Anna Demontis, chargée de projet éditorial pour l'ACAT

TOUS SUR ÉCOUTE ?

Les avancées technologiques et législatives ont permis une surveillance accrue de nos moindres faits et gestes. Pourtant, la collecte et l'exploitation massives de nos données personnelles sont des pratiques qui portent en elles l'atteinte aux droits fondamentaux.

Pas un trimestre ne se passe sans que le monde ne découvre de nouvelles révélations du lanceur d'alerte, Edward Snowden, sur le programme de surveillance mis en place par les agences de renseignement américaines, après les attentats du 11 septembre 2001. Commission européenne, siège de l'ONU, réseaux téléphoniques, entreprises privées telles que Microsoft, Google, Facebook ou Apple… Les communications de tout le monde, ou presque, seraient passées par les oreilles de la NSA et de la CIA. Un scenarii de science-fiction qui a dévoilé au monde le potentiel de surveillance offert par les évolutions technologiques.
« *Aujourd'hui, en matière de surveillance, on est capable d'intercepter les métadonnées (c'est-à-dire le contenant des communications : qui écrit à qui, quand, pendant combien de temps, depuis quel lieu et à quelle fréquence) et les données (c'est-à-dire le contenu) de ce que l'on fait ou dit sur Internet* », explique Adrienne Charmet, porte-parole et coordinatrice des campagnes de la Quadrature du Net, une association de défense des droits fondamentaux sur Internet. Lorsque nous communiquons, que nous cherchons des informations ou que nous consultons des sites, nous laissons des traces derrière nous. Ces informations, appelées « données personnelles », sont de véritables mines d'or pour qui veut espionner la terre entière.

RÉGIME DE SURVEILLANCE

« *C'est une intrusion énorme dans la vie privée des gens*, précise Adrienne Charmet. *C'est comme si on entrait dans votre cerveau.* » Un sombre dessein permis par des évolutions technologiques toujours plus poussées. Par exemple, il est aujourd'hui possible de détecter les comportements suspects sur Internet, en se basant sur l'analyse de navigation des utilisateurs. En bref, avec un simple ordinateur et des « boîtes noires » installées chez les fournisseurs d'accès à Internet (FAI), l'homme peut identifier à distance des terroristes. Dévoilés lors des débats sur la loi sur le renseignement en 2015, ces dispositifs n'ont, dans les faits, toujours pas été installés.

Il n'empêche : de là à penser que la France se dote des moyens technologiques d'une cyberdictature, il n'y a qu'un pas. Que le journalistique d'investigation Jean-Marc Manach, spécialiste d'Internet, des questions de surveillance et de vie privée, refuse de franchir : « *Nous sommes tous potentiellement écoutables et potentiellement écoutés, mais cela ne signifie pas que les services de renseignement ont comme objectif d'espionner tout le monde.* » D'ailleurs, ils n'en ont pas les moyens humains et financiers. Avec un peu plus d'un milliard de lignes de téléphone fixe, 3,7 milliards d'internautes et près de 6 milliards de téléphones portables, la tâche serait trop grande pour les 35 000 employés de la NSA ou les 5 000 salariés de la Direction générale de la sécurité extérieure (DGSE).

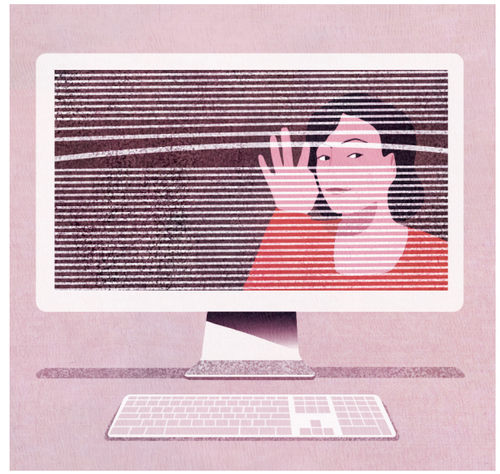
AUTOCENSURE

Il s'agit aussi de distinguer la « collecte de masse », qui consiste à intercepter et stocker les données personnelles des utilisateurs, de la « surveillance de masse », qui permet d'exploiter ces données et de les analyser dans un but précis. Tous ne sont pas d'accord sur où commence la surveillance. « *Selon La Quadrature du Net, elle se fait à partir du moment où nos données sont collectées, tandis que d'autres considèrent que la surveillance commence lorsque l'on exploite les données d'une personne* », détaille Adrienne Charmet.
Tous les moyens doivent-ils être autorisés s'ils peuvent permettre d'arrêter quelques terroristes, ou sont-ils trop intrusifs quel que soit l'enjeu et la finalité poursuivie ? Ce débat est inaudible dans l'espace public. D'une part, car la surveillance n'est pas considérée comme portant suffisamment atteinte aux droits fondamentaux. D'autre part, ses opposants doivent affronter l'argument de la lutte antiterroriste, qui apparaît comme imparable dans un contexte sécuritaire toujours plus prégnant. Cette absence de débat en dit long sur le modèle de démocratie promis par les partisans d'une surveillance accrue. D'autant qu'« *une société où le citoyen intègre le fait qu'il soit surveillable est une société qui va développer de l'autocensure* », ajoute Adrienne Charmet. « *Quand on sait qu'on est surveillé, on est tenté de se conformer à ce que l'on attend de vous*, complète Maryse Artiguelong, membre de la Ligue des droits de l'Homme (LDH) et co-animatrice de l'Observatoire des libertés et du numérique. *C'est une atteinte à la liberté d'expression, mais aussi d'information puisque vous ne pouvez plus consulter les sites qui, par exemple, publient des études sur le djihadisme.* »

PRÉSOMPTION D'INNOCENCE

La lutte antiterroriste incite également à remonter toujours plus haut dans la prévention du crime, ce qui pousse à toujours plus de surveillance. « *Dans les années 1980, vous étiez terroriste parce que vous aviez commis un acte terroriste ou parce qu'on avait la preuve que vous en prépariez un*, développe Adrienne Charmet. *Avec la loi antiterroriste de 2014, vous pouviez être inculpé pour entreprise individuelle terroriste parce que vous remplissiez une série de critères comme savoir piloter un avion ou avoir des produits chimiques chez vous. Aujourd'hui, on en est au délit de consultation de site faisant l'apologie du terrorisme, sans qu'aucune preuve matérielle ne soit nécessaire.* » S'ajoute le dessaisissement du juge judiciaire vers le juge administratif qui a été formalisé par l'État d'urgence. Plus besoin de l'aval de la justice pour bloquer un site internet, effectuer une perquisition ou assigner quelqu'un à résidence. La police agit d'abord, le citoyen dépose un recours après.
« *Le problème pour notre démocratie c'est* Minority Report *ou* Le Procès *de Kafka : le fait qu'un jour votre nom va apparaître dans un fichier et que vous devrez démontrer votre innocence* », développe Jean-Marc Manach. Cette inversion de la charge de la preuve est dommageable dans un État de droit où la présomption d'innocence prévaut. Elle peut également mener à des situations dramatiques pour les personnes visées par les opérations policières. « *Avec l'État d'urgence, certaines personnes ont vu leur vie chamboulée par les assignations à résidence ou les perquisitions administratives* », précise Maryse Artiguelong. Même sous couvert de lutte antiterroriste, difficile de justifier de telles atteintes aux droits fondamentaux. Surtout quand on sait que l'État ne pourra jamais garantir une sécurité absolue. •

Pour aller plus loin
La vie privée, un problème de vieux con ?
Jean-Marc Manach.



LA VIE PRIVÉE EST UN DROIT

Protégé par la Convention européenne des droits de l'homme (CEDH), le droit au respect de la vie privée est fondamental. « *Sans vie privée, on n'a plus la sécurité nécessaire pour créer, s'informer, s'exprimer* », selon Adrienne Charmet. L'impératif de protéger nos données personnelles en est donc le corollaire. Internet est en outre un outil incontournable pour s'exprimer et s'informer, qui doit être préservé. Enfin, si nos démocraties offrent des garde-fous aux dérives de la surveillance, qu'en est-il des activistes et défenseurs des droits qui agissent dans les pays autoritaires, voire dictatoriaux ? En étudiant leurs données personnelles, les États ont accès à leurs communications, ils peuvent même les identifier et les géolocaliser. D'où l'intérêt, pour ces activistes, d'être vigilants quant à la surveillance dont ils peuvent faire l'objet et aux informations qu'ils laissent derrière eux.

SURVEILLANCE : L'EMPILEMENT DE LOIS SÉCURITAIRES

2012
Après les attentats commis par Mohamed Merah, la loi relative à la sécurité et à la lutte contre le terrorisme est votée par le Parlement. Elle prolonge la disposition temporaire votée en 2005 sur la surveillance des données de connexion dans un but préventif. Elle modifie aussi le code pénal afin de poursuivre les ressortissants étrangers suspectés ou auteurs d'actes terroristes à l'étranger.

2014
La loi renforçant les dispositions relatives à la lutte contre le terrorisme est adoptée. Elle autorise notamment le blocage de sites Internet incitant à commettre des actes de terrorisme ou en faisant l'apologie.

2015
La loi sur le renseignement est adoptée après les attentats de Charlie Hebdo. Elle « *définit un cadre dans lequel les services de renseignement sont autorisés à recourir à des techniques d'accès à l'information* ». En bref, plusieurs techniques de recueil de données, jusque-là permises dans un cadre judiciaire, ont été étendues aux services de renseignement.

2016
Adoption de la loi visant à renforcer « *la lutte contre le crime organisé, le terrorisme et leur financement* ». Ce texte créé notamment le délit de consultation de site Internet faisant l'apologie du terrorisme. Décriée par la gauche lorsque Nicolas Sarkozy était président de la République, cette mesure est alors remise au goût du jour par le gouvernement de Manuel Valls.