La fin de la vie privée : logiciels mouchards, métadonnées, réseaux sociaux et profilage – Comment l'État français nous surveille

lundi 4 mai 2015, par KNAEBEL Rachel (Date de rédaction antérieure : 2 février 2015).

La France suit-elle le même chemin que les États-Unis, et sa National Security Agency (NSA), en matière d'espionnage généralisé des citoyens ? Quelques jours après les attaques des 7 et 9 janvier, Manuel Valls annonce de nouvelles mesures pour mieux surveiller Internet. Une loi sur le renseignement, déjà prévue avant les attentats, sera votée dans les prochains mois. Elle vient renforcer la nouvelle loi antiterroriste votée en novembre 2014, ainsi que la loi de programmation militaire adoptée un an plus tôt et la loi sur la sécurité intérieure (Loppsi 2) de 2011. Tous ces textes élargissent progressivement les possibilités de surveillance d'Internet. Et ce en dehors du contrôle judiciaire et quel que soit le profil des citoyens. Qui communique avec qui ? Quand ? Et de quel endroit... Nous sommes désormais tous sous surveillance.

Depuis les attentats de Paris, le gouvernement veut légiférer au plus vite sur le renseignement. Un projet de loi était déjà dans les cartons. Il doit maintenant être accéléré, pour une discussion au Parlement dès mars. Avec, dans le viseur, le net et les réseaux sociaux, « plus que jamais utilisés pour l'embrigadement, la mise en contact et l'acquisition de techniques permettant de passer à l'acte » terroriste, selon Manuel Valls.

La France dispose pourtant déjà d'un arsenal conséquent en ce qui concerne la surveillance d'Internet. Les données de communications électroniques sont systématiquement conservées pendant un an par les fournisseurs d'accès à internet. Et ce depuis un décret de 2006. Les fournisseurs d'accès doivent mettre à disposition : les informations permettant d'identifier l'utilisateur et le destinataire de la communication, les données concernant les équipements utilisés, la date, l'horaire et la durée de chaque communication [1]. Ces données sont conservées pour tout le monde, pas seulement pour les personnes qui font l'objet d'une enquête ou d'une surveillance particulière.

La mesure n'a jamais fait l'objet d'un véritable débat parlementaire, puisqu'elle a été mise en place par décret. Elle est pourtant loin d'être anodine. Chez notre voisin allemand, la conservation des données de communication électronique, jugée anti-constitutionnelle, est interdite au delà de quelques jours. Cette surveillance est rejetée par une majorité du monde politique. L'actuel ministre de la Justice allemand, le social-démocrate Heiko Maas, a même réaffirmé ce refus après les attentats des 7 et 9 janvier. Avec l'argument qu'en France, cela n'avait pas empêché ces attaques... En France au contraire, les lois se succèdent, qui viennent renforcer année après année l'arsenal juridique pour une surveillance de plus en plus rapprochée des citoyens – et pas seulement des terroristes ou criminels présumés.

2011 : captation des données informatiques et logiciels mouchards

En 2011, la loi d'orientation et de programmation pour la performance de la sécurité intérieure, dite Loppsi 2, légalise l'espionnage des ordinateurs privés par l'intermédiaire de logiciels mouchards. Le législateur appelle cela la « captation des données informatiques ». Cette loi autorise la mise en place de dispositifs qui permettent, sans le consentement des personnes concernées, d'accéder *« à des données informatiques, de les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur »*.

Avec de tels dispositifs, les enquêteurs peuvent voir et enregistrer en temps réel, à distance, tout ce qui se passe sur un ordinateur. La Loppsi 2 limitait toutefois cette surveillance informatique au seul cadre d'une procédure judiciaire. C'est le juge d'instruction qui peut décider de poser un logiciel mouchard, pas les services de renseignement [2].

2013 : loi de programmation militaire et métadonnées

Avec la loi de programmation militaire (LPM) adoptée en décembre 2013, ce verrou a sauté. L'article 20 (auparavant article 13) de cette loi autorise toute une série d'agences de l'État à accéder directement, non pas au contenu d'un ordinateur ou des communications, mais aux données de connexions des internautes et aux relevés détaillés des communications téléphoniques. Il s'agit-là d'un accès dit administratif, qui se pratique donc sans passer par un juge et peut se faire hors d'une procédure judiciaire.

Cet article est en vigueur depuis le 1er janvier 2015, suite à la publication de son décret d'application à la veille de Noël. Ce qui est visé par cette surveillance : les métadonnées. C'est-à-dire non pas le contenu des communications mais les données sur ces communications – qui appelle ou écrit à qui, à quelle heure, quels sites sont visités par qui, quand. Ainsi que la géolocalisation, en temps réel, des utilisateurs.

2013 : extension de la surveillance en dehors des procédures judiciaires

La formulation utilisée par la loi de programmation militaire est assez floue pour laisser penser que l'éventail des données recueillies ira plus loin encore. La Commission nationale de l'informatique et des libertés (Cnil) souligne ainsi en 2013, que le recours dans la loi à la notion vague « d'informations et documents » « semble permettre aux services de renseignement d'avoir accès aux données de contenu, et non pas seulement aux données de connexion ».

Par ailleurs, ces données pourront être demandées par toute une série de services de renseignement. Avec son article 20, la loi de programmation militaire pérennise un dispositif de surveillance des données déjà en place depuis 2006. Mais celui-ci était alors limité à la lutte contre le terrorisme. Avec la LPM, l'accès aux données peut maintenant se faire « au titre de la sécurité nationale, de la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France ou de la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous ». En plus de l'unité de coordination de la lutte anti-terroriste et de différents services de police et de renseignements, d'autres services sont ainsi autorisés à accéder à ces informations, comme l'Office central pour la répression de l'immigration irrégulière et de l'emploi d'étrangers sans titre. Ou des services dépendant du ministère des Finances, comme les douanes et Tracfin, qui s'occupe notamment d'évasion fiscale [3]. Et cela, encore une fois, en dehors de procédures judiciaires.

Des garde-fous insuffisants

Dans une délibération du 4 décembre 2014, la Cnil attire *« l'attention du gouvernement sur les risques (…) pour la vie privée et la protection des données à caractère personnel ». Les données*

détenues par les opérateurs qui peuvent être demandées « sont de plus en plus nombreuses, sont accessibles à un nombre de plus en plus important d'organismes, sur réquisitions judiciaires ou administratives ou en exécution d'un droit de communication, et ce pour des finalités très différentes », pointe la Cnil.

Il existe tout de même quelques garde-fous. Une personnalité qualifiée placée auprès du Premier ministre est chargée d'autoriser le recueil de ces informations. Et la Commission nationale de contrôle des interceptions de sécurité (CNCIS), mise en place en 1991, veille à la légalité des écoutes téléphoniques, en les contrôlant a posteriori. Mais cette commission ne dispose que de peu de moyens : six postes seulement et un budget en baisse entre 2011 et 2013. Elle fonctionne à effectifs constants *« depuis sa création il y a près d'un quart de siècle »*, alors que ses missions se sont pourtant *« considérablement accrues au fil des années »*, déplore la CNCIS dans son dernier rapport d'activité.

2014 : délit d'apologie de terrorisme et blocage de sites web

Depuis les attaques contre *Charlie Hebdo* et au supermarché casher de Vincennes, des dizaines de personnes ont été arrêtées pour apologie du terrorisme. Cette multiplication des procédures et l'application de lourdes peines découlent de la dernière loi antiterroriste, adoptée il y a à peine deux mois. Qui prévoit jusqu'à cinq ans d'emprisonnement et 75 000 euros d'amende en cas d'apologie du terrorisme.

Cette loi de novembre 2014 alourdit également la peine maximale quand le délit est commis sur internet. La peine encourue est de sept ans d'emprisonnement et 100 000 euros d'amende *« lorsque les faits ont été commis en utilisant un service de communication au public en ligne ». « Pour un message Facebook faisant l'apologie du terrorisme, vous risquez deux ans de prison en plus que si vous dites la même chose dans la rue »*, résume Adrienne Charmet, coordinatrice des campagnes à la Quadrature du net, association de défense des droits et libertés des citoyens sur Internet. Un différentiel inédit selon elle.

La même loi autorise aussi le blocage administratif – c'est-à-dire sans décision judiciaire – des sites internet *« provoquant à des actes terroriste ou en faisant l'apologie »*. Cette mesure attend encore son décret d'application, qui va arriver très vite, a promis Manuel Valls. La loi a été critiquée par le Conseil national du numérique, un organisme consultatif indépendant. Celui-ci juge qu'*« en minimisant le rôle de l'autorité judiciaire, (le dispositif) n'offre pas de garanties suffisantes en matière de libertés »*.

2015 : surveiller les conversations sur Skype

Elle était prévue pour juillet 2015. Mais suite aux attentats, le Premier ministre veut en accélérer l'adoption. La future loi sur le renseignement sera discutée dès mars. Manuel Valls promet un texte protecteur des libertés publiques, mais qui vise à renforcer *« la surveillance des communications et de l'Internet des jihadistes ». « Nous voulons avoir accès aux ordinateurs »*, déclare le député Jean-Jacques Urvoas, président de la commission des lois, sur Europe 1, le 14 janvier.

Objectif de la loi : pouvoir surveiller par exemple ce qui s'échange via le logiciel de communication Skype. Ce qui peut apparaitre a priori comme un simple ajustement juridique face à l'évolution des technologies de communication. Mais la loi sur le renseignement *« augmente le périmètre de surveillance avec la capacité de récolter des renseignements non seulement sur une personne, mais aussi sur tout son réseau, alerte Adrienne Charmet. C'est vraiment la logique de la NSA. C'est ce type de législation qui est envisagée. »*

« Le profilage absolu » via les métadonnées

La stratégie des dernières lois françaises ressemble à celle de l'Agence nationale de la sécurité états-unienne sur au moins un aspect : viser un ramassage toujours plus large des métadonnées. Ce serait un moindre mal pour la vie privée, arguent les promoteurs de ces lois. *« La réquisition de ces données constitue une démarche beaucoup moins intrusive pour la vie privée que la pratique des écoutes téléphoniques »*, avancent ainsi les députés Jean-Jacques Urvoas et Patrice Verchère dans un rapport d'information sur l'accès aux métadonnées de connexions, en 2013.

« Les métadonnées, c'est le profilage absolu, analyse au contraire Adrienne Charmet. *Avec les métadonnées, plus besoin d'avoir le contenu des communications. Si on a les métadonnées, on peut reconstruire tout le réseau d'une personne, ses déplacements, son rythme de vie. »* Est-ce vraiment moins attentatoire à la vie privée de suivre à la trace les déplacements, les contacts et les activités de quelqu'un que de surveiller le contenu de ses échanges ? *« Quoique moins intrusive dans le secret des correspondances, cette mesure porte atteinte à d'autres droits des citoyens, comme le droit à l'intimité de la vie privée et à la liberté d'aller et venir »*, souligne la Commission nationale de contrôle des interceptions de sécurité [4].

Tout savoir sur nos réseaux et contacts

« Ce qui constitue la vraie nouveauté, l'information principale du programme Prism (de la NSA, ndlr) et de ses suites, c'est que l'information recherchée n'est pas ce que nous disons, mais à qui nous le disons. Le contenu de nos conversations reste intéressant bien sûr (surtout pour les entreprises qui ont intérêt à tout savoir de nos vies), mais pas tellement pour les États. Ce que veulent les États, c'est tout savoir de nos réseaux », analyse l'activiste du net Laurent Chemla sur son blog, le 6 janvier. *« Ce sont nos metadatas qu'ils stockent, pour ensuite pouvoir, quand bon leur semble, décider qui surveiller plus spécifiquement. »*

Poussée à bout, cette logique de profilage par l'intermédiaire de notre réseau de contacts et de nos déplacements, peut aboutir à un ciblage au sens littéral du terme. Les « signature strikes » du programme états-unien d'assassinats ciblés de terroristes, à l'aide de drones armés en Afghanistan, Yémen et Pakistan, en est un exemple. Lors de ces tirs, les drones visent des cibles non pas parce que les services de renseignements savent que ces personnes sont des « terroristes », mais parce que le profil de leurs déplacements, de leurs réseaux, de leur rythme de vie, sont ceux de terroristes. Le contrôle des métadonnées ouvre ainsi la porte à de dangereuses dérives. Nous voici pourtant désormais surveillés en permanence, soumis à un « profilage » de tous les instants.

Rachel Knaebel

P.-S.

* Basta ! : http://www.bastamag.net/Logiciels-mouchards-metadonnees-reseaux-sociaux-et-profilage-comment-l-Etat

---

Notes

[1] « Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales », les fournisseurs d'accès à Internet doivent mettre à disposition « les informations permettant d'identifier l'utilisateur ; les données relatives aux équipements terminaux de communication utilisés ; les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ; les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ; les données permettant d'identifier le ou les destinataires de la communication. »

[2] La Loppsi 2 mettait aussi en place l'obligation pour les fournisseurs d'accès de bloquer les images pédopornographiques sur des sites notifiés par le ministère de l'Intérieur.

[3] Traitement du renseignement et action contre les circuits financiers clandestins.

[4] Dans son dernier rapport d'activité.