

## **Big Brother est parmi nous. Quelques réflexions sur le projet de loi relatif au renseignement**

Guy DROUOT

Professeur des universités à l'Institut d'études politiques d'Aix-en-Provence

\* Sauf indication contraire, les articles cités ci-après sont ceux du Code de la sécurité intérieure (2012)

Le Conseil des ministres a adopté le projet de loi relatif au renseignement, lors de sa réunion du 19 mars 2015. Ce texte, déposé à l'Assemblée nationale, avec engagement de la procédure accélérée (article 45, al. 2 de la Constitution), sera défendu par le Premier ministre, signes de l'importance que le gouvernement entend lui attacher.

Prévue de longue date, accélérée par les attentats de Paris de janvier 2015, l'initiative avait été annoncée par Manuel Valls devant les députés dans la foulée de « l'esprit du 11 janvier ». Le projet de loi porte une marque nettement antiterroriste, même si le dispositif est prévu pour être utilisé dans la lutte contre la grande criminalité, la délinquance organisée, le blanchiment ou l'évasion fiscale.

En réalité, comme ce fut le cas pour les écoutes téléphoniques avec la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par voie électronique, le projet vient encadrer des pratiques largement utilisées dans le passé par les services et ne viserait qu'à donner un cadre légal à ces dernières. Après la réforme annoncée le 17 juin 2013 par le gouvernement, l'organigramme du renseignement, placé sous l'autorité du Premier ministre, inclut les ministres de l'Intérieur, de la Défense, le ministre en charge du Budget et des Douanes, ces derniers ayant eux-mêmes autorité sur les services spécialisés : DGSI, SDIG, DRPP, UCLAT (pour l'Intérieur), DGSE, DPSD (pour La Défense), Tracfin (pour le Budget et les Douanes). Sans compter la mystérieuse Plateforme nationale de cryptage et de décryptement (PNCD), dont la presse a rappelé l'existence clandestine.

Peut-on voir dans ce projet un *Patriot Act* à la française ? L'exécutif s'en défend. Mais les mises en garde ne se sont pas fait attendre, émanant d'une « galaxie d'opposants » que *Le Monde* classe en trois catégories : *le monde de la justice et des régulateurs* (Syndicat de la magistrature, Union syndicale des magistrats, Défenseur des droits, Ordre des avocats de Paris, CNIL, CNCIS, ainsi que des magistrats -y compris membres du pôle antiterroriste- à titre personnel), *les associations et ONG* (Amnesty international, Ligue des droits de l'homme, Reporters sans frontières, Quadrature du cercle, Human Rights Watch, Renaissance numérique, Fournisseurs d'accès associatifs), *les syndicats et groupements professionnels* (Conseil national du numérique, CGT Police, Fédération Syntec, AFDEL, Asic). À quoi on pourrait ajouter la presse nationale et même internationale, ainsi que la presse informatique en ligne (Charlie, New York Times, etc.). Outre la crainte d'un *Patriot Act*, il est reproché à l'exécutif d'exploiter un contexte dramatique pour justifier l'engagement de la procédure d'urgence, peu propice aux débats de fond. Les mises en garde portent également sur l'ampleur et la pérennité de mesures dont le caractère étendu et vague risque d'engendrer une société de surveillance de masse et un climat de suspicion généralisée. Sont vivement critiqués les moyens intrusifs de collecte mis à disposition des services. Enfin, les attaques portent sur la mise à l'écart du juge judiciaire dans la procédure et l'absence de garanties suffisantes pour les citoyens, ainsi que les menaces sur certaines professions telles que journaliste, chercheur en sciences sociales, ou lanceur d'alerte. En écho à ces inquiétudes, le président de la commission des lois, Jean-Jacques Urvoas (PS), a déposé un amendement tendant à la protection d'éventuels lanceurs d'alerte. De manière similaire à celui présenté par les écologistes, l'amendement entend mettre en place « une protection juridique à un agent des services de renseignement qui souhaiterait dénoncer la mise en œuvre illégale d'une technique de recueil du renseignement ou une surveillance abusive », en saisissant la CNCTR.

Dérive sécuritaire ou recherche objective d'un cadre législatif adapté à des menaces grandissantes ? Il n'est pas inutile d'insister sur le fait qu'un texte législatif est indispensable pour encadrer l'action des services de renseignement. Soyons clairs : sans tomber dans l'angélisme, on est en droit de s'inquiéter des dérives et des menaces qui pèsent sur les droits et libertés des citoyens. Ce projet vient s'ajouter à l'arsenal des lois antiterroristes promulguées depuis 1986 : loi 86-1020 du 9 septembre 1986 relative à la lutte contre le terrorisme, loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, loi n° 2012-1432 du 21 décembre 2012 relative à la sécurité et à la lutte contre le terrorisme et loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme. Cette inflation de textes illustre la difficulté, voire l'impossibilité de trouver un équilibre satisfaisant entre le respect des droits des citoyens et l'efficacité des services de renseignement, dès lors qu'une menace grave se précise (risques d'attentats sur l'ensemble du territoire). En d'autres termes, le juste milieu entre la sauvegarde des libertés publiques et individuelles et l'impératif sécuritaire, l'alternative étant fortement obérée par le choc traumatique causé par les attentats de janvier 2015. L'inquiétude soulevée par le projet repose essentiellement sur l'impératif d'anticipation pesant sur les services de renseignement. Comme le précise l'exposé des motifs qui reprend les idées du *Livre blanc de La Défense* de 2013, « efficace dans la neutralisation, la France doit désormais améliorer la détection. »

Un projet certes indispensable pour la sécurité nationale, mais qui ne contient pas moins des dispositions susceptibles de menacer directement les droits et libertés des citoyens (I). Un dispositif accordant des pouvoirs considérables au Premier ministre sans pour autant prévoir de garde-fous efficaces pour assurer la protection de ces droits et libertés (II).

## **I- Une menace directe pour les droits et libertés des citoyens ?**

La réaction des organisations de défense des droits de l'homme, auxquelles se sont jointes des institutions publiques, des médias, traduit l'inquiétude engendrée par un projet aux aspects tentaculaires. Les inquiétudes sont inspirées d'une part par l'octroi aux services de renseignement de missions étendues et aux contours flous, d'autre part par la légalisation de méthodes d'investigation intrusives et massives'.

- *Des missions étendues aux contours flous.*

Le texte définit les missions des services de renseignement dont la liste doit être fixée par décret. D'autres services peuvent être habilités par décret en Conseil d'État, après avis de la Commission nationale de contrôle des techniques de renseignement. Ces missions consistent en France et à l'étranger, en « la recherche, la collecte, l'exploitation et la mise à disposition du gouvernement des renseignements relatifs aux enjeux géopolitiques et stratégiques ainsi qu'aux menaces et aux risques susceptibles d'affecter la vie de la Nation. Ils contribuent à la connaissance et à l'anticipation de ces enjeux ainsi qu'à la prévention et à l'entrave de ces risques et menaces ».

L'objet de la collecte des renseignements est, selon le texte, la défense des intérêts publics (art. L. 811-3), ainsi énumérés :

- 1° La sécurité nationale ;
- 2° Les intérêts essentiels de la politique étrangère et l'exécution des engagements européens et internationaux de la France ;
- 3° Les intérêts économiques et scientifiques essentiels de la France
- 4° La prévention du terrorisme
- 5° La prévention de la reconstitution ou du maintien de groupement dissous en application de l'article L. 212-1
- 6° La prévention de la criminalité et de la délinquance organisées
- 7° La prévention des violences collectives de nature à porter gravement atteinte à la paix publique.

Un amendement adopté par la commission des lois de l'Assemblée a ajouté à cette liste la « prévention des atteintes à la forme républicaine des institutions ». Ce qui permettrait la mise en cause de mouvements monarchistes... Autre ajout, la prévention de « la prolifération des armes de destruction massive ».

Dans un communiqué mis en ligne sur son site, le Conseil national du numérique s'inquiète de « l'extension significative du périmètre de la surveillance ». En effet, au terrorisme ou à la prévention de la criminalité et la délinquance organisée, viennent s'ajouter les intérêts essentiels de la politique étrangère de la France, l'ingérence étrangère et la prévention des violences collectives, dont les contours sont trop flous, ouvrant de ce fait la voie à une interprétation extensive du texte par le Premier ministre.

- *Des méthodes d'investigation intrusives.*

Outre les méthodes classiques, les techniques nouvelles employées pour la collecte des renseignements sont aussi sophistiquées qu'intrusives. Elles se veulent une parade aux moyens employés par les terroristes et le crime organisé qui ont largement recours aux moyens électroniques. L'exemple du piratage des sites internet, page Facebook et compte Twitter de la chaîne *TV 5 Monde* en avril 2015 l'a démontré.

Seraient autorisés l'interception des correspondances privées par voie électronique, ce qui inclut le courriel, les SMS, MMS, Twitter, WhatsApp, Messenger, Skype, Google, Facebook... Toutes les données transitant sur ces plateformes sont susceptibles d'être « aspirées » dès lors qu'elles entrent dans les finalités définies à l'art. L 811-3. Cela concerne non seulement les personnes suspectes, mais également leur entourage (art. L 852-1).

Le recueil de données serait autorisé *en temps réel* sur les réseaux des opérateurs (Bouygues, Orange, Neuf, SFR, La Poste, etc.). L'administration peut ainsi obliger un opérateur à révéler une menace terroriste en levant l'anonymat à la demande du Premier ministre. Les opérateurs sont tenus d'autoriser, aux fins de contrôle, les membres et les agents de la CNCTR, dûment mandatés à cet effet par le président, à entrer dans les locaux dans lesquels sont mises en œuvre des techniques de recueil du renseignement. Ils sont également tenus de fournir à la Commission toutes les informations liées à l'opération. De plus, la géolocalisation en temps réel d'une personne, d'un véhicule, ou d'un objet sera possible et, en cas d'urgence liée à une menace imminente ou à un risque très élevé de ne pouvoir effectuer l'opération ultérieurement, cette géolocalisation pourra être effectuée sans autorisation préalable (art. L 851-6).

Les services pourront localiser les équipements terminaux (ordinateurs personnels et objets connectés), ainsi que s'introduire dans un ordinateur aux fins d'identification d'un terminal ou du n° d'abonnement. Afin de suivre les suspects à la trace, le texte autorise la localisation, la sonorisation (pose de dispositifs d'écoute) des lieux et des véhicules, la captation des images ainsi que des données informatiques (art. L 851-7). L'art. L 853-1 autorise, sous le contrôle de la CNCTR, la captation et la fixation des paroles prononcées à titre privé ou confidentiel, ainsi que des images, y compris dans un lieu privé.

Lorsque les renseignements relatifs aux finalités prévues à l'article L. 811-3 ne peuvent être recueillis par un autre moyen légalement autorisé, peuvent être expressément autorisés d'une part l'introduction dans un véhicule ou dans un lieu privé à la seule fin de mettre en place, d'utiliser ou de retirer les dispositifs techniques mentionnés aux articles L. 851-6 et L. 853-1 ; d'autre part lorsque les données informatiques sont contenues dans le système de traitement automatisé de données, l'introduction dans ce système, directement ou par l'intermédiaire d'un réseau de communications électroniques (il s'agit ni plus ni moins que de s'introduire dans l'ordinateur des gens, après avoir envahi leur domicile et leur véhicule privés). Il s'agit du seul cas de figure où le principe de subsidiarité est appliqué (art. L. 853-2).

S'agissant des techniques avancées, la Cnil pointe deux systèmes de surveillance, actuellement illégaux :

Le *Keylogger* : un logiciel permettant aux services, en s'introduisant dans un ordinateur, de lire un texte à l'instant même où l'auteur le frappe sur son clavier. Les avantages de ce logiciel sont évidents pour les services de renseignement qui, sous couvert de légitimité, agissent en violant l'intimité informatique de l'utilisateur.

L'*IMSI Catcher* : l'appareil le plus contesté par les détracteurs du projet. Il simule un relais téléphonique en s'intercalant entre l'utilisateur d'un téléphone mobile et l'antenne relais d'un opérateur. Ce dispositif léger, extrêmement coûteux (100.000 € l'unité), non conçu pour une écoute ciblée, permet au contraire une captation de toutes les conversations à l'entour. On ne manquera pas de rappeler que cet appareil avait été considéré comme dangereux par le ministre de l'Intérieur lui-même lors du vote de la loi antiterrorisme de 2014, mais qu'il revient à la faveur de ce projet. Le fait de légaliser cet appareil n'empêchera pas son utilisation par quelque officine douteuse, y compris privée...

Le Conseil du numérique voit dans ces dispositifs des techniques de surveillance de masse par algorithmes.

De tels techniques permettent la mise en place d'un dispositif de détection de *comportements significatifs des méthodes de communication des terroristes*. Une mesure destinée à déjouer un projet d'attentat sur le sol français avant qu'il ne soit commis, grâce à l'analyse en temps réel des métadonnées des communications (expéditeur, horaire, destinataire, type de message...) et non leur contenu. Un algorithme détermine alors automatiquement les « profils » ayant un comportement correspondant à des critères définis par les services de renseignement – et signalant des modes de communication propres à des réseaux terroristes. En cas d'imminence suspectée d'une attaque, l'anonymat (déjà relatif) de ces communications pourrait alors être levé.

Ces dispositifs, prenant la forme d'une boîte noire, seraient placés directement chez les fournisseurs d'accès à Internet ainsi que les hébergeurs de données, sous le contrôle de la CNCTR. Ces derniers ont menacé de s'expatrier si le texte était adopté en l'état. La loi française n'opère pas de distinction entre les opérateurs de téléphonie et les différentes plateformes ou services de communication en ligne.

Au cœur du dispositif du renseignement se trouve le Premier ministre, dont les pouvoirs en la matière sont trop étendus, aux yeux des détracteurs du projet.

## **II- Des garde-fous insuffisants face aux pouvoirs étendus conférés au Premier ministre.**

La première observation porte sur la mise à l'écart de l'autorité judiciaire du dispositif. Certes le projet met en place une nouvelle autorité administrative indépendante, la CNCTR, dont on se demande déjà si elle fera le poids face à un Premier ministre détenteur de pouvoirs étendus.

- *La mise à l'écart de l'autorité judiciaire.*

Existe-t-il une défiance de l'exécutif à l'égard de l'autorité judiciaire en matière de renseignement ? Les professions judiciaires, avocats et magistrats du pôle antiterroriste regrettent que la procédure dominée par l'administration ait exclu le juge judiciaire, gardien des libertés individuelles en vertu de la Constitution. Le renseignement et la justice n'ont jamais fait bon ménage car ils relèvent de cultures radicalement opposées : d'un côté le règne du secret et des actions extra légales, de l'autre l'exigence de transparence et le respect de l'État de droit. La CNCIS n'a-t-elle pas rappelé dans son rapport 2013 que « indépendamment des questions constitutionnelles, tous les services de renseignement se montrent résolument rétifs à l'intrusion dans leur périmètre d'intervention, où

bien entendu s'impose un absolu secret, de magistrats dont l'activité obéit au contraire à des impératifs incontournables de transparence et de publicité des débats » ?

La mise à l'écart du juge judiciaire est d'autant plus surprenante que la loi n° 86-1020 du 9 septembre 1986 a créé le Pôle antiterroriste du tribunal de grande instance de Paris dont la mission est de démanteler les réseaux avant qu'ils n'aient commis un attentat. Par ailleurs, la loi n° 2000-516 du 15 juin 2000 reconnaît au juge des libertés et de la détention des pouvoirs importants en matière de renseignement, sans pour autant que dans les faits les moyens correspondant lui soient alloués. Le JLD est compétent pour ordonner diverses mesures de perquisitions en matière de terrorisme, d'interceptions de sécurité, de visites ou de saisies dans certains domaines dont le fisc, la santé publique, les armes à feu, etc. Or dans les faits, ce sont les services de renseignement qui détiennent un monopole de fait sur les outils de surveillance. Une judiciarisation du renseignement permettrait de lever un pan du secret.

La procédure -écrite- est conduite de bout en bout par le Premier ministre, dont le rôle est prépondérant, même s'il est tenu de saisir la nouvelle autorité indépendante (la CNCTR) pour avis.

- *Une nouvelle autorité administrative indépendante aux pouvoirs limités.*

La Commission nationale de contrôle des techniques de renseignement (CNCTR) est l'instance de régulation qui se substitue à la CNCIS appelée à disparaître. Cette dernière avait été créée par la loi du 10 juillet 1991, dans le contexte spécifique de l'affaire des Irlandais de Vincennes, à une époque où l'écoute téléphonique constituait à peu près la seule technique d'espionnage électronique. De nos jours, elle ne représente qu'un moyen parmi d'autres, plus adaptés aux plateformes de communication actuelles et aux réseaux sociaux. L'appellation de la future autorité de régulation traduit bien cette évolution en introduisant les termes plus génériques de « techniques de renseignement ».

La CNCTR, dotée du statut d'autorité administrative indépendante, est composée de 9 membres :

- 2 députés désignés par le Président de l'Assemblée nationale pour la durée de la législature ;
- 2 sénateurs désignés par le Président du Sénat à chaque renouvellement triennal ;
- 2 conseillers d'État\* nommés sur proposition du vice-Président du Conseil d'État ;
- 2 conseillers\* hors hiérarchie à la Cour de cassation, nommés sur proposition conjointe du Premier président et du Procureur général de la Cour de cassation ;
- Une personnalité qualifiée nommée sur proposition du président de l'ARCEP.

Les magistrats\* sont renouvelables par moitié tous les trois ans. Le mandat de chaque membre est de six ans non renouvelables. Sur le plan déontologique, les garanties classiques sont reconnues aux membres de cette nouvelle autorité : incompatibilités, secret professionnel, interdiction de recevoir des instructions, etc. Le président, qui ne peut détenir de mandat électif, est ordonnateur des dépenses de la commission, il est assisté d'un secrétaire général.

La mission de la commission est de veiller au respect des textes en exerçant un contrôle de légalité et d'opportunité. Ses prérogatives légèrement renforcées par rapport à celles de la CNCIS, demeurent toutefois limitées au regard des pouvoirs conférés au Premier ministre, dans la mesure où elles sont purement consultatives et qu'à aucun stade de la procédure elle ne peut réellement s'opposer à lui. La CNCTR est informée par le Premier ministre de toutes les autorisations qu'il est amené à délivrer. Elle dispose d'un droit d'accès et est informée des modalités d'exécution des opérations de renseignement. Elle publie un rapport annuel d'activités.

Le Premier ministre détient quant à lui et à tous les stades du déroulement de la procédure des prérogatives importantes lui permettant d'agir même contre l'avis de la commission. Des prérogatives que l'Union syndicale des magistrats n'hésite pas à qualifier d'exorbitantes. Une crainte qui ne peut que s'aggraver si le Premier ministre délègue ses pouvoirs à ses conseillers. La

procédure commence par la décision d'autorisation délivrée par le Premier ministre aux ministres concernés.

- *Au stade de l'autorisation*, le Premier ministre est tenu « sans délai » à une obligation d'information à l'égard de la commission, en précisant les techniques mises en œuvre, les finalités de l'opération, la durée de validité de l'autorisation, les personnes, lieux ou véhicules visés, les services spécialisés dans le renseignement désignés par lui (art. L 821-4). Le président de la commission rend son avis dans un délai vingt quatre heures, sauf lorsqu'il estime que la validité de la demande soulève un doute et décide de réunir la commission. Le Premier ministre est immédiatement informé de la décision. La commission rend alors son avis dans un délai de trois jours ouvrables. En l'absence d'avis rendu par le président, ou par le membre de la commission désigné par lui, dans le délai de vingt-quatre heures ou, si elle a été saisie, par la commission dans le délai de trois jours ouvrables, l'avis est réputé rendu. Mais en cas « d'urgence absolue », situation appréciée comme telle par le seul Premier ministre, cette obligation d'information tombe. Dans ce cas, la commission n'est saisie qu'*a posteriori*. Elle peut lui adresser une recommandation si elle estime que les dispositions légales ont été méconnues, aux fins de suspendre l'opération et détruire les données collectées. Encore un fois, le Premier ministre peut passer outre. La dernière possibilité est alors pour la commission, mais seulement à la majorité absolue de ses membres, de saisir le Conseil d'État.
- *La décision d'autorisation* du Premier ministre ou d'une des personnes par lui déléguées est écrite et motivée. Elle vaut pour une durée maximale de quatre mois et est renouvelable dans les mêmes conditions de forme et de durée que l'autorisation initiale. Elle précise la ou les techniques de renseignement mises en œuvre ; la ou les finalités poursuivies ; la durée de sa validité ; la ou les personnes, le ou les lieux ou véhicules concernés. L'interception et l'exploitation ultérieure des correspondances émises ou reçues de l'étranger sont également soumises à autorisation du Premier ministre.
- *Au stade de la mise en œuvre des opérations*, le Premier ministre définit les modalités de centralisation des renseignements collectés et en assure le respect par les services. Il est responsable de la traçabilité de l'exécution des techniques de renseignement. Il a autorité sur la conduite de toutes les opérations de collecte. Ensuite il est tenu de veiller au respect de l'obligation de destruction portant sur les données collectées, leur transcription, ainsi que leur extraction. Enfin, il doit tenir la commission informée du déroulement des opérations. À ce stade, il peut encore passer outre l'éventuelle recommandation de la commission en cas de méconnaissance de la loi. La commission peut alors saisir le Conseil d'État en application de l'art. L 821-6.

L'absence d'un contrôle *a priori* efficace peut ouvrir la voie à tous les abus. Un ancien juge du pôle antiterroriste, pourtant favorable au projet, soulève la question de l'utilisation que pourrait faire de ces moyens un gouvernement peu regardant sur les libertés, en ciblant par exemple l'opposition...

### **Pour conclure : le Conseil d'État, ultime recours.**

Le projet place le Conseil d'État au cœur du dispositif de contrôle juridictionnel *a posteriori* en lui donnant compétence pour connaître en premier et dernier ressort des requêtes concernant la mise en œuvre des techniques de renseignement mentionnées dans le texte (article L. 841-1). À cet effet, la haute juridiction peut tout d'abord être saisie par la CNCTR ainsi que par toute personne y ayant intérêt ou par les juridictions administratives ou judiciaires dès lors que le secret de la défense nationale est en cause. Les exigences de la procédure du contradictoire doivent se plier à celles du secret-défense, ainsi qu'à la nature particulière du traitement concerné lorsqu'il s'agit de Le président de la formation de jugement ordonne le huis-clos lorsqu'est en cause le secret de la défense nationale.

Les affaires sont portées devant une formation particulière dont la création est envisagée et à laquelle le secret-défense ne pourra être opposé. Les membres et le rapporteur public sont habilités ès-qualité au secret de la défense nationale et sont astreints, comme les agents qui les

assistent, au respect des secrets protégés par les articles 413-10, 226-13 et 226-14 du code pénal pour les faits, actes et renseignements dont ils peuvent avoir connaissance dans l'exercice de leurs fonctions.

La formation d'instruction entend les parties séparément, lorsqu'est en cause le secret de la défense nationale.

La formation de jugement peut se trouver devant deux possibilités : soit elle constate l'absence d'illégalité parce que le requérant n'a fait l'objet d'aucune mesures de surveillance, ou que ces mesures ont été mises en œuvre régulièrement, auquel cas la décision indique au requérant ou à la juridiction de renvoi qu'aucune illégalité n'a été commise, sans confirmer ni infirmer la mise en œuvre d'une technique ; soit elle constate qu'une technique de renseignement est ou a été mise en œuvre ou exploitée illégalement, elle peut annuler l'autorisation et ordonner, s'il y a lieu, la destruction des renseignements irrégulièrement collectés. Le requérant est informé qu'une illégalité a été commise et peut obtenir que l'État soit condamné à l'indemniser du préjudice qu'il a subi.

Si l'illégalité constatée est susceptible de constituer une infraction, la formation de jugement en avise le procureur de la République et transmet l'ensemble des éléments du dossier au vu duquel elle a statué à la CNCTR afin que celle-ci donne au Premier ministre son avis sur la possibilité de déclassifier tout ou partie de ces éléments en vue de leur transmission au procureur de la République.

---