ÉDITORIAL
ÉRIC CHOL

Controlite aigüe

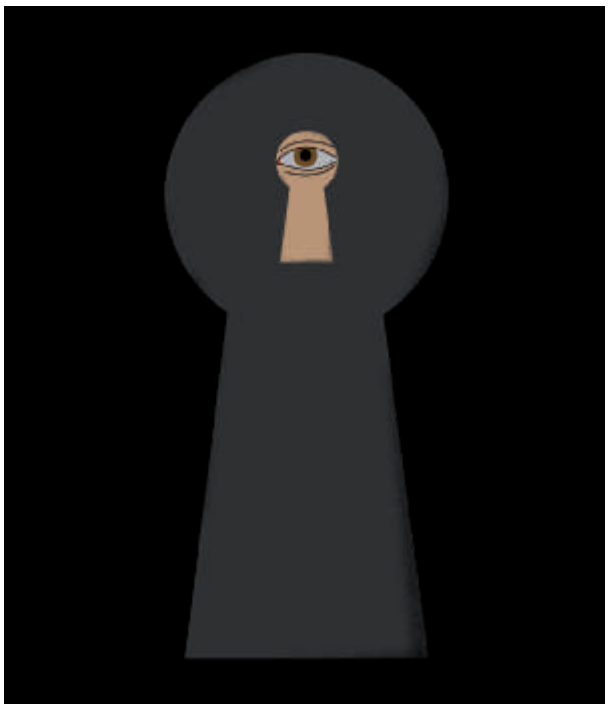
Au moment où les Etats-Unis, tirant les leçons des excès et surtout de l'inefficacité du Patriot Act, acceptent enfin d'alléger ce dispositif liberticide, au moment où les juges de la Cour constitutionnelle de Belgique font valdinguer l'arsenal de surveillance, les parlementaires français, eux, jouent le filon sécuritaire, symbolisé par l'adoption du projet de loi sur le renseignement. Le débat est presque clos et, reconnaissons-le, en dehors d'une poignée de juristes, d'ONG ou de défenseurs des libertés, il n'aura intéressé personne. A croire que nos démocraties valent bien quelques messes basses sur le renseignement : pour vivre heureux, vivons sous surveillance ! Car c'est de cela qu'il s'agit. Deux siècles après les fiches du ministre de la Police Joseph Fouché, voici venu le temps des boîtes noires et des métadonnées. Au nom de la lutte contre le terrorisme, la préservation de la sécurité publique passerait par des petits arrangements avec les libertés privées : la liste – chaque jour plus longue – des candidats français au djihad donne carte blanche aux successeurs de Fouché, désireux de posséder à leur tour *"des yeux pour voir et des oreilles pour entendre"**. Mais pour voir qui ou entendre quoi ? *"Si des algorithmes sont capables de nous recommander des films à regarder, pourquoi ne pourraient-ils pas nous conseiller des suspects sur lesquels enquêter ?"* s'interroge le chercheur américain Evgeny Morozov**. Certes, la France n'est pas la seule à vouloir déplacer le curseur vers un peu moins de liberté et un peu plus de sécurité. Le Canada et la Suisse sont eux aussi touchés par la même fièvre. Pour éviter que ce virus de la controlite de masse s'étende, il est urgent de multiplier les garde-fous. La Cour européenne de justice a montré la voie en avril 2014, en invalidant une directive européenne sur la conservation des données. En France, le Conseil constitutionnel aura lui aussi son mot à dire. Pour tenter de concilier ordre et libertés, les sages pourront évoquer les cinquante nuances élémentaires de la démocratie, allant de la transparence jusqu'à l'octroi de garanties.

* *Mémoires* de Joseph Fouché, 1825.
** *Le Monde* du 2 juin 2015.

En couverture :
— *Dessin de Brian Stauffer/The Ispot.com*
— *Lisbonne : photo de Pauliana Pimente/Picture Tank*
— *Dessin de Faber paru dans* Le Jeudi, *Luxembourg*

La photo du film Waterloo, 1970 *en une du nº 1284 provenait de l'agence Photo12/Alamy*

Sommaire



FALCO, CUBA

KOUNTOURIS, GRÈCE

SUR NOTRE SITE

www.courrierinternational.com

Enquête. *En quoi les traités transatlantiques sont des permis de polluer, par l'hebdomadaire allemand* Die Zeit.

Télévision. *Regardez l'émission* Tea Time Club, *talk-show planétaire de la journaliste Caroline Gillet, qui contacte des gens aux quatre coins de la planète. Sur Skype, elle discute avec eux de sujets très personnels.*

Waterloo. *Le 18 juin, l'Europe célèbre le bicentenaire de la défaite de Napoléon. Suivez les réactions de la presse européenne.*

Retrouvez-nous aussi sur Facebook, Twitter, Google+ et Pinterest

à la une

TOUS SUSPECTS

Dans une large indifférence, l'Assemblée nationale puis le Sénat français ont voté un projet de loi qui étend considérablement les pouvoirs de surveillance du gouvernement. La France n'est pas la seule : la peur des attentats pousse de nombreux pays occidentaux à faire le choix de la surveillance *(lire p. 33)* et les opinions publiques ne s'émeuvent guère des risques pour la vie privée. Celle-ci est pourtant un fondement de la démocratie *(p. 31)* et de nos relations sociales *(p. 34)*.

La fin de la **vie privée ?**

La révolution numérique a eu des répercussions colossales sur la surveillance. Pour préserver notre intimité, il est urgent d'encadrer l'usage des nouvelles technologies.

—The Nation *(extraits) New York*

Imaginez un Etat qui obligerait ses citoyens à déclarer en permanence où ils se trouvent, avec qui, ce qu'ils font, à qui ils parlent, à quoi ils consacrent leur temps et leur argent. Aucun de nous ne voudrait y vivre. Les associations de défense des droits de l'homme condamneraient cet Etat qui bafoue la dignité humaine et la liberté. Nous plaindrions ses habitants, privés des droits essentiels dans une démocratie libérale.

Et pourtant, c'est dans cet Etat que nous vivons aujourd'hui, à une différence près : l'Etat ne nous oblige pas directement à partager avec lui ces informations personnelles. Il en délègue la collecte à des entreprises privées, puis il pioche à volonté. Nous "acceptons" de partager ces informations avec les entreprises qui nous permettent d'accéder à notre monde connecté. Nos téléphones portables informent en permanence notre opérateur de notre localisation et des destinataires de nos appels et messages. A chaque courrier électronique envoyé, nous partageons l'adresse, l'objet et le contenu du mail avec le fournisseur d'accès. A chaque recherche ou lecture sur Internet, nous dévoilons nos centres d'intérêt aux compagnies qui gèrent les navigateurs et les moteurs de recherche. Et à chaque achat avec notre carte de crédit, des traces de la transaction sont conservées.

Bref, nous partageons la quasi-intégralité de nos vies avec toute une série d'entreprises privées. En théorie, nous gardons la possibilité de "refuser" cette collecte : nous pouvons faire le choix d'une vie d'ermite et nous couper de tous les moyens de communication modernes. Mais c'est cher payer la préservation de notre intimité. Ne pouvons-nous pas avoir à la fois un smartphone et une vie privée ?

Ermite. La révolution numérique a des répercussions colossales sur la surveillance. Avant Internet, l'essentiel des renseignements qui sont désormais recueillis sur nous n'était pas disponible, ou bien à un coût prohibitif. Si l'Etat voulait vous localiser à n'importe quel moment, il pouvait mettre en place une filature vingt-quatre heures sur vingt-quatre, sept jours sur sept, mais la procédure était très coûteuse et vouée, à long terme, à être éventée. Et cette surveillance, si suivie soit-elle, ne permettait pas de voir ce que vous faisiez derrière des murs. De nos jours, nous avons toujours ou presque notre téléphone portable sur nous, qui nous piste en permanence.

Autrefois, si l'Etat voulait connaître vos lectures ou vos pensées, il avait la possibilité de perquisitionner votre domicile, à condition d'avoir des soupçons légitimes et un mandat de la justice. Mais il ne trouvait chez vous que ce que vous gardiez à portée de main. L'Etat n'avait, en revanche, aucun moyen de savoir à quoi vous pensiez, si ce n'est en vous posant directement la question. Aujourd'hui, il n'a qu'à télécharger l'historique de vos recherches sur Google, qui en dit plus long sur vos pensées que vous ne pourriez le faire vous-même. D'autant que l'ordinateur, lui, n'oublie rien.

Et les ordinateurs n'ont pas seulement une mémoire infaillible : ils ont aussi la capacité de stocker et d'analyser des quantités phénoménales de renseignements sur n'importe qui – et même sur chacun de nous –, comme l'ont montré en 2013 les révélations du lanceur d'alerte Edward Snowden sur les programmes de surveillance de masse de l'Etat américain. Snowden a révélé que, depuis plus de dix ans, l'Agence de sécurité nationale américaine (NSA) collectait les métadonnées téléphoniques [heure et durée de l'appel, numéro appelé] de presque tous les Américains [cette collecte a été arrêtée avec le vote du Freedom Act le 2 juin, *voir p. 34*].

Traque généralisée. La surveillance exercée par la NSA à l'étranger est plus intrusive encore. L'agence intercepte et collecte en masse les échanges électroniques (SMS, appels, courriers électroniques, listes de contacts et navigation Internet) de millions d'étrangers sur lesquels ne pèse pas le moindre soupçon. La traque généralisée, impossible jusqu'à une date récente, est aujourd'hui une réalité. Les technologies numériques ont augmenté de façon exponentielle la capacité de l'Etat à dresser le portrait intime de n'importe quel individu à partir de données diverses, qu'il peut combiner et analyser.

Les partisans de la surveillance de masse brandissent souvent l'argument selon lequel quand on n'a rien à cacher, on n'a rien à craindre. Mais ce raisonnement fait fi du fait qu'il n'y a pas que les délinquants qui tiennent à leur vie privée. Nous fermons tous la porte de nos chambres et de nos domiciles, que nous nous livrions à des activités criminelles ou non. Nous protégeons l'accès à nos ordinateurs par des mots de passe. La vie privée a une foule d'autres vertus que celle de protéger les criminels. Si ce n'était pas le cas, nous n'aurions jamais cherché à la préserver. Certains estiment que le concept de vie privée est relativement récent, l'humanité ayant vécu l'essentiel de son histoire dans de petites communautés rurales où nul n'ignorait les secrets de ses voisins. Mais la question n'est pas de savoir si la vie privée est une invention récente ou non, mais si elle est précieuse : dès lors qu'elle nous est précieuse, nous devons nous battre pour la protéger des assauts des nouvelles technologies de surveillance.

Il est possible de faire évoluer la réglementation au regard des nouvelles technologies. C'est d'ailleurs ce que fait régulièrement la Cour suprême américaine dans les domaines, par exemple, de l'automobile, de la téléphonie ou de l'imagerie thermique. En 2012, la Cour a ainsi estimé que le quatrième amendement n'autorisait pas l'Etat à utiliser un GPS pour suivre, vingt-quatre heures sur vingt-quatre durant vingt-huit jours, les déplacements publics d'une voiture. Les pouvoirs publics se fondaient sur un précédent, datant de l'ère des technologies analogiques, qui avait autorisé les agents publics à utiliser un bipper caché dans un colis pour suivre le trajet d'une automobile sur des routes publiques, au motif que ce qui est visible en public ne peut être privé. Dans le cas du GPS, cependant, la Cour a délivré un verdict contraire, cinq juges ayant estimé que les technologies du numérique changeaient la donne et nécessitaient un cadre réglementaire nouveau et plus protecteur. De son côté, le Congrès peut aussi adopter des lois pour protéger la vie privée des menaces créées par les nouvelles technologies.

Sondage

LES AMÉRICAINS DOUTENT

D'après un récent sondage de la chaîne CNN, 61 % des Américains souhaitaient que le programme de collecte de métadonnées téléphoniques de la NSA, reposant sur des dispositions du Patriot Act arrivées à expiration, soit prolongé. Pourtant, selon un autre sondage de l'institut Pew, deux semaines plus tôt, 74 % des personnes interrogées affirmaient qu'il est *"très important"* d'avoir un contrôle sur *"les personnes qui peuvent avoir des informations sur vous"*. La clé de cette contradiction serait à chercher du côté de la peur, estime le site The Daily Beast : *"Quand on a peur, on est prêt à renoncer à des libertés. Et nous, peuple américain, nous avons peur depuis le 11 septembre."*

→ *Dessin de* **Beppe Giacobbe,** *Italie.*

Nous partageons la quasi-intégralité de nos vies avec toute une série d'entreprises privées

Il nous faut également lutter contre les menaces sur la vie privée émanant du secteur privé. Nul doute que nous ayons davantage à craindre de l'Etat que de Google : seul l'Etat a le pouvoir d'arrêter, de traduire en justice et d'emprisonner, et tous les gouvernements ont tendance à cibler les opposants. Il n'en reste pas moins que, face à des entreprises qui elles aussi s'immiscent dans notre vie privée, nous avons intérêt à encadrer les usages qu'elles peuvent faire des renseignements collectés par nous et sur nous. En Europe, par exemple, des lois limitent l'usage des données personnelles, aussi bien par les pouvoirs publics que par le secteur privé.

Pronostic. C'est un fait : la vie privée n'a jamais été plus menacée qu'aujourd'hui. L'ère du numérique nous apporte de nombreux avantages, mais elle fait aussi surgir de nouveaux périls. Fort de ce constat, certains estiment déjà que la vie privée est morte. C'est un verdict excessif et dangereux : il est, pour l'heure, largement exagéré d'annoncer la fin de la vie privée, mais il se peut que son pronostic vital soit engagé. Si nous n'exigeons pas une nouvelle réglementation pour régir et encadrer l'usage de ces nouvelles technologies, nous y laisserons non seulement notre vie privée, mais aussi tout ce qui en découle – dont la démocratie elle-même.

—David Cole
Publié le 23 mars

SOURCE

THE NATION
New York, Etats-Unis
Hebdomadaire, 113 000 ex.
www.thenation.com
Fondé en 1865, résolument à gauche, **The Nation** est l'un des premiers magazines d'opinion américains. Il s'intéresse autant à la politique qu'aux faits de société et à la culture.

Le virage **sécuritaire** français

Le gouvernement a choisi de renforcer la surveillance numérique au détriment des libertés civiles. Dans une indifférence quasi générale, s'étonnent ces deux chroniqueurs américains.

—The New York Times *New York*

Deux années durant, après les révélations d'Edward Snowden, les débats ont fait florès en Europe à propos des excès commis par les Américains dans le domaine de la surveillance de masse. On y dénonçait – y compris de dirigeants comme la chancelière allemande Angela Merkel – les opérations de la NSA, qui interceptait courriels et conversations téléphoniques, tissant ainsi un réseau qui semblait envelopper le continent.

Mais, à la lueur de ces derniers mois, on comprend ce qui dérangeait en réalité l'Europe : le fait que ce réseau soit américain plutôt que la surveillance en elle-même. Redoutant les extrémistes islamiques sur son territoire, la Grande-Bretagne, pendant l'été [dernier], a voté des lois encore plus draconiennes à ce propos. Et au lendemain des attentats de janvier à Paris les Français ont entrepris ce qui est presque devenu un rite de passage dans les pays occidentaux depuis le 11 septembre 2001 et les attentats aux Etats-Unis, en faisant voter par l'Assemblée le 5 mai [et par le Sénat le 9 juin] une extension considérable des pouvoirs des autorités en matière de protection et d'espionnage de ses propres citoyens.

Métadonnées. Même Angela Merkel, qui en 2013 avait fait la leçon à Barack Obama sur ce qu'avait vécu sa famille du temps de la Stasi en Allemagne de l'Est, a dû rappeler à des journalistes il y a peu que l'Allemagne était souvent contrainte de surveiller ses citoyens – tout en éludant la question de l'ampleur de la coopération de ses services avec la NSA pour fouiner du côté de chez Airbus.

Cette tendance européenne à davantage de protection gouvernementale au détriment des libertés civiles n'a rien de nouveau. Tout le monde a entendu parler des réseaux de télésurveillance dans les quartiers des grandes villes britanniques. La France procède de même depuis des années, mais sans autorisation légale explicite. Reste que certaines des mesures prévues par le nouveau projet de loi sont inédites, permettant notamment le recours à des technologies dernier cri pour analyser des métadonnées brutes, selon les spécialistes.

En réalité, cependant, il est peu probable que l'une ou l'autre des mesures envisagées aurait pu empêcher l'attentat contre *Charlie Hebdo* en janvier, dit-on de source bien informée à Paris. Et si la lutte contre le terrorisme a servi de justification au vote de l'Assemblée, qui va donc accroître considérablement les pouvoirs des services de renseignements du pays, d'aucuns soulignent que la loi autorise également une surveillance élargie dans d'autres domaines.

Ces mesures n'ont presque pas éveillé l'attention de l'opinion publique ni suscité de débat – par exemple pour savoir si la France a besoin dans ce secteur de garde-fous comparables à ceux mis en place aux Etats-Unis. A vrai dire, c'est tout juste si la nouvelle a fait la une des journaux, alors même que, les jours précédant le vote, plusieurs médias avaient clairement mis en lumière les risques potentiels d'abus inhérents à ce projet de loi exhaustif.

Il est peu probable que l'une ou l'autre des mesures envisagées aurait pu empêcher l'attentat contre *Charlie Hebdo*

Dans le même temps, le Congrès américain, lui, fait marche arrière. [Un projet de loi qui met fin à la collecte massive de données téléphoniques par le gouvernement a été voté le 2 juin. Ces données seront désormais stockées par les opérateurs téléphoniques et transmises sur autorisation d'un juge, voir p. 34]. Après plus de dix ans d'opérations de surveillance massives, dont l'étendue est restée floue jusqu'aux révélations de Snowden, la NSA se voit désormais obligée de justifier ses programmes auprès de la Maison-Blanche et du peuple américain.

En Europe, le tollé provoqué par les fuites de Snowden était surtout lié à ce qui était perçu comme une intrusion du système de surveillance de Washington sur le sol européen, parfois avec l'aide, volontaire ou non, de sociétés américaines. *"Chez les Européens, il est courant de considérer que le continent favorise le respect de la vie privée tandis que les Etats-Unis s'accommoderaient, eux, d'une NSA digne de la Stasi et de fourbes collecteurs de données comme Google et Facebook,* explique Benjamin Wittes, coauteur de *The Future of Violence* ["L'avenir de la violence", inédit en français]. *C'est absurde. Ce qui les dérange, c'est que ce soit américain."*

A l'exception, peut-être, de l'Allemagne, où la levée de boucliers concerne les agissements supposés du BND, les services de renseignement fédéraux, en liaison avec les Etats-Unis. Pour ce qui est des réseaux sociaux, les sensibilités européennes sont en train d'évoluer. Même les pays qui chérissent la discrétion sont confrontés au fait, incontournable, que nous vivons dans une nouvelle ère de communications planétaires qui compromettent le respect de la vie privée, et qu'il est difficile de préserver quelque secret que ce soit sur Internet. C'est peut-être cela qui pousse les citoyens à accepter plus facilement la surveillance des autorités.

En France, l'opposition au projet de loi n'a eu que peu d'écho, même si ses détracteurs ont avancé qu'il allait permettre au renseignement français de récolter et de traiter toutes les communications, de lire les textos et les courriels, et de mettre sur écoute les téléphones portables sans réel discernement judiciaire. De nombreux opérateurs Internet, des militants des droits civiques et certains députés de gauche, mais aussi des juges et des avocats sont ainsi montés au créneau pour dénoncer le projet. Mais ils n'ont guère été soutenus sur le plan politique : l'hostilité viscérale à l'Etat qu'on peut rencontrer chez les libertariens ou chez les membres du Tea Party aux Etats-Unis n'existe pas en Europe occidentale. Et, si les projets de loi ne sont pas tous votés aveuglément, les propositions du gouvernement sont rarement passées au crible.

Exemple. De même que les attentats du 11 septembre avaient conduit le président George W. Bush et le Congrès à accorder des pouvoirs démesurés aux services de renseignements américains, les attaques meurtrières en France et en Europe ainsi que l'inquiétude suscitée par le départ de milliers de jeunes munis de passeports européens en Syrie et en Irak vont permettre au renseignement et aux services de sécurité d'obtenir des pouvoirs dont ils étaient auparavant dépourvus.

Les défenseurs des droits de l'homme et de la vie privée s'inquiètent de la façon dont le gouvernement français va se servir de cette nouvelle loi, mais surtout du précédent créé par la France. *"J'ai bien peur que la France ne soit montrée en exemple, et que cela n'entraîne une escalade au niveau mondial",* explique Cynthia Wong, avocate et spécialiste des questions liées à Internet pour Human Rights Watch. *"Si la France s'y met, qu'est-ce qui va empêcher les autres gouvernements de faire pareil ?"*

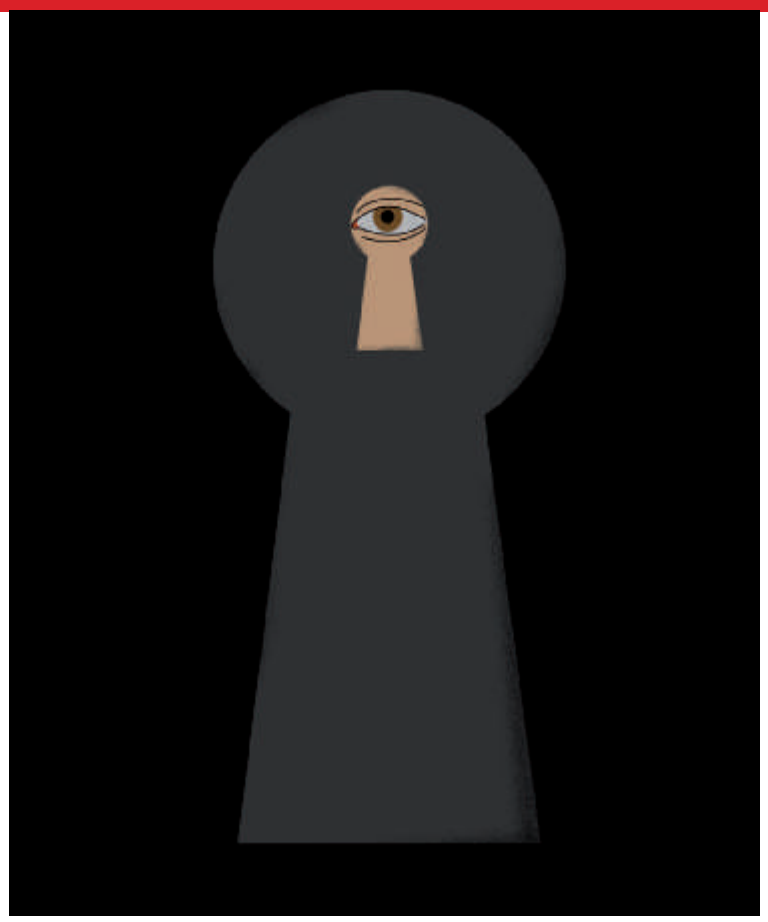
—Alissa J. Rubin et David E. Sanger
Publié le 6 mai

Vu de Berlin

DOUBLE JEU

"Le scandale de l'espionnage par la NSA [...] est aussi un scandale pour la chancelière", accuse **Der Spiegel** dans son édition du 2 mai titrée *"La trahison".* A l'index : Angela Merkel (CDU), le ministre de l'Intérieur Thomas de Maizière (CDU) et le chef du BND (renseignement extérieur allemand). En cause : la collaboration encore plus importante que ce qu'on pensait jusque-là entre les services de renseignements allemands et la NSA américaine. Et le cœur du pouvoir était au courant, dénonce l'hebdomadaire. Grâce à l'aide du BND, la NSA a ainsi pu espionner pendant des années des entreprises comme EADS, mais aussi des institutions et des hommes politiques européens.

↓ *Dessin de* **Walenta,** *Pologne.*



← *Dessin de* **Falco,** *Cuba.*

ROYAUME-UNI NON À L'ÉTAT ESPION

Le raisonnement qui sous-tend le projet de loi donnant plus de pouvoirs aux renseignements britanniques est erroné : la collecte tous azimuts de données ne mène pas à plus de sécurité.

—The Guardian *Londres*

Alors que le Congrès américain vient de voter [le 2 juin 2015] le USA Freedom Act afin de limiter les pouvoirs de collecte d'informations sur la vie des citoyens américains, le gouvernement britannique avance inexorablement dans le sens opposé : David Cameron entend faire passer sa "charte des fouineurs" [Snoopers'Act]. Ce projet de loi, rejeté lors de la dernière session parlementaire, vise à étendre les pouvoirs de surveillance de la police et des services de renseignements et à interdire le recours à des systèmes de cryptage pouvant les gêner dans leurs opérations.

Pour le grand public, c'est l'incompréhension totale. Ceux qui contestent un renforcement du pouvoir de l'Etat sont hostiles à une surveillance accrue. D'autres sont d'accord avec l'ancien ministre des Affaires étrangères William Hague, et avec le Big Brother du roman de George Orwell, pour dire que *"ceux qui n'ont rien à cacher n'ont rien à craindre"*.

Aucun démocrate digne de ce nom n'a pu ignorer les révélations d'Edward Snowden. Elles ont montré que des gouvernements se livraient à des écoutes massives sans obligation légale ou démocratique de rendre compte de leurs opérations. Ces révélations n'ont d'ailleurs pas été ignorées. Le président Obama a créé une commission qui a publié un rapport de 300 pages sur le sujet. Le Congrès a tenu des auditions publiques. Le directeur du renseignement américain, James Clapper, a reconnu que les accusations de Snowden étaient fondées. Il y a eu des démissions, 30 projets de loi pour réglementer l'Agence de sécurité nationale (NSA) et, dernièrement, une loi. Le quatrième amendement de la Constitution américaine, qui protège la propriété privée, stipule clairement, comme les journaux l'ont souligné : *"Aucun mandat ne sera délivré, sauf sur présomption sérieuse."*

La Grande-Bretagne n'arrive pas à comprendre l'importance que les Etats-Unis attachent à la confidentialité des informations. Le Parlement a réagi aux révélations de Snowden en dénonçant sa "trahison". L'an dernier, le Comité du renseignement et de la sécurité s'est incliné devant les patrons de la sécurité britanniques comme un moine novice devant un collège de cardinaux. A aucun moment il n'a contesté l'envergure de leurs opérations ou leurs méthodes. Et il n'a mené aucune discussion sur les coûts financiers. Il a fait preuve de la déférence la plus servile envers le pouvoir de l'Etat.

Pouvoirs accrus. Les services de sécurité ont manifestement besoin de pouvoirs accrus, mais ils s'y sont très mal pris pour les obtenir. L'heure n'est plus aux lettres décachetées à la vapeur ni aux écoutes téléphoniques. Pour que les autorités puissent trouver une aiguille dans une meule de foin, elles doivent avoir accès à la meule.

Mais le débat ne fait que commencer. A ma connaissance, les partisans de la sécurité considèrent la liberté civile comme l'ennemi de leur chapelle. Chez eux, le désir affirmé de collecter toujours plus d'informations l'emporte sur les vagues idées libérales de la vie privée, exceptée la leur. Toutes les informations se justifient d'elles-mêmes. Comme l'a fait observer un informateur de Snowden, *"on collecte tout parce qu'on le peut"*.

Traditionnellement, les renseignements militaires visaient à défendre le pays contre une menace existentielle. Depuis la fin de la guerre froide, et probablement bien avant, il n'y avait aucune menace de ce genre en Grande-Bretagne, et c'est pourquoi le lobby de la sécurité nationale s'est jeté avec autant d'empressement dans ce que [l'ancien Premier ministre] Tony Blair appelait *"la guerre contre le terrorisme"*. Mais le terrorisme ne représente pas une menace pour la sécurité de l'Etat, hormis pour des esprits délirants. Il représente un risque criminel. Il est dangereux de prétendre qu'un acte terroriste est un acte de guerre, car on octroie au meurtrier le statut auquel il aspire : celui du soldat qui combat une grande puissance. Avec une bombe à fragmentation et un fusil, il entend menacer un pays tout entier. Et il n'est pas le seul. Blanchisseurs d'argent, trafiquants de drogue et pédophiles font figure eux aussi de terroristes dans la démonologie de la paranoïa d'Etat.

Selon des observations empiriques, la collecte d'informations ne joue qu'un rôle mineur dans la protection de l'Etat. Même dans le domaine du terrorisme, la commission Obama a trouvé peu de preuves indiquant que les banques de données avaient directement amélioré la sécurité nationale.

Les partisans de la sécurité considèrent la liberté civile comme l'ennemi de leur chapelle

Une collecte d'informations dangereuse et peu fiable

Presque tous les actes terroristes, des attentats à la bombe du marathon de Boston [le 15 avril 2013] à l'assassinat de Lee Rigby [soldat britannique tué à la machette le 22 mai 2013], sont commis par des personnes connues des services de police, et donc au sein du système de surveillance en place. Les forces armées occidentales perdent guerre après guerre contre des hommes armés de kalachnikovs et de bombes artisanales.

Pour arrêter des criminels, une surveillance s'impose, mais la collecte d'informations – autorisée ou non – par l'Etat et par des entreprises privées est à la fois dangereuse pour les citoyens et peu fiable. On sait qu'un membre du gouvernement a mis sur écoute des avocats et des contacts de journalistes. Le NHS [système d'assurance-maladie] vend des dossiers médicaux à des entreprises pharmaceutiques. Le fisc perd des fichiers et la police transmet des documents à la presse. Comme Snowden en a apporté la preuve, l'Etat espion est indiscipliné et chaotique.

De même qu'il n'existe pas de droit à une liberté sans entraves, il n'existe pas non plus de droit à une ingérence incontrôlée de l'Etat. Je ne souhaite pas que mes mouvements, mes contacts et mes conversations soient suivis quotidiennement par une taupe algorithmique ni que ces informations soient ensuite vendues ou révélées à un "collecteur" du web. Je ne veux pas me retrouver sans raison valable sur une liste noire, comme cela se produit aux Etats-Unis.

D'où l'importance d'associer un débat transparent et éclairé à un protocole de surveillance international. Mais à la base il y a un principe constitutionnel très simple à respecter : un mandat d'ingérence, comme un mandat d'arrêt, ne peut être délivré que pour une raison valable et ne peut être autorisé que par une instance indépendante. Notre liberté, comme l'a souligné le président Obama l'an dernier, *"ne peut être tributaire des bonnes intentions de ceux qui sont au pouvoir ; elle est tributaire de la loi"*. Les Américains comprennent ce principe. Pas les Britanniques. Pauvres de nous !

—Simon Jenkins
Publié le 3 juin

Canada

LE POUVOIR MISE SUR LA PEUR

A quelques mois des législatives, prévues en novembre, le gouvernement conservateur de Stephen Harper a fait voter un projet de loi antiterroriste controversé, qui étend notamment les pouvoirs des services de renseignements. *"Les mesures drastiques du projet constituent une atteinte injustifiée aux droits des Canadiens"*, a estimé le quotidien The Globe and Mail. Annoncé juste après la fusillade du Parlement d'Ottawa, en octobre dernier, ce projet adopté par le Sénat le 9 juin confirme que les conservateurs *"jouent clairement la carte de la sécurité et du terrorisme"*, comme l'a déclaré au Financial Times l'ancien vice-Premier ministre John Manley.

LA NSA TOUJOURS PUISSANTE

Deux ans après les révélations d'Edward Snowden, le Congrès américain a mis fin à la collecte de données téléphoniques par l'agence de renseignements. Mais celle-ci garde l'essentiel de ses prérogatives.

—Financial Times *(extraits)Londres*

Le vote d'une loi qui pour la première fois depuis le 11 septembre 2001 va restreindre la surveillance du gouvernement représente un revirement spectaculaire sur le plan politique, mais ne bridera guère les activités du renseignement américain. Le Freedom Act, voté à une large majorité par le Sénat et la Chambre des représentants, interdit désormais au gouvernement de collecter les données téléphoniques de millions de citoyens américains, un programme de surveillance qui avait cristallisé les inquiétudes de l'opinion à propos des excès de l'espionnage électronique. Mais la réforme actuelle laisse tout de même aux services de renseignements américains des outils et des pouvoirs juridiques colossaux pour collecter des données et autres informations sur Internet dans le cadre d'enquêtes contre le terrorisme.

La toute première révélation d'Edward Snowden concernait un mandat d'une cour de justice secrète demandant à [l'opérateur de téléphonie mobile] Verizon de fournir à la NSA les données concernant les appels de ses clients. L'opinion publique a ainsi découvert que le gouvernement faisait main basse sur des informations qui concernaient des dizaines de millions d'Américains. C'est ce programme qui, dans la masse des documents fournis par Snowden, a mis le feu aux poudres et déclenché un scandale aux Etats-Unis. Le gouvernement était accusé de violer le droit à la vie privée sous prétexte de détecter les menaces terroristes.

Le Freedom Act a été conçu pour répondre à ces inquiétudes. La nouvelle loi demande aux opérateurs téléphoniques et non plus au gouvernement de stocker ces informations, et il faut un mandat spécifique pour lancer une recherche dans ces données.

Le vote de cette loi est un tournant politique majeur en matière de sécurité nationale. Avant les révélations de Snowden, le climat politique autour du terrorisme était tel que le renouvellement des dispositions du Patriot Act de 2001, désormais remplacées par le Freedom Act, aurait été une opération de routine.

Mais en réalité, depuis les dix-huit derniers mois, le gouvernement a opéré une retraite tactique en prenant ses distances avec ce programme de collecte de données téléphoniques. Un comité de spécialistes nommés par la Maison-Blanche a déclaré en décembre 2013 que le programme n'était *"pas indispensable"* dans la prévention des attentats. Et début 2014 le président Obama s'est prononcé en faveur de nombreux changements contenus dans la nouvelle législation. *"On peut s'en accommoder"*, explique un ancien responsable des services secrets qui a participé à l'élaboration de cette loi. Même les plus fervents partisans de la nouvelle législation reconnaissent que les services secrets ont toujours les coudées franches pour espionner leurs concitoyens.

Excès. *"Nous nous sommes attaqués aux excès mis au jour par les toutes premières révélations de Snowden, et je m'en félicite,* déclare Julian Sanchez, du [think tank libertarien] Cato Institute à Washington. *Mais il reste encore du travail. Ce n'est qu'une toute petite partie de la surveillance conduite par la NSA."*

La plupart des données numériques collectées par la NSA viennent en effet de l'étranger [ou de communications impliquant des ressortissants étrangers], et cette surveillance est autorisée par des dispositions légales qui n'ont pas été amendées par le Freedom Act. Il s'agit en particulier de la section 702 de la loi Fisa [une loi sur la surveillance et le renseignement étranger, qui permet notamment à la NSA d'accéder aux serveurs des entreprises du secteur des technologies] et du décret 12333, qui remonte à l'ère Reagan [et régit l'interception de communications hors du territoire américain].

Reste à savoir si le vote du Sénat sera l'apogée des efforts consentis par l'exécutif ou s'il ne s'agit que du début d'une plus vaste offensive contre les pouvoirs du renseignement. Les entreprises technologiques américaines, qui ont des millions de clients à l'étranger, réclament de nouvelles restrictions sur la collecte des données à l'international. Le prochain bras de fer aura peut-être lieu en 2017, à l'expiration de la section 702 de la loi Fisa.

—Geoff Dyer
Publié le 3 juin

↑ *Dessin de* **Beppe Giacobbe,** *Italie.*

Contexte

Le Freedom Act (Loi pour la liberté) confie aux opérateurs téléphoniques le stockage des métadonnées (heure, durée et numéro de l'appel). Il a été voté le 2 juin après l'expiration de la section 215 du Patriot Act, la loi antiterroriste de 2001. C'est sur cette section que reposait la collecte des données par la NSA. L'USA Patriot Act est en fait un acronyme qui signifie "Unir et renforcer l'Amérique en fournissant les outils appropriés pour intercepter le terrorisme et y faire obstacle". L'USA Freedom Act est aussi un acronyme. On peut le traduire par "Unir et renforcer l'Amérique en respectant les droits et en mettant fin à l'espionnage, à la collecte massive et à la surveillance électronique".

On a tous des choses à cacher

L'argument est souvent avancé par ses partisans : il n'y a rien à craindre de la surveillance numérique si on n'a rien à cacher. Faux ! écrivaient dès 2013 des journalistes néerlandais. Onze raisons de ne pas se résigner.

—De Correspondent *Amsterdam*

1. Je cache, donc je suis

La vie privée est presque toujours considérée comme une notion juridique, alors qu'elle est avant tout une caractéristique humaine. Nous gardons pour nous la majorité de nos pensées, de nos sentiments et de nos expériences. Le caractère privé de notre conscience intérieure est une condition déterminante du "je". Dire *"je n'ai rien à cacher"* revient donc à dire *"ma conscience intérieure n'a rien à cacher"*. Un excellent exemple de contradiction en termes philosophiques.

2. Les relations sociales nécessitent que l'on cache certaines choses

Chaque être humain montre une personnalité différente en fonction du contexte, du moment, et des personnes qui l'entourent. Ceux qui disent *"je n'ai rien à cacher"* oublient cette réalité sociale. Dans un contexte social, tout le monde a des choses à cacher. Au travail, il peut s'agir du caractère colérique qui ressort parfois en présence de son conjoint, qui n'a par contre jamais vu le masque de séducteur que l'on revêt devant des inconnus.

3. On cache déjà des choses sans s'en rendre compte

Cacher des choses est devenu tellement naturel qu'on le fait sans réfléchir. Nous cachons notre corps, nos défauts, nos courriels, notre fiche de paie, etc. Ceux qui affirment *"ne rien avoir à cacher"* passent outre à cette réalité.

4. L'interdit dépend du contexte

Dans notre pays l'adultère n'est pas interdit par la loi, mais en Arabie Saoudite il est passible de la peine de mort. La question de savoir si quelque chose est interdit (et s'il vaut mieux le cacher) dépend donc du contexte. Autre exemple : imaginez une photo où vous êtes ivre avec une strip-teaseuse sur les genoux pendant un enterrement de vie de garçon. Elle ne montre pas un "interdit" en soi, jusqu'à ce que votre patron, très soucieux de l'image de son entreprise, en prenne connaissance. Et, quant à votre homosexualité, qui n'intéresse personne [aux Pays-Bas], elle peut vous causer des ennuis devant la douane russe. Bref, on ne peut jamais être sûr de ne pas enfreindre un "interdit".

5. Les interdits évoluent

Dans les années 1970, des voix s'élevaient publiquement pour demander le droit d'avoir des relations sexuelles avec des enfants. Aujourd'hui, ces mêmes personnes seraient inculpées. On peut donc penser ne rien faire d'"interdit" (et donc ne rien avoir à cacher) alors que nos actions pourraient nous causer de gros ennuis ultérieurement.

6. Tout le monde enfreint les interdits

Différentes études ont montré que l'homme cache la vérité (donc qu'il ment) 1,5 à 4 fois par jour. La plupart du temps pour ne pas perdre la face, éviter les confrontations, rejeter la responsabilité sur un autre, obtenir ce qu'il souhaite, se montrer sous un jour meilleur et (peut-être la raison la plus importante) pour être jugé sympathique. Comme l'a écrit l'auteur irlandais du XVIIIe siècle Oliver Goldsmith : "*"Ne me posez pas de questions, je n'aurai pas à vous mentir."*

7. Des faits et gestes mal interprétés

Imaginons que vous êtes journaliste et que vous voulez écrire un article sur les jeunes Néerlandais qui vont faire le djihad en Syrie. Après de nombreuses recherches sur Internet, vous avez trouvé plusieurs numéros de téléphone et adresses mél pour faire des interviews. Une fois l'article terminé, vous voulez aller en vacances à New York et ne prenez qu'un aller simple parce que vous ne savez pas combien de temps vous voudrez y rester. Avant de partir, vous réalisez que vous et votre petite amie venez d'acheter ensemble votre première maison et qu'elle se retrouverait avec des mensualités trop lourdes s'il vous arrivait quelque chose. Vous prenez donc une assurance-vie juste avant votre départ. Vous avez donc les numéros de plusieurs djihadistes dans votre téléphone, vous avez acheté un aller simple pour New York et vous venez de contracter une assurance-vie. La NSA ne risque-t-elle pas de trouver votre voyage suspect ? Qu'est-ce qui garantit que ses algorithmes de recherche ou les personnes qui les interprètent ne tireront pas de mauvaises conclusions vous concernant ?

8. On n'a pas en tête toutes les lois

Sur son blog ThoughtCrime.org , l'expert en cybersécurité américain Matthew Rosenfeld (pseudonyme : Moxie Marlinspike) explique qu'aux Etats-Unis il existe tellement d'actes punissables que même les pouvoirs publics (et donc a priori les citoyens) n'en connaissent pas le nombre exact. Quant aux Pays-Bas, il y existe environ 11 000 lois et règles, et 140 000 articles annexes. Il est donc impossible de savoir si on n'enfreint pas par hasard telle ou telle loi.

9. On ne peut pas faire confiance aux pouvoirs publics

Plusieurs fois déjà, les pouvoirs publics néerlandais se sont révélés incapables de bien protéger les données personnelles des citoyens. Quasiment tous les grands projets informatiques de ces dernières années (comme le dossier médical électronique, le vote en ligne ou la carte de transports publics) avaient des failles techniques mettant en danger la sécurité des données. Certes, nous n'avons probablement rien à cacher à l'organisme auquel nous donnons nos informations personnelles, mais cela pose un problème dès lors que d'autres parties ont potentiellement accès à ces données.

10. Les pouvoirs publics font des erreurs

Les exemples ne manquent pas. Prenons l'homme d'affaires néerlandais Ron Kowsoleea. Il a été victime de données mal enregistrées dans les bases de données de différents services de recherche néerlandais pendant plus de quinze ans. Kowsoleea a été arrêté et inculpé plusieurs fois parce que quelqu'un d'autre commettait des délits sous son nom et que les pouvoirs publics néerlandais n'étaient pas capables de corriger les erreurs. Autre exemple : des centaines de travailleurs indépendants ont atterri sur une liste de fraudeurs aux allocations à cause d'un problème informatique. Ils ont été condamnés et ont dû payer de fortes amendes. Et que penser du tragique suicide du [membre de l'opposition russe] Alexander Dolmatov [en janvier 2013, dans un centre de détention pour les personnes déboutées du droit d'asile à Rotterdam] ? A cause d'une erreur du système informatique du service d'immigration, alors qu'il devait être expulsé, il a été placé en détention et a fini par se pendre.

11. Quid de nos futurs dirigeants ?

Si certaines données ont déjà été collectées pour une raison x, pourquoi ne pas les utiliser pour une raison y ? Les spécialistes appellent cela le détournement d'usage. Prenons par exemple les empreintes digitales enregistrées sur les passeports de l'Union européenne. A la base, cette mesure de Bruxelles avait pour but de prévenir l'usurpation d'identité, mais aujourd'hui les empreintes digitales sont également utilisées pour des enquêtes judiciaires. Certes, aujourd'hui, les autorités néerlandaises ne s'y intéressent pas, mais il est naïf de croire qu'il pourrait en être autrement dans l'avenir. Nous ne savons pas encore qui seront les futurs dirigeants et quels seront leurs agendas politiques.

—Maurits Martijn et Rob Wijnberg

Publié le 21 octobre 2013