités par des algorithmes en fonction de critères économiques, sociaux ou politiques. Les données sont donc davantage « générées » par les surveillants que réellement collectées. Seul l'algorithme leur donnera un sens et une utilité.

La question n'est donc pas tant de savoir quelles données sont collectées mais quels algorithmes leurs sont appliqués. Or, ces derniers ont souvent le même but : préempter l'avenir. Le bon technologique en matière de statistiques et de probabilités a permis de mettre au point de nouveaux « algorithmes prédictifs », capables « d'auto-apprendre » des données pour se perfectionner grâce à la technique du machine learning. Ces nouveaux logiciels ont d'abord été le fruit de partenariats entre laboratoires de recherche et sociétés privées. Mais, très vite, ces nouveaux algorithmes ont séduit les gouvernements.

En 2002, la presse américaine a ainsi révélé l'existence du programme **« Total Information Awareness »**, TIA (« Connaissance totale de l'information »), mené par l'Information Awareness Office (IAO), le bureau de la connaissance de l'information, une émanation du département de recherches du Pentagone, le Darpa. Le programme TIA était fondé sur le « maintien de l'ordre prédictif » par le data mining et avait pour but de constituer une gigantesque base de données sur les citoyens américains afin de détecter d'éventuelles menaces. Face à la polémique provoquée par ces révélations, le Congrès avait, fin 2003, supprimé le financement de l'IAO. Le programme TIA, lui, a été abandonné au même moment, tout du moins officiellement. Car les programmes dévoilés par Edward Snowden montrent que le projet **n'a en réalité jamais été interrompu**, seulement réparti au sein d'autres programmes ou sous-traité par des contractants.

En France, les fameuses boîtes noires de la loi renseignement s'inscrivent directement dans cette logique de « police prédictive ». Celle-ci est d'ailleurs pleinement assumée par le ministère de l'Intérieur. Le jeudi 21 mai 2015, à Cergy-Pontoise, Bernard Cazeneuve a ainsi inauguré les nouveaux locaux du pôle judiciaire de la gendarmerie nationale (PJGN) abritant le SCRC (le service central de renseignement criminel), l'Institut de recherche criminelle de la

gendarmerie nationale (IRCGN), le Centre de lutte contre les criminalités numériques (C3N). À cette occasion, la gendarmerie a fait **la démonstration d'un algorithme prédictif** en activité depuis la fin de l'année 2014. Il intègre des données issues des faits constatés par les forces de l'ordre et des statistiques de l'Insee, pour ensuite fournir des cartes permettant d'analyser la criminalité et de prédire son évolution.

Ce nouveau mode de surveillance soulève de nombreuses questions. À commencer par celle de son efficacité. La plupart du temps, les résultats de ces prédictions sont gardés secrets, et donc invérifiables. Si les progrès techniques en matière de prédiction sont indéniables, beaucoup de chercheurs alertent sur les différents biais pouvant fausser des résultats et donner des « faux positifs » qui, même minoritaires, sont susceptibles d'être catastrophiques pour les personnes concernées.

Au mois de mars 2014, un groupe de chercheurs avait publié **dans la revue *Science* une étude** sur l'un des exemples ayant contribué à la popularisation du big data : le suivi de l'épidémie de grippe par Google en 2008. À l'époque, le géant américain avait annoncé en grande pompe qu'il mettait la puissance de ses algorithmes au service de la santé publique, alors menacée par la propagation du virus de la grippe aux États-Unis. L'outil Google Flu Trends était censé repérer les premières apparitions de la grippe dans une région, avant qu'elle ait eu le temps de s'installer, grâce à une analyse des métadonnées collectées sur les usagers de Google.

Cependant, selon les chercheurs, les prévisions de Google se sont révélées fausses. L'algorithme collectait la moindre donnée pouvant faire penser à la grippe. Or, un individu qui réalise une recherche sur Internet parce que son nez coule un peu n'est pas forcément atteint par le virus. Dans ce cas, l'algorithme avait largement surestimé les cas d'infection, rendant invalides tous les calculs. Les chercheurs soulignaient ainsi l'un des grands dangers de ces prédictions qu'ils nomment le *big data hubris*. Cela désigne *« la supposition souvent implicite que le big data est un substitut, plutôt qu'un complément, à la collecte et l'analyse traditionnelle des données »*.

De la surveillance au contrôle des populations

Au-delà des questions d'efficacité ou de protection de la vie privée, le big data est un choix politique. Il impose un nouveau mode de gouvernance non plus fondé sur la recherche d'informations ou de causes mais sur la gestion de risques. On ne cherche plus à comprendre, à analyser, par exemple un contenu radical. Il suffit de surveiller qui le visionne, le « like », le partage. On ne cherche plus le « pourquoi » mais le « quand », à établir un lien entre les terroristes d'hier et ceux de demain.

Cette surveillance passive, globale, indifférenciée, visant non pas à espionner tel ou tel individu mais à garder sous contrôle l'ensemble de la population afin d'y détecter les « signaux faibles », a été traitée par de nombreux chercheurs et experts. Certains l'appellent ***« dataveillance »*** ou encore ***« surveillance liquide »***. La chercheuse belge Antoinette Rouvroy a, elle, théorisé la notion de *« gouvernementalité algorithmique »* qu'elle définit comme *« une stratégie de neutralisation de l'incertitude »*. Cette politique de gestion de risques appliquée à la population a pour but d'éradiquer la subjectivité en appliquant aux individus une réalité imposée par les catégories entrées dans les algorithmes. L'objectif n'est pas tant d'intervenir mais de préempter le futur, de faire en sorte que des événements ne se produisent pas. L'algorithme remplace ainsi la norme. *« Nous sommes passés du couple "normatif-répression" à un couple "anomie-préemption" »*, expliquait Antoinette Rouvroy à Mediapart dans **une interview réalisée au mois de mai 2015**. *« Les décideurs politiques*

ne veulent plus décider du contenu de la norme. Les données donnent les critères de qualification du réel », expliquait-elle.

La prison Presidio Modelo à Cuba © *Friman / Wikipedia*

Mais de nombreux chercheurs voient dans la société actuelle la réalisation de la *« société de contrôle »* annoncée (notamment) par Gilles Deleuze au début des années quatre-vingt-dix. Le philosophe entendait alors prolonger les travaux de Michel Foucault, théoricien de la société disciplinaire et auteur de Surveiller et punir. Dans cet ouvrage de référence, publié en 1975, le philosophe analysait les mécanismes disciplinaires de la société. Ces derniers reposaient sur un contrôle direct des corps des individus à travers une série de lieux fermés. On passait de la cellule familiale à l'école, puis à l'armée, à l'usine, éventuellement par l'hôpital ou la prison. Chacun de ces lieux était organisé selon des règles strictes et un quadrillage spatial permettant une surveillance totale. Celle-ci était fondée sur le modèle du « panopticon », une architecture imaginée au XVIII^{e}siècle par le philosophe britannique Jeremy Bentham. Au centre s'y trouve le surveillant, dissimulé dans une tour lui offrant une vision à trois cent soixante degrés. Autour, les surveillés installés dans des cellules ouvertes pour être vus à chaque instant.

[[lire_aussi]]

Cette grille d'analyse ne correspond plus à la situation actuelle et au passage à la « société de contrôle » décrit par Gilles Deleuze dans son ***Post-scriptum sur les sociétés de contrôle***. À l'époque, la société disciplinaire reposait sur une organisation économique et sociale fixe, permettant d'encadrer physiquement les citoyens. Mais, aujourd'hui, la plupart de ces institutions se sont en grande partie transformées et ouvertes vers l'extérieur. La surveillance a donc dû s'adapter. Suivant l'évolution de la société, elle est à la fois plus fluide, plus mobile et surtout invisible. De centralisée elle devient « rhizomique », c'est-à-dire horizontale et multidirectionnelle, capable de s'infiltrer dans tous les espaces. Contrairement à la société disciplinaire, la surveillance à l'ère des big data ne se focalise plus seulement sur les corps, sur la population, mais sur leurs interactions quotidiennes. Selon le philosophe, les individus sont dépouillés de ce qui faisait leur « individualité » par les catégories imposées par les algorithmes. Ils deviennent des « dividuels ».

Plus qu'un simple système d'espionnage mondial, c'est un nouveau mode de gouvernance fondé sur un contrôle secret et insidieux des populations qu'Edward Snowden nous a révélé. La nature même de cette nouvelle idéologie explique en partie les difficultés à le rendre explicite auprès du grand public. Non, la NSA n'a pas la capacité d'intercepter et de stocker l'intégralité du trafic mondial d'Internet. Mais, oui, elle a la capacité de le « monitorer », de le surveiller pour collecter de manière automatisée toutes les données qui l'intéressent et d'y repérer des « signaux faibles ». Non, les services de renseignement n'écoutent pas toutes les conversations, pas plus qu'ils ne lisent tous les e-mails. Mais, oui, ils disposent des outils permettant d'en analyser les métadonnées et ainsi retracer tous vos contacts, vos cercles relationnels et même deviner vos envies et vos désirs.

Les concepts de métadonnées ou de big data sont encore trop récents pour avoir été assimilés dans le débat public. **La validation de la loi renseignement** par le Conseil constitutionnel, le 23 juillet 2015, a été un coup dur pour les défenseurs des libertés. Mais ils ne désarment pas. Les débats parlementaires ont eu comme effet positif de mobiliser les opposants et de sensibiliser certains acteurs. Jamais un texte de loi n'a été autant critiqué, par les ONG mais aussi par des syndicats professionnels et des autorités administratives telles que la Cnil, le Conseil national du numérique, la Commission nationale de contrôle des interceptions de sécurité

ou encore la Commission nationale consultative des droits de l'homme. L'ensemble des rapports et avis produits ces derniers mois, la mobilisation impressionnante des associations, celle de certains élus, a incontestablement permis d'ouvrir une brèche dans le discours sécuritaire du gouvernement.

Ces militants ont également lancé une véritable guérilla juridique, débutée devant le Conseil d'État et Conseil constitutionnel et qui devrait se poursuivre devant les juridictions européennes. **Mardi 6 octobre**, la Cour de justice de l'Union européenne (CJUE), saisie par un jeune Autrichien en conflit avec Facebook, a justement annulé le Safe Harbor, l'accord autorisant les entreprises américaines à transférer sur leur territoire les données collectées sur les citoyens américains. L'un des principaux arguments avancés par les juges dans cette décision historique est le fait que les activités des services américains ne permettent pas d'assurer un niveau de protection des données personnelles suffisant. Or, c'est peu ou prou les mêmes mesures que la France est en train de décider dans ses lois renseignement et sur la surveillance internationale.

Certes, cette mobilisation n'a pas suffi pour faire obstacle à ces textes. Mais si les États-Unis ont été forcés de reconnaître en partie leurs erreurs, pourquoi pas la France ? Un jour…

Sur mediapart.fr, un objet graphique est disponible à cet endroit.

La République sur écoute,
chroniques d'une France sous surveillance
Editions Don Quichotte
276 pages. 18,90 euros

Directeur de la publication : Edwy Plenel
Directeur éditorial : François Bonnet
Le journal MEDIAPART est édité par la Société Editrice de Mediapart (SAS).
Durée de la société : quatre-vingt-dix-neuf ans à compter du 24 octobre 2007.
Capital social : 28 501,20€.
Immatriculée sous le numéro 500 631 932 RCS PARIS. Numéro de Commission paritaire des publications et agences de presse : 1214Y90071 et 1219Y90071.
Conseil d'administration : François Bonnet, Michel Broué, Gérard Cicurel, Laurent Mauduit, Edwy Plenel (Président), Marie-Hélène Smiéjan, Thierry Wilhelm. Actionnaires directs et indirects : Godefroy Beauvallet, François Bonnet, Laurent Mauduit, Edwy Plenel, Marie-Hélène Smiéjan ; Laurent Chemla, F. Vitrani ; Société Ecofinance, Société Doxa, Société des Amis de Mediapart.
Rédaction et administration : 8 passage Brulon 75012 Paris
Courriel : contact@mediapart.fr
Téléphone : + 33 (0) 1 44 68 99 08
Télécopie : + 33 (0) 1 44 68 01 90
Propriétaire, éditeur, imprimeur : la Société Editrice de Mediapart, Société par actions simplifiée au capital de 28 501,20€, immatriculée sous le numéro 500 631 932 RCS PARIS, dont le siège social est situé au 8 passage Brulon, 75012 Paris.
Abonnement : pour toute information, question ou conseil, le service abonné de Mediapart peut être contacté par courriel à l'adresse : serviceabonnement@mediapart.fr. ou par courrier à l'adresse : Service abonnés Mediapart, 4, rue Saint Hilaire 86000 Poitiers. Vous pouvez également adresser vos courriers à Société Editrice de Mediapart, 8 passage Brulon, 75012 Paris.