Entre terrorisme et surveillance de masse, quelle place pour les citoyens ?

L’arsenal déployé pour surveiller les Français s’étoffe d’année en année. Mais quels sont les risques de ce gardiennage de masse pour l’avenir de notre démocratie ?

Temps de lecture : minute

13 juillet 2018

La France, toujours le pays des droits de l’Homme ? La question mérite d’être posée, alors que les tragiques événements terroristes perpétrés sur notre territoire ces dernières années ont poussé pouvoirs publics et entreprises privées à instaurer une vigilance maximale en matière de cybersécurité, au détriment, parfois, de la protection de la vie privée et des libertés des citoyens.

Si la Convention européenne des droits de l'homme assure la protection de la vie privée et la garantie de la liberté d'expression, il semble en effet aujourd’hui compliqué de concilier ces acquis avec la nécessité d’assurer la sécurité publique. Dès le début du mandat de François Hollande, en 2012, le code pénal et les outils de surveillance à disposition de l’administration se sont vus renforcés en réaction aux tueries perpétrées par Mohamed Merah. Trois ans plus tard et à la suite des attentats terroristes de Paris en janvier 2015, la loi sur le renseignement était annoncée pour permettre aux services secrets du pays d'espionner les communications numériques et mobiles de toute personne liée à une enquête terroriste. Les fournisseurs de services internet et téléphoniques, de leur côté, apprenaient qu’ils seraient forcés d'installer des “boîtes noires” par les services de renseignements. Celles-ci, reposant sur

l'utilisation d'un algorithme capable d’analyser les données de communications de particuliers (destinataire d’un message, heure et lieu de l’envoi, etc.), doivent permettre de détecter des connexions susceptibles de révéler une menace terroriste. Une première a officiellement été activée en novembre 2017.

Un encadrement légitime ?

Autant d’évolutions qui poussent les militants des droits de l'Homme et de la vie privée, ainsi que les Nations Unies, à tirer la sonnette d’alarme. La Loi sur le Renseignement notamment, décrite comme ouvrant la voie à une surveillance intrusive et à un piratage informatique, amenait ainsi le comité des droits de l'Homme des Nations Unies à avertir au travers d’un communiqué sur le caractère "excessivement large" des pouvoirs de surveillance accordés aux services de renseignement français *“sur la base d'objectifs vastes et mal définis”*. Amnesty International, de son côté, estimait que l'État français se donnait “*des pouvoirs extrêmement importants et intrusifs”* sans

aucun contrôle judiciaire.

Interrogé dans le cadre d'une table ronde organisée par Le Monde en France (Juin 2014), le journaliste Glenn Greenwald (qui publiait en 2013 les révélations d'Edward Snowden sur les programmes de surveillance de la NSA) l'assure : la surveillance n'est pas la clé de la lutte contre le terrorisme. "*La NSA, qui coûte 15 milliards de dollars par an aux contribuables américains, n'a pu prévoir l'attentat des frères Tsarnaev à Boston en avril 2013 alors que les deux hommes affichaient clairement leurs objectifs sur les réseaux sociaux.*"

Une opinion partagée par le juge antiterroriste Marc Trévidic, pour lequel il *"ne sert à rien de noyer la justice sous des tonnes d'informations inutiles". "Il y a beaucoup de monde qui parle de "bombes" ou de "Palestine" dans les conversations et les emails. Il faut cibler les gens vraiment dangereux pour en tirer des informations précises"*, explique-t-il.

Et les citoyens ? Si 53% d'entre-eux ne considèrent pas l'état d'urgence efficace pour lutter contre les réseaux terroristes ainsi qu'empêcher de nouvelles attaques terroristes, ils ne sont que 14% à souhaiter sa suppression (Les Français et l'état d'urgence - Ifop - Juin 2016). Des chiffres qui ne disent pas si les Français sont aujourd'hui conscients de ce que cet état d'urgence et la surveillance de masse qu'il implique peuvent avoir comme conséquences sur leur vie privée, à court et à long terme. En particulier lorsque l'on sait qu'ils sont aujourd'hui près de 20% à estimer n'avoir aucune connaissance pour protéger leurs données en ligne, et avoir besoin d'aide (Sondage sur la protection des données - Mozilla - mars 2017).

Au total, ce sont ainsi 20 282 personnes qui ont été espionnées par les services français entre le 3 octobre 2015 et le 2 octobre 2016, pour seulement 2 000 personnes soupçonnées d'être, de près ou de loin, impliquées dans des phénomènes de radicalisation religieuse violente ou

dans des filières de recrutements djihadistes.

Entre régulation et solutions alternatives

Pourtant, la Commission nationale de contrôle des techniques de renseignement l'assure : les services de renseignement bénéficient, certes, de moyens importants pour surveiller les citoyens, mais ceux-ci sont mieux encadrés. Dans son premier rapport annuel, publié en décembre 2016, celle-ci fait ainsi état de *"procédures internes rigoureuses"* liées à ses missions de surveillance, comme par exemple sur la durée de conservation des données récoltées par les Imsi-catchers, ces "valises-espionnes" qui interceptent les numéros des correspondants lors d'échanges téléphoniques, la durée de l'appel, l'heure, la date ou encore la localisation.

À côté, plusieurs produits innovants, développés en France ou non, permettent aujourd'hui aux citoyens de laisser le moins de traces possibles sur internet. "*On peut assez facilement effacer certaines traces vis-à-vis de la surveillance privée, comme celle exercée par Google, en utilisant des moteurs de recherche comme DuckDuckGo ou le navigateur anonyme Tor, en utilisant des logiciels libres comme Linux ou en utilisant une messagerie instantanée comme Signal*", expliquait Marc Meillassoux, réalisateur du documentaire *Nothing to Hide, aux Inrocks en septembre 2017, "il y a différents niveaux de protection et il n'est pas nécessaire d'aller au stade le plus extrême pour avoir une utilisation d'internet qui soit satisfaisante*".

L'Allemand Telegram, quant à lui, a su jouer sur les craintes de surveillance de masse partagées par une partie de la population, pour réunir plus de 100 millions d'utilisateurs par mois sur son application de messagerie cryptée. Prisée par la classe politique française, celle-ci l'est également par les réseaux djihadistes, lui valant une réputation mitigée. Après les attentats de novembre 2015, ses deux créateurs avaient ainsi

déclaré qu'ils ne se plieraient pas à "*des restrictions locales à la liberté d'expression*" en dévoilant les informations de leur réseau social. "*Ce sont 15 milliards de messages par jour, soit 10 millions par heure qui sont échangés*", explique Gérôme Billois, expert en sécurité pour le cabinet de conseil Wavestone, à France24. "*On peut vouloir tout regarder, mais, en moyens humains, c'est très difficile. Et cela devient ensuite une question sociétale de respect de la vie privée, avec une vraie atteinte aux libertés individuelles*", ajoute-t-il.

Pas de solution miracle

Alors comment réussir à concilier libertés fondamentales et sécurité publique, ces deux piliers de la démocratie que tout semble désormais opposer ? Si le défi semble aujourd'hui compliqué à relever, Isabelle Falque-Pierrotin, Présidente de la CNIL, plaide pour l'intégration d'une notion de garantie pour les citoyens dans les réflexions.

Celle-ci, qui insiste sur le rôle de la CNIL dans cet équilibre fragile à trouver, estime en effet indispensable de sortir d'une opposition binaire entre ces deux notions, afin d'introduire un troisième élément : les garanties pour les personnes. *"Pour être acceptable d'un point de vue juridique, éthique et social, le déplacement éventuel du curseur vers plus de sécurité doit nécessairement s'accompagner d'un renforcement des garanties qui encadrent l'action des services de sécurité"*, précise-t-elle dans une tribune publiée sur Les Échos.

Une harmonie qui passera notamment par la mise en place de dispositifs de recherche plus ciblés, et non plus massifs, mais également par l'information des citoyens à ce sujet, l'ajustement des durées de conservation des recherches effectuées, ou encore le renforcement des contrôles liés à ces dispositifs. À chacun donc, pouvoirs publics et privés en tête, de prendre ses responsabilités, malgré qu'il n'existe à ce jour, aucune science exacte ou solution miracle à cette problématique en

constante évolution.

Article écrit par Iris Maignan