UNION SYNDICALE DES MAGISTRATS

18 rue de la Grange Batelière - 75009 PARIS

Tél : 01.43.54.21.26. - Fax : 01.43.29.96.20.

E-mail : contact@union-syndicale-magistrats.org

Site : www.union-syndicale-magistrats.org

Paris, le 26 mars 2015

OBSERVATIONS DE L'USM
SUR LE PROJET DE LOI RELATIF AU RENSEIGNEMENT

L'Union Syndicale des Magistrats est le syndicat le plus représentatif des magistrats de l'ordre judiciaire (72,5% des voix aux élections au Conseil supérieur de la magistrature en 2014).

Elle s'interdit tout engagement politique et a pour objet d'assurer l'indépendance de la fonction judiciaire, garantie essentielle des droits et libertés du citoyen, de défendre les intérêts moraux et matériels des magistrats de l'ordre judiciaire et de contribuer au progrès du droit et des institutions judiciaires, afin de promouvoir une justice accessible, efficace et humaine.

La réforme du renseignement est une nécessité régulièrement mise en avant depuis plusieurs années (livres blancs sur la défense et la sécurité nationale), la France ne disposant pas d'un cadre juridique global en la matière.

L'exposé des motifs du projet de loi sur le renseignement met en avant un triple constat :

- Le renseignement est indispensable à la prévention des risques et menaces pesant sur le pays et les citoyens. Il contribue à assurer l'ordre public, sans lequel les droits des citoyens ne peuvent s'exercer pleinement.
- Pour autant, ces activités de renseignement sont actuellement dépourvues d'un cadre juridique général et cohérent, les textes en la matière étant limités.
- Cette absence de cadre juridique engendre d'importantes difficultés auxquelles le projet de loi entend remédier :

  * les agents des services de renseignements sont exposés dans le cadre de leur activité à des risques pénaux injustifiés

  * l'absence de règles claires génère une suspicion infondée sur l'activité des services,

  * cette même activité fait l'objet d'un contrôle limité, ce qui est inacceptable dans une société démocratique dès lors que cette activité touche aux libertés fondamentales.

Le texte s'articule donc autour de trois axes essentiels, visant à :

- assurer dans la loi la légitimité de la politique publique de renseignement, en définissant ses principes, ses finalités et son champ d'application;
- assurer un contrôle des techniques de recueil du renseignement par le biais notamment d'une nouvelle autorité administrative indépendante et d'un contrôle juridictionnel confié au Conseil d'Etat;
- définir les techniques de recueil de renseignement pouvant être utilisées par les services, ce qui implique, outre la reprise de dispositions sur les interceptions administratives ou l'accès aux données de connexion, la légalisation de l'usage de techniques actuellement mises en œuvre en dehors de tout texte.

L'USM déplore que la procédure accélérée soit engagée sur un projet de loi aussi important, dont les répercussions sur le respect des libertés individuelles sont particulièrement lourdes.

Si les annonces ministérielles laissent à penser que ce projet de loi favorisera la prévention du terrorisme, qui justifierait un encadrement des techniques mises en œuvre, il convient de rappeler que ce projet de loi porte sur le renseignement au delà de la seule question du terrorisme et qu'il est en réflexion depuis plusieurs mois. Rien ne justifie donc la procédure accélérée, qui ne favorise pas un débat réel et serein et qui pose ici un réel problème de respect des principes démocratiques.

Dans la présente note, l'USM développera précisément sa position sur les différentes dispositions du texte.

Elle entend toutefois d'ores et déjà poser, à titre de préambule, les points suivants :

1/ l'activité de renseignement relève effectivement d'une politique publique essentielle, destinée à assurer la « sûreté », au sens de la Déclaration des droits de l'Homme et du citoyen de 1789, ou à préserver « l'ordre public », sans lequel, selon le Conseil constitutionnel, « l'exercice des libertés publiques ne saurait être assuré ».

L'USM est donc favorable à la définition d'un cadre légal de l'activité des services de renseignement, préalable indispensable au contrôle de cette activité.

Pour autant, parce que l'exercice de cette activité implique de potentielles atteintes à des libertés individuelles à valeur constitutionnelle, telles que la sûreté, le respect de la vie privée, l'inviolabilité du domicile ou des correspondances, les libertés de conscience, d'opinion, de manifestation, d'expression etc... son champ d'application doit être défini aussi restrictivement que possible. En l'occurrence, le texte prévoit une extension de la sphère d'intervention des services de renseignement, que l'USM juge injustifiée et inquiétante.

2/ Le texte prétend instaurer « un contrôle strict » sur la mise en œuvre des techniques de recueil du renseignement, par le biais d'une nouvelle autorité administrative indépendante (la Commission nationale de contrôle des techniques de renseignement) et d'une procédure juridictionnelle relevant du Conseil d'Etat.

Ce contrôle est censé garantir une juste proportionnalité entre les buts poursuivis, les moyens techniques mis en œuvre et les atteintes portées aux libertés individuelles.

Sur ce point absolument essentiel, l'USM dénonce l'hypocrisie du texte. Tout en affirmant mettre en place un système de contrôle étendu, le projet de loi définit en réalité des modalités d'exercice de ce « contrôle » qui lui ôte toute efficience.

3/ Enfin, s'agissant des techniques susceptibles d'être mises en œuvre par les services de renseignement, l'USM n'est pas opposée par principe à leur extension, dans un cadre légal.

Toutefois les techniques employées impliquent toutes des atteintes aux libertés individuelles, d'une extrême importance pour certaines d'entre elles. La légitimité de leur emploi renvoie donc à la question du contrôle de l'activité des services, au contrôle de la proportionnalité entre le but poursuivi et les moyens employés. L'usage d'une technique spécifique pourra en effet être jugée légitime dès lors qu'il s'agit de prévenir des actes de terrorisme alors qu'il pourrait ne pas l'être pour la prévention d'éventuelles violences collectives.

L'USM estime donc que la question des moyens techniques mis à la disposition des services dépend de l'évolution du texte sur le contrôle réel de la mise en œuvre de ces mêmes moyens par les services.

Enfin, parce que ce texte touche aux libertés fondamentales, l'USM demande instamment qu'à l'issue du processus législatif, le Conseil constitutionnel soit saisi par les parlementaires et mis ainsi en mesure d'apprécier la conformité de ce texte au regard des normes constitutionnelles et de l'équilibre qu'il convient de conserver entre ces dernières.

Plan :

I. Définition d'un cadre légal pour l'activité de renseignement

1/ Un cadre nécessaire

2/ Mais une extension injustifiée et inquiétante du champ d'intervention des services de renseignement

II. Le pseudo-contrôle de la mise en œuvre des techniques de recueil de renseignement

1/ La Commission nationale de contrôle des techniques de renseignement

1. Un circuit d'autorisation inefficient
2. La composition de la CNCTR
3. Les missions

2/ Les recours relatifs à la mise en œuvre des techniques de renseignement

1. La compétence exclusive du Conseil d'Etat : pour une compétence judiciaire
2. Les conditions de saisine
3. L'instauration d'une question préjudicielle, y compris en matière pénale lorsqu'est mis en cause le secret de la défense nationale

3/ Le contentieux de la mise en œuvre des techniques de renseignement

III. Les techniques de renseignement mises en œuvre par les services : des techniques très larges, sans réel contrôle

1/ l'accès administratif aux données de connexion

2/ les interceptions de sécurité

3/ les dispositifs mobiles de proximité (IMSI-catchers)

4/ la géolocalisation

5/ l'enregistrement des paroles ou images d'une personne et la captation de ses données informatiques

6/ les interceptions de communications électroniques émises ou reçues à l'étranger : une absence totale de contrôle

IV. Dispositions particulières

1/ La surveillance des détenus

2/ La protection des agents

3/ Renforcement des pouvoirs de TRACFIN

4/ Dispositions diverses et recodification

I. Définition d'un cadre légal pour l'activité de renseignement

1/ Un cadre nécessaire :

L'activité de renseignement relève d'une prérogative étatique aussi ancienne que les Etats eux-mêmes. Elle vise à fournir à l'exécutif les informations importantes pour la sécurité nationale et fait partie à ce titre des instruments de protection de la démocratie.

Pour autant, la rareté des textes régissant l'activité des services de renseignements et le caractère secret de cette activité peuvent favoriser de possibles dévoiements individuels ou collectifs. Elle génère, a minima, un climat de suspicion sur le rôle et les actions des services concernés.

Dans le contexte post 11 septembre 2001, les services de renseignements ont connu une mutation profonde de leur organisation. Celle-ci s'est encore accrue après les attentats de Toulouse et Montauban, en mars 2012.

Les six services de renseignement français (Direction générale de la sécurité extérieure -DGSE-, Direction du renseignement militaire -DRM-, Direction de la protection et de la sécurité de la défense -DPSD-, Cellule de traitement du renseignement et action contre les circuits financiers clandestin -TRACFIN-, Direction nationale du renseignement et des enquêtes douanières -DNDRED-, et, depuis 2014, la Direction centrale du renseignement intérieur -DCRI-), sont désormais constitués en « communauté du renseignement ».

Un coordonnateur national, conseiller du Président de la République, veille à la bonne coopération des services. Une « Académie du renseignement », rattachée au Premier Ministre, forme les personnels de ces services.

Le Parlement a accompagné cette évolution et la Délégation parlementaire au renseignement (DPR) a publié en décembre 2014 son premier rapport entièrement public relatif à son activité de contrôle de l'activité des services de renseignement. Il faisait suite au rapport d'information de mai 2013, présenté par MM. Urvoas et Verchère, préconisant nombre des modifications envisagées par la présente loi.

Des moyens importants sont dévolus à ces services, notamment en personnel (13 000 ETPT dans le budget 2014). Après les attentats de janvier 2015, des renforts, à hauteur de 500 postes, ont été annoncés.

Dans ce contexte de réorganisation, le cadre légal dans lequel œuvrent officiellement ces services est présenté par ces derniers comme particulièrement limité.

De fait, ces services s'appuient, pour exercer leurs missions, sur les seules dispositions de :

- la loi du 10 juillet 1991 relative au secret des correspondances, codifiée dans le code de la sécurité intérieure (articles L 241-1 et suivants). Elle définit le régime permettant la mise en œuvre des interceptions de sécurité administratives, placées sous le contrôle d'une autorité administrative indépendante, la Commission nationale de contrôle des interceptions de sécurité (CNCIS).
- la loi du 23 janvier 2006 (modifiée par la loi du 18 décembre 2013), permettant aux services de renseignements d'accéder aux données de connexion d'une personne, sous le contrôle d'une personne qualifiée (article L. 34-1 et suivants du code des postes et communications électroniques), rattachée au Premier Ministre mais placée sous le contrôle de la CNCIS.

- la loi de programmation militaire du 18 décembre 2013 qui a étendu la compétence de la CNCIS à la transmission de données de connexion en temps réel (géolocalisation)
- la loi du 06 janvier 1978 (modifiée) qui autorise les services de renseignement à avoir accès à divers fichiers (CNI, gestion des passeports, contrôle des étrangers visé au CESEDA etc...).
- la loi de programmation militaire précitée qui autorise la création et l'exploitation de données relatives aux passagers aériens (décrets de 2014).

Les rapports parlementaires évoqués précédemment reconnaissent implicitement que l'activité réelle des services ne se résume pas aux actes prévus, et autorisés par l'actuel cadre légal et qu'ils agissent donc en usant d'autres moyens, par conséquent non contrôlés.

C'est cette absolue nécessité d'un contrôle réel, effectif et complet de l'activité des services de renseignement qui justifie, car il correspond à un impératif démocratique essentiel, la totale remise à plat du cadre légal dans lequel oeuvrent ces services.

Pour que ce contrôle puisse s'exercer, cela suppose en effet un préalable indispensable : l'inscription de l'activité de renseignement dans le domaine de la Loi, la définition de son contour et des moyens susceptibles d'être légalement employés.

L'USM ne peut donc qu'être favorable au principe d'une loi qui aurait une telle ambition.... et déçue de constater à quel point le présent projet de loi s'avère, *in fine*, très en-deçà des ambitions affichées...

2/ Une extension injustifiée et inquiétante du champ d'intervention des services de renseignements

En premier lieu, sous couvert de mieux définir le champ de compétence des services de renseignements, le projet de loi étend celui-ci de manière subreptice.

Actuellement, le champ d'intervention de ces services est défini indirectement par la loi du 10 juillet 1991, qui précise les différents cas dans lesquels peuvent être mises en œuvre les interceptions de sécurité (article L241-1 du CSI). Ces motifs sont déjà nombreux puisqu'ils recouvrent la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de l'article L.212-1 (groupes de combat ou milices privées, groupes provoquant à la discrimination, à la haine...).

Le projet de loi va plus loin encore.

Ainsi, selon l'article L811-3 du CSI tel qu'issu du projet, les services spécialisés peuvent être autorisés à recourir aux techniques de renseignement pour le recueil de renseignements « relatifs aux intérêts publics suivants :

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 ».

L'absence de définition claire et précise des « intérêts publics » en jeu permettra la mise en œuvre des techniques de renseignement, bien plus larges que les seules écoutes téléphoniques, dans de très nombreux domaines.

En l'espèce, on notera, s'agissant des critères ajoutés par le projet de loi et susceptibles de justifier la mise en œuvre de techniques de renseignements, le caractère particulièrement flou de la notion « d'intérêts essentiels de la politique étrangère ».

De même, le nombre singulièrement élevé et le caractère disparate des « engagements internationaux et internationaux de la France » rend cette dernière notion potentiellement très large.

S'agissant de « la prévention des violences collectives », cet ajout revient à contrer les décisions de la CNCIS qui, en matière d'interceptions de sécurité, a toujours refusé de les autoriser dès lors que la sécurité nationale n'était pas menacée. Dans son dernier rapport, la CNCIS a ainsi précisé qu'en l'état des textes actuels, aucune interception ne pouvait être autorisée sur la seule crainte d'un trouble à l'ordre public, « comme y expose plus ou moins toute manifestation ». Désormais, cette possibilité serait ouverte, non seulement pour des écoutes mais pour toutes les nouvelles techniques légalisées par le projet de loi (cf partie III).

Concrètement, en l'état, ce projet de loi autorise par exemple la mise en œuvre de multiples outils de renseignement en amont de toute manifestation, quel qu'en soit l'objet, au seul motif de « prévenir des violences collectives de nature à porter gravement atteinte à la paix publique ». Ainsi, à la veille d'une manifestation serait légalisée l'introduction d'agents de renseignement, au sein du domicile de tout représentant syndical voire même de tout potentiel participant, pour qu'ils y installent des micros ou des caméras, et ce sans réel contrôle, ni préalablement, ni postérieurement.

De même, dans son dernier rapport, la CNCIS a rappelé, s'agissant des intérêts économiques et scientifiques essentiels, que le texte visait à assurer leur sauvegarde, ce qui supposait de caractériser clairement une menace et que la personne objet des écoutes soit directement impliquée dans cette menace. La rédaction actuelle, en faisant disparaître la notion de menace, permet donc d'envisager un usage très élargi des moyens de renseignements...

Il ne s'agit pas pour l'USM de refuser la mise en œuvre d'outils technologiques nécessaires à la préservation des intérêts de l'Etat.

Mais, au regard de l'ampleur des outils à la disposition des agents spécialisés, les domaines d'intervention doivent être plus précisément définis et un contrôle effectif doit être mis en place, s'agissant d'atteintes potentiellement graves aux libertés individuelles.

L'USM demande donc que la sphère d'intervention des services de renseignement reste limitée aux seuls domaines visés dans la loi de juillet 1991. Les extensions envisagées par le projet de loi ne présentent pas de caractère d'évidente nécessité, alors même qu'ils portent en germe le risque d'abus majeurs.

II. Le pseudo-contrôle de la mise en œuvre des techniques de recueil de renseignement

Selon les promoteurs de la loi, le circuit d'autorisation envisagé pour permettre la mise en œuvre des diverses mesures dorénavant à la disposition des services de renseignement (écoutes, pose de balise, introduction dans un domicile, dans un système de données informatiques etc...) assurerait un contrôle efficace de l'activité des services.

Complétée par un possible contrôle juridictionnel confié au Conseil d'Etat, cette procédure permettrait d'assurer « la protection des libertés constitutionnellement garanties ».

En réalité, l'examen attentif des mécanismes de contrôle envisagés démontre que ces derniers risquent de rester théoriques.

1/ La commission nationale de contrôle des techniques de renseignement :

Destinée à remplacer l'actuelle Commission Nationale de Contrôle des Interceptions de Sécurité (CNCIS, compétente pour les interceptions de sécurité et l'accès administratif aux données de connexion), serait instituée une Commission nationale de contrôle des techniques de renseignement (CNCTR). Celle-ci aurait vocation à être saisie de demandes portant sur l'ensemble des techniques de renseignement reconnues par la présente loi.

Après plus de 20 ans d'existence, la CNCIS a démontré sa capacité à opérer un réel contrôle sur l'action des services, dans le champ de compétence restreint qui est le sien. Elle a bâti une jurisprudence protectrice, tout en étant pragmatique au regard du rôle et des missions spécifiques des services de renseignement. Elle a ainsi imposé un contrôle préalable que ne prévoyaient pas les textes, procédé à un examen de la motivation et de la pertinence des demandes, vérifié le respect du principe de subsidiarité (pas d'autorisation d'écoutes si les informations recherchées peuvent être recueillies par d'autres moyens...). Elle répond aux demandes qui lui sont soumises en quelques heures, conciliant donc respect des droits et besoins des services.

Au vu de cet apport, l'USM est favorable au maintien d'un régime d'autorisation donné par une autorité administrative indépendante, comme le suggère le projet de loi. Toutefois, cet accord ne s'entend que sous réserve que la nouvelle autorité administrative indépendante présente a minima les mêmes apports que la CNCIS : une équipe réduite, disponible, opérationnelle, dont les membres présenteraient des garanties d'indépendance affirmées. La procédure devrait également assurer à la CNCTR un rôle incontournable. Tel n'est malheureusement pas le cas en l'état du texte.

Enfin, si la procédure prévue par le projet de loi envisage la possibilité d'un recours juridictionnel, l'USM demande que ce recours relève de la compétence d'une composition spéciale de la Cour de cassation et non du Conseil d'Etat, ainsi que cela est envisagé.

1.1 : un circuit d'autorisation inefficient (art. L. 821 et suivants du projet de loi)

Présentation du circuit général d'autorisation, tel que prévu par le projet de loi :

- les trois ministres compétents en la matière (Défense, Intérieur, Budget), qui sont par ailleurs assistés chacun de trois personnes spécialement désignés, adressent une demande

écrite et motivée de mise en œuvre d'une ou plusieurs techniques de recueil de renseignement (art. L 821-2)

- cette demande est communiquée au président de la Commission nationale de contrôle des techniques de renseignement ou, à défaut, à un membre de la commission désigné par celui-ci, qui délivre son avis sous 24 heures. En cas de doute sur la validité de la demande, le président (ou membre désigné) réunit la commission qui rend un avis dans les 3 jours. A défaut d'avis dans les 24 h ou, le cas échéant, dans les trois jours, l'avis est réputé rendu. En tout état de cause, cet avis ne lie pas le Premier ministre.
- l'autorisation, écrite et motivée, est rendue par le Premier ministre (ou l'une des 6 personnes désignées par lui), pour une durée de 4 mois, renouvelable selon les mêmes formes.
- en cas d'urgence absolue, le Premier ministre peut autoriser la mise en œuvre de la mesure sans avis préalable de la commission et en informe la commission.
- si une autorisation paraît à la commission avoir été accordée en méconnaissance des dispositions légales, la commission adresse au Premier ministre une recommandation, tendant à l'interruption de cette mesure et à la destruction des renseignements collectés.
- à défaut, la commission, peut, à la majorité absolue de ses membres, saisir le Conseil d'Etat.
- chacun des services établit un registre de mise en œuvre, tenu à la disposition de la Commission.

* Les dispositions organisant actuellement les autorisations d'interceptions de sécurité de nature administrative prévoient en théorie un contrôle a posteriori des autorisations délivrées par le Premier ministre (art. L 243-8 du code de la sécurité intérieure). En réalité, très rapidement après sa mise en place, cette commission a instauré avec l'accord des Premiers ministres successifs, en allant au-delà des textes, la pratique d'un accord préalable à l'autorisation, transformant de fait le contrôle exercé par la commission en contrôle a priori.

Le ministre qui demandait l'instauration d'une écoute adressait donc celle-ci à la commission qui donnait son avis. Ensuite seulement, le Premier ministre prenait sa décision, généralement en conformité avec l'avis donné.

Les demandes étaient examinées par la commission dans le délai de quelques heures en cas d'urgence signalée (¼ des demandes), en moins d'une semaine dans les autres cas.

Dans le projet de loi, toutes les demandes ne seraient plus présentées à la CNCTR avant la mise en œuvre des mesures. En effet, en cas « d'urgence absolue », un régime dérogatoire permettrait au Premier ministre d'autoriser la mise en œuvre des mesures sollicitées sans avis préalable de la commission. Alors même que la CNCIS a démontré sa capacité à répondre à toutes les situations d'urgence qui lui étaient soumises, cette procédure spécifique envisagée devant la CNCTR correspond à une incontestable régression. Il suffira donc aux services de renseignement de qualifier eux-mêmes leur demande d'urgente, pour qu'elle soit exonérée du contrôle a priori prévu par les textes.

En tout état de cause, rien ne justifie que les demandes de placement sur écoutes, qui pouvaient toutes être examinées préalablement en urgence, ne le soient plus à l'avenir.

L'USM demande donc la suppression de ce dispositif dérogatoire et que l'ensemble des demandes fasse l'objet d'un contrôle a priori.

* L'esprit même des textes a changé. L'article L 241-2, actuellement en vigueur, dispose que les demandes d'interceptions de sécurité, formées devant la CNCIS, revêtent un caractère « exceptionnel ». C'est cette exigence de principe qui a permis à la CNCIS de bâtir une jurisprudence (cf. le 22ème rapport d'activité de la CNCIS) sur le caractère subsidiaire des mesures sollicitées : dans le cadre de son contrôle de légalité la commission vérifiait que la mesure sollicitée était l'unique moyen de répondre à la menace spécifique qui était évoquée par le service de renseignement.

Or, dans les dispositions du projet de loi, cette notion de subsidiarité a disparu. L'article L 811-3 évoque l'aspect formel de la demande (la technique à mettre en œuvre, la finalité poursuivie, le motif de la demande, la personne, le lieu ou le véhicule concerné, le service bénéficiaire).

Dans son avis, le Conseil d'Etat a demandé, sans être suivi à ce stade, que le principe de subsidiarité (qui découle du principe de proportionnalité entre les différentes valeurs constitutionnelles) soit rappelé pour la mise en œuvre des mesures les plus attentatoires aux libertés (captation, enregistrement de son et image, introduction dans un domicile, véhicule, etc...), ce qui supposerait une motivation renforcée (permettant alors un contrôle par la commission de la pertinence de la demande).

L'USM demande instamment la modification des textes proposés pour faire apparaître le caractère exceptionnel des mesures sollicitées, dont rien ne justifierait qu'elles soient banalisées, ainsi que la notion de subsidiarité. Ces modifications, au-delà du symbole, sont indispensables pour asseoir un contrôle réel sur la pertinence des mesures et leur adéquation aux objectifs poursuivis. A défaut, le contrôle mis en place ne serait que formel.

* Plus généralement, l'USM demande que soit posé le principe d'un avis préalable et conforme de la commission.

* Le projet de loi prévoit que la mise à exécution des différentes données fasse l'objet d'une traçabilité (art. L 821-5 du CSI) et que chaque service tienne à jour des registres permettant à la CNCTR d'effectuer des vérifications en cours d'exécution, comme le faisait la CNCIS en matière d'écoutes administratives. Pour autant, l'USM demande que l'ensemble des données soit centralisé afin de faciliter ces opérations de contrôle. En l'état du texte, rien ne paraît avoir été envisagé pour rendre le contrôle aussi efficient que possible. Il est regrettable que l'avis du Conseil d'Etat (allant dans le sens de nos demandes) n'ait pas été suivi.

* Enfin, le nombre des interceptions de sécurité fait l'objet d'un contingentement. En l'état des textes, ce contingent relève d'un décret et est donc à la seule discrétion du Premier ministre. L'USM suggère que le Parlement soit associé à la fixation de ce contingent, ce qui contribuerait à renforcer le contrôle exercé par le législateur sur l'action des services.

1.2 : la composition de la CNCTR et la déontologie

Composition :

Le projet de loi prévoit la création d'une nouvelle autorité administrative indépendante, composée de 9 membres :

- deux députés désignés pour la durée de la législature par le président de l'Assemblée nationale

- deux sénateurs, désignés après chaque renouvellement partiel du Sénat par le président du Sénat,
- deux membres ou anciens membres du Conseil d'Etat, d'un grade au moins égal à celui de conseiller d'Etat, nommés sur proposition du vice-président du Conseil d'Etat, pour une durée de 6 ans.
- deux magistrats ou anciens magistrats hors hiérarchie de la Cour de cassation, nommés sur proposition conjointe du Premier président et du Procureur général de la Cour de cassation, pour une durée de 6 ans.
- une personnalité qualifiée pour sa connaissance en matière de communications électroniques, nommée sur proposition du président de l'Autorité de régulation des communications électroniques et des postes, pour une durée de 6 ans.

Il sera rappelé que l'actuelle CNCIS est composée de 3 membres :

- un magistrat ou magistrat honoraire de l'ordre judiciaire ou administratif

- un député

- un sénateur

La CNCIS bénéficie également du soutien de trois collaborateurs qui sont actuellement trois magistrats de l'ordre judiciaire, en détachement.

L'USM considère que le rôle crucial dévolu à la CNCTR implique une composition resserrée, des membres indépendants et disponibles et une présidence à temps plein. Dans son avis, le Conseil d'Etat suggère, pour les mêmes raisons, une composition de 5 personnalités présentant ces garanties.

L'USM partage cet avis.

Le projet de loi prévoyant le nombres des personnes détachées auprès des trois ministres concernés (3) et auprès du Premier ministre (6), l'USM demande que l'existence des collaborateurs de la commission soient également officialisée et, surtout, qu'il s'agisse impérativement de magistrats de l'ordre judiciaire, en détachement.

S'agissant du recrutement des membres de la commission, l'USM regrette qu'aucune validation par les commissions des lois ne soit prévue pour la désignation des parlementaires membres de la CNCTR. A titre de comparaison, les parlementaires membres de la CNIL sont désignés par l'assemblée dont ils sont issus.

S'agissant du président, le projet de loi prévoit sa désignation par décret, parmi les membres issus du Conseil d'Etat ou de la Cour de cassation.

Faute de précision du signataire de ce décret, on peut supposer qu'il s'agirait du Premier ministre.

L'USM conteste ces dispositions qui permettent au Premier Ministre de désigner lui-même le président de la CNCTR, président qui serait amené à lui donner, seul, un avis sur la mise en œuvre des techniques de renseignements envisagées.

Le mode de désignation du président doit permettre de lever tout doute sur une nomination politique.

L'USM demande que le président de la CNCTR soit désigné, parmi les membres issus du Conseil d'Etat ou de la Cour de cassation, par un collège composé du vice-président du Conseil d'Etat, du premier Président de la Cour des Comptes, du Premier Président de la Cour de Cassation, du Procureur Général près la Cour de Cassation, du Président du Conseil économique, social et environnemental, du Défenseur des droits et du président de la CNIL.

A défaut, la présidence pourrait être assurée successivement pendant le mandat de 6 ans par chacun des magistrats administratifs et judiciaires, en alternance.

Règles de déontologie et de fonctionnement (articles L832-1 et suivants du CSI)

Le projet de loi prévoit des règles de déontologie et d'incompatibilité qui n'appellent pas d'observation particulière de l'USM.

Il est prévu que la CNCTR ne puisse valablement délibérer que si au moins 4 membres sont présents.

Le projet de loi prévoit que les agents des services de la commission sont choisis notamment en raison de leurs compétences juridiques, économiques et techniques en matière de communications électroniques et de protection des données personnelles.

L'USM considère que ce choix doit être opéré sur proposition du président de la commission et après avis conforme de la majorité de ses membres.

1.3 : les missions de la CNCTR

Veiller au respect des règles du code de la sécurité intérieure

Le projet de loi prévoit que la CNCTR veille à ce que les techniques de recueil du renseignement soient mises en œuvre conformément aux règles du code de la sécurité intérieure.

Pour l'accomplissement de sa mission, il est prévu qu'elle :

- reçoive communication de toutes les autorisations délivrées par le Premier ministre et les personnes que ce dernier délègue,
- dispose d'un droit d'accès aux autorisations, relevés, registres, données collectives, transcriptions et extractions …
- soit informée à tout moment, à sa demande, des modalités d'exécution des autorisations en cours.

L'USM estime que ces dispositions sont insuffisantes pour permettre un réel contrôle des techniques de renseignement mises en œuvre. Au-delà des simples droits d'accès et informations prévues, la commission doit être rendue destinataire de l'ensemble de ces éléments sans qu'une démarche volontaire de sa part soit préalablement nécessaire.

De même, il est prévu que le Premier ministre puisse communiquer à la CNCTR tout ou partie des rapports de l'inspection des services de renseignement ainsi que des rapports des services d'inspection générale des ministères, en lien avec les missions de la commission. Cette communication ne doit pas relever d'une seule possibilité mais d'une obligation mise à la charge des services du Premier Ministre.

Les réclamations

Selon l'état actuel du projet, la CNCTR peut être saisie d'une réclamation de toute personne ayant un intérêt direct et personnel, ou procéder au contrôle du respect des dispositions légales de sa propre initiative.

Est ainsi exclu le recours de toute association. L'USM s'interroge sur la notion d'intérêt personnel et direct qui pourrait être invoquée par les particuliers. Comment en justifier, si ce n'est en émettant un doute quant à l'utilisation d'une technique de renseignement à son encontre. C'est donc la CNCTR qui décidera de la recevabilité de la réclamation.

Si la demande est recevable, et lorsque des vérifications auront été réalisées, la CNCTR ne confirme, ni n'infirme la mise en œuvre d'une technique de renseignement. Elle notifie seulement au réclamant qu'il a été procédé aux vérifications nécessaires.

Si la CNCTR constate une irrégularité, elle adresse au service concerné et au premier ministre une recommandation tendant à ce que la mise en œuvre de la technique concernée soit interrompue et les renseignements collectés détruits (article L821-6 et L du CSI).

Il est également prévu qu'elle fasse état dans son rapport public annuel du nombre de recommandations, tendant à ce que la mise en œuvre d'une technique, soit interrompue adressées au premier ministre et du nombre de fois où le Premier ministre a décidé de ne pas procéder à l'interruption.

Alors que le projet ne prévoit aucun délai de recevabilité de réclamation, on peut s'interroger sur la manière dont le contrôle pourra être réalisé, dès lors que la commission ne reçoit pas tous les éléments. Quid si les éléments ont été détruits ?

L'USM déplore que la CNCTR n'ait, ici encore, aucun pouvoir coercitif.

La seule recommandation qu'elle peut adresser au Premier ministre paraît totalement insuffisante et inadaptée puisque celui-ci est libre de la suivre ou non.

Le fait que la CNCTR puisse faire état dans son rapport annuel du nombre de fois où le Premier ministre a décidé de ne pas procéder à l'interruption de la technique de renseignement ne pallie pas cet écueil.

Ne suffit pas non plus le fait que la commission puisse saisir, à la majorité absolue de ses membres, le Conseil d'Etat, lorsque ses recommandations ne sont pas suivies d'effet.

2/ Les recours relatifs à la mise en œuvre des techniques de renseignement

Le projet de loi attribue compétence au Conseil d'État pour connaître des requêtes concernant la mise en œuvre des techniques de renseignements soumises à autorisation (L841-1 du CSI et L411-4-1 du code de justice administrative).

Le Conseil d'État peut être saisi par :

1° toute personne y ayant un intérêt direct et personnel et justifiant de la mise en œuvre préalable de la procédure prévue à l'article L.833-3 (c'est-à-dire la saisine de la Commission nationale de contrôle des techniques de renseignement),

2° la Commission nationale de contrôle des techniques de renseignement.

Lorsqu'est en cause le secret de la défense nationale, le Conseil d'État peut également être saisi à titre préjudiciel, par toute juridiction administrative ou toute autorité judiciaire saisie d'une procédure ou d'un litige dont la solution dépend de l'examen de la régularité des techniques de renseignement dont la mise en œuvre est alléguée par l'une des parties. Il statue dans le délai d'un mois à compter de la décision de saisine de la juridiction de renvoi.

Ces dispositions appellent les observations suivantes sur la compétence exclusive du Conseil d'État, sur les conditions de sa saisine et sur l'instauration d'une question préjudicielle y compris en matière pénale.

2.1 La compétence exclusive du Conseil d'État

Le Conseil d'État, dans son avis sur le projet de loi, a considéré que la mise en œuvre des techniques prévues relevaient de la police administrative et que la juridiction administrative était compétente pour connaître des litiges relatifs à celle-ci.

Toutefois, l'article 66 de la Constitution de 1958 dispose que nul ne peut être détenu arbitrairement et institue l'autorité judiciaire comme gardienne de la liberté individuelle pour assurer le respect de ce principe dans les conditions prévues par la loi.

Le Conseil constitutionnel a, jusqu'en 1999, rattaché les principes fondamentaux garantis par les lois de la République à la liberté individuelle et a déterminé les composantes de la liberté individuelle en imposant l'intervention de l'autorité judiciaire.

À partir de 1999, la jurisprudence du Conseil constitutionnel a évolué.

Relèvent désormais de la compétence de principe du juge judiciaire les contentieux d'atteinte grave et prolongée à la liberté individuelle ainsi que le contentieux des droits fondamentaux qui lui est réservé par tradition.

La violation du domicile met en cause la liberté individuelle. Les visites et les perquisitions sont subordonnées à une autorisation et un contrôle de l'autorité judiciaire. Ainsi le juge de la liberté et de la détention est compétent pour autoriser les perquisitions de nuit ainsi que les visites domiciliaires et les saisies de pièces à conviction. Le procureur de la république est également compétent pour les perquisitions effectuées dans le cadre de l'enquête préliminaire et le juge d'instruction pour les perquisitions effectuées au cours de l'information judiciaire. Les visites de l'administration fiscale sont soumises au contrôle du président du tribunal de grande instance.

Il sera par ailleurs rappelé que tous les contrôles d'identité, y compris de nature administrative (préventif, hors réquisitions et indépendamment du comportement de la personne – art. 78-2 alinéa 7 du CPP), et toutes les fouilles de véhicules, même dans le cadre de l'exercice de pouvoirs de police administrative (art. 78-2-4), sont placés sous le contrôle de l'autorité judiciaire (article 78-1 du code de procédure pénale). Le Conseil constitutionnel, maintes fois saisi au gré des réformes en la matière, a estimé que cette réglementation doit « *concilier les valeurs de liberté et de sûreté* » et que, « *compte tenu en particulier du rôle confié à l'autorité judiciaire, (ces dispositions) ne sont pas contraires à la conciliation qui doit être opérée entre l'exercice des libertés constitutionnellement reconnues et les besoins de la recherche des auteurs d'infraction et la prévention d'atteintes à*

l'ordre public, nécessaires l'une et l'autre à la sauvegarde des valeurs constitutionnelles » (DC 26/08/86)

Il est à noter que le contentieux des décisions de l'Autorité de régulation des communications électroniques et des postes a été expressément dévolu par le législateur au juge judiciaire.

Par ailleurs, parmi les contentieux des droits fondamentaux réservés par tradition au juge judiciaire figure le droit au respect de la vie privée. Le contentieux civil du droit au respect de la vie privée se fonde sur l'article 9 du code civil : « *Chacun a droit au respect de sa vie privée* ». Cet article garantit le droit à l'intimité physique et morale de la personne, ce qui inclut la protection du domicile et des correspondances.

L'application de ces critères de compétence traditionnelle du juge judiciaire aurait dû conduire le gouvernement à soumettre les atteintes les plus graves à la liberté individuelle, impliquant à la fois la violation de la vie privée et du domicile, au juge judiciaire.

Il en va ainsi des dispositions prévues à l'article L.853-1 qui prévoient que « *Peut-être autorisée, lorsque les renseignements relatifs aux finalités prévues à l'article L.811-3 ne peuvent être recueillis par un autre moyen légalement autorisé, l'utilisation de dispositifs techniques permettant : 1° la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel, ou d'images dans un lieu privé* ».

Il en va ainsi également de l'introduction, prévue à l'article L.853-2, 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.

2.2 Les conditions de la saisine du Conseil d'État (article 4)

Il peut être saisi par toute personne qui y a un intérêt direct et personnel et qui justifie de la mise en œuvre préalable de la procédure prévue à l'article L. 833-3 et par la Commission nationale de contrôle des techniques de renseignements.

La saisine de la juridiction chargée des recours relatifs à la mise en œuvre des techniques de renseignements est par conséquent exclue pour les associations en charge de la défense des droits et libertés. Cette saisine aurait néanmoins pu être envisagée dans un État démocratique.

La CNCTR peut saisir le Conseil d'Etat dans deux cas : lorsque le Premier ministre n'a pas suivi ses recommandations après que la commission a estimé qu'une autorisation de mise en œuvre des dispositifs de renseignement n'aurait pas dû être accordée (L. 821-6) ou que son avis défavorable à l'introduction dans un local ou un système de traitement automatisé de données n'a pas été suivi (L 853-2). L'USM estime que devrait être ajoutée la possibilité de saisir le Conseil d'Etat lorsque ses recommandations tendant à la destruction de données ne sont pas suivies (art. L. 822-2).

Surtout la faculté ouverte à la commission de contrôle de saisir le Conseil d'État, à la majorité absolue de ses membres, lorsque le premier ministre n'a pas donné suite à ses recommandations souligne la faiblesse des pouvoirs de cette Commission. Non seulement elle ne donne qu'un avis, mais cet avis ne lie pas le premier ministre qui peut passer outre ou même se dispenser de son avis

préalable en cas d'urgence absolue, mais il n'est pas non plus tenu de suivre ses recommandations lorsqu'elle estime qu'une autorisation a été accordée en méconnaissance des dispositions légales ou qu'une technique de renseignement a été mise en œuvre en méconnaissance des mêmes dispositions.

Cette commission, décrite dans l'avis du Conseil d'État comme constituant l'une des garanties essentielles entourant la mise en œuvre des techniques de renseignements énumérés dans le projet de loi, est en réalité dénuée de pouvoir de décision, celui-ci étant exercée par le premier ministre sous le seul contrôle du Conseil d'État.

Aucun délai de recours n'est prévu, alors que des délais sont prévus pour la destruction des pièces obtenues par les techniques de renseignement. Certains recours seront donc fictifs.

Aucun délai n'est imposé au Conseil d'Etat pour rendre sa décision. Là encore, la destruction des pièces pourra priver le recours de toute efficacité dès lors que le Conseil d'Etat n'aura pas rendu sa décision avant.

De plus, la question de l'objet d'un recours contre des mesures qui auraient pris fin se pose légitimement.

Seule une procédure d'urgence, encadrée de garanties quant à l'absence de destruction des pièces dès la saisine de la CNCTR, pourrait constituer un recours effectif au sens de la CEDH.

2.3 L'instauration d'une question préjudicielle y compris en matière pénale lorsqu'est en cause le secret de la défense nationale

L'article L. 841-1 prévoit la saisine du Conseil d'État, à titre préjudiciel, par toute autorité judiciaire saisie d'une procédure ou d'un litige dont la solution dépend de l'examen de la régularité des techniques de renseignements dont la mise en œuvre est alléguée par l'une des parties, dès lors qu'est en cause le secret de défense nationale.

Il s'ensuit que la question préjudicielle s'impose tant au juge civil qu'au juge pénal.

Or, l'article 111-5 du code pénal dispose que *« les juridictions pénales sont compétentes pour interpréter les actes administratifs, réglementaires ou individuels et pour en apprécier la légalité lorsque, de cet examen, dépend la solution du procès pénal qui leur est soumis »*.

Le juge répressif peut donc se prononcer sur la validité de l'acte administratif dont dépend la solution du procès. Il n'a pas à renvoyer son examen au juge administratif.

Si l'USM peut comprendre que le secret de la défense nationale impose l'instauration de règles strictes pour l'efficacité de sa protection, elle s'étonne que le juge judiciaire soit totalement évincé, même en matière pénale et même en cas d'atteinte à la liberté individuelle, du dispositif de contrôle.

Un cadre tout aussi protecteur que celui prévu doit mis en place avec l'habilitation de certains magistrats de la Cour de cassation au secret défense.

3/ Le contentieux de la mise en œuvre des techniques de renseignement

Les affaires relevant de ce contentieux sont portées devant une formation particulière du Conseil d'État. Les membres de cette formation et le rapporteur public sont habilités ès-qualités 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.

Les membres de la formation de jugement et le rapporteur public sont autorisés à prendre connaissance de l'ensemble des pièces en possession de la Commission nationale de contrôle des techniques du renseignement ou des services concernés.

Ces dispositions n'appellent pas d'observations particulières.

Par contre l'article L.773-3 du code de justice administrative dispose que les exigences de la contradiction mentionnées à l'article L.5 sont adaptées à celles du secret de la défense nationale. Cette rédaction est insuffisamment précise. Il conviendrait de mentionner dans la loi elle-même les dérogations qui peuvent être faites au respect de ce principe essentiel de procédure.

La formation de jugement peut relever d'office tout moyen. Cette disposition doit être approuvée, elle doit néanmoins se concilier avec le respect du principe du contradictoire ce qui suppose que les parties soient appelées à présenter leurs observations écrites ou orales sur les moyens soulevés d'office par la formation de jugement.

Si l'USM comprend que le huis clos puisse être ordonné lorsqu'est en cause le secret de la défense nationale, elle considère que la décision doit être prise par la formation de jugement dans son ensemble et non par le seul président (L773-4 du code de la justice administrative).

Le projet de loi prévoit que la formation chargée de l'instruction entend les parties séparément, lorsqu'est en cause le secret de la défense nationale. Cette disposition destinée à la protection d'un secret qui ne saurait être partagé n'apparaît pas critiquable.

La commission nationale de contrôle des techniques de renseignement est informée de toute requête dont est saisie la formation particulière du Conseil d'État (L773-4). Cette commission doit être invitée à présenter, non pas *le cas échéant*, comme il est prévu, mais systématiquement et pour chaque procédure, des observations écrites ou orales.

Dès lors que la mise en œuvre des techniques de renseignement est enfermée dans un cadre légal, les recours sont destinés à sanctionner les irrégularités commises. Il n'apparaît donc pas choquant que lorsque la formation de jugement constate l'absence d'illégalité dans la mise en œuvre d'une technique de renseignement, la décision indique simplement au requérant qu'aucune illégalité n'a été commise, sans confirmer ni infirmer la mise en œuvre d'une telle technique.

Par contre, lorsque la formation de jugement constate qu'une technique de renseignement a été mise en œuvre ou exploitée illégalement, le projet de loi prévoit qu'elle *peut* annuler l'autorisation et ordonner, s'il y a lieu, la destruction des renseignements irrégulièrement collectés (L773-7). Cette rédaction doit être modifiée. Dès lors qu'une technique de renseignement a été mise en œuvre illégalement, les renseignements recueillis *doivent* être détruits et l'autorisation annulée.

Le projet de loi prévoit que la décision ne doit faire état d'aucun élément protégé par le secret de la défense nationale, ce qui peut être compris au regard des intérêts protégés. Elle informe simplement le requérant qu'une illégalité a été commise et peut, lorsqu'une demande en ce sens a été faite, condamner l'État à indemniser le requérant du préjudice qu'il a subi.

Il conviendrait de préciser que la décision devra en outre mentionner que la destruction des renseignements irrégulièrement collectés a été ordonnée.

Enfin, le projet de loi (L773-7 dernier alinéa) prévoit que lorsque la formation de jugement estime que l'illégalité constatée est susceptible de constituer une infraction, elle en avise le procureur de la République et transmet l'ensemble des éléments du dossier au vu duquel elle a statué à la commission consultative du secret de la défense nationale 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.

Il convient de préciser que l'avis de la commission consultative du secret de la défense nationale devra être transmis non seulement à la formation particulière du Conseil d'État mais également au procureur de la République dans le délai de 2 mois à compter de sa saisine.

III. Les techniques de renseignement mises en œuvre par les services : des techniques très larges, sans réel contrôle

L'article 2 traite des techniques de renseignement soumises à autorisation et prévoit une nouvelle classification des articles du code de la sécurité intérieure.

Les techniques de renseignement à la disposition des agents spécialisés sont nombreuses.

1. La procédure particulière applicable à l'accès administratif aux données de connexion

Les articles L246-1 et L246-2 du CSI deviennent respectivement les articles L851-1 et L851-2.

Le recueil des données de connexion (informatiques ou téléphoniques) est ainsi organisé : pour les finalités énumérées à l'article L811-3, « *peut être autorisé le recueil, auprès des opérateurs de communications électroniques (…), des informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications* ».

De manière dérogatoire aux règles fixées par le présent projet de loi, la demande est formulée par l'agent de renseignement habilité lui-même, et non par le ministre dont relève le service de renseignement de manière précise, écrite et motivée

Par ailleurs, l'autorisation n'est pas délivrée par le Premier ministre (ou l'une des 6 personnes spécialement déléguées par lui) après avis du président de la CNCTR. En effet, faute de suppression du point II de l'article L246-2 devenu L851-2, les demandes des agents restent soumises à la décision d'une personnalité qualifiée placée auprès du Premier Ministre, sans avis préalable.

L'USM s'étonne que cette personnalité qualifiée établisse un rapport d'activité annuel adressé à la CNCIS. Il s'agit visiblement d'un problème de rédaction de la loi. L'article L 246-2 est remplacé par l'article L. 851-2 sans modification de la référence à la CNCIS.

L'USM déplore ce régime dérogatoire au dispositif mis en place par le présent projet de loi. Une telle dérogation, moins contraignante, ne se justifie aucunement. A tout le moins, l'autorisation doit être délivrée par le Premier Ministre ou l'une des 6 personnes spécialement déléguée par lui, après avis de la CNCTR.

Pour les seuls besoins de la prévention du terrorisme, l'article L851-3 du CSI créé par le présent projet de loi prévoit que ces données de connexion sur les opérateurs puissent être recueillies en temps réel, et non pas sur demande. Ces dispositions sont mises en œuvre après avis de la CNCTR.

Par ailleurs, toujours pour les seuls besoins de la prévention du terrorisme, les agents de renseignement peuvent demander au Premier ministre (ou l'une des personnes déléguée par lui) l'autorisation, après avis de la CNCTR, d'imposer aux opérateurs « *la mise en œuvre sur les*

informations et documents traités par leurs réseaux d'un dispositif destiné à révéler, sur la seule base de traitements automatisés d'éléments anonymes, une menace terroriste » (L851-4).

« *Si une telle menace est ainsi révélée, le Premier ministre ou l'une des personnes déléguées par lui peut décider de la levée de l'anonymat sur les données, informations et documents afférents* » après avis de la CNCTR, non nécessaire en cas d'urgence absolue. La mise en œuvre d'autres techniques de renseignement serait alors possible.

Ici encore, la demande peut être formulée par les agents eux-mêmes, sans qu'il soit fait référence au formalisme de demande d'utilisation prévu par l'article L821-2 du CSI.

La presse a évoqué la notion de « boite noire » installée sur les équipements des opérateurs télécoms : des algorithmes viseraient à détecter des possibles suspects terroristes au cœur des données internet.

Ces deux techniques (recueil des données de connexion en temps réel et utilisation d'algorithmes) pourraient être mises en œuvre auprès des opérateurs télécoms et viser également les communications sur Facebook, Google ou Skype.

Le dispositif légal proposé ne permet pas un contrôle suffisant, s'agissant de techniques à visée générale, portant atteinte aux libertés individuelles de nombreuses personnes, indistinctement et simultanément.

Dès lors que de telles mesures sont vouées à assurer la surveillance de personnes soupçonnées de terrorisme, l'ouverture d'une enquête judiciaire apparaît nécessaire. Tel est particulièrement le cas lorsqu'une *« menace de terrorisme est révélée* ». L'USM déplore que le contrôle de l'autorité judiciaire soit ainsi écarté.

En tout état de cause, il est essentiel que de telles mesures gravement attentatoires aux libertés soient strictement limitées à la prévention du terrorisme, à l'exclusion de toute autre infraction.

Pour ces deux techniques, l'article L851-5 du CSI créé prévoit que l'autorisation est accordée pour une durée maximale de 30 jours, et peut être renouvelée dans les mêmes conditions de forme et de durée.

L'USM sollicite qu'un compte-rendu de l'utilisation de ces techniques soit envisagé préalablement à toute demande de renouvellement, afin de permettre un avis plus éclairé de la CNCTR et du Premier ministre, comme c'est d'ailleurs le cas dans un cadre judiciaire.

2. Les interceptions de sécurité (écoutes téléphoniques administratives)

L'article L852-1 du CSI selon le projet prévoit la possibilité des « *interceptions de correspondances émises par la voie des communications électroniques et susceptibles de révéler des renseignements entrant dans les finalités mentionnées à l'article L811-3* ».

Ajoutant au dispositif actuellement en vigueur, le projet de loi prévoit que « *lorsqu'une ou plusieurs personnes appartenant à l'entourage de la personne visée par l'autorisation sont susceptibles de jouer un rôle d'intermédiaire, volontaire ou non, pour le compte de celle-ci ou de fournir des informations au titre de la finalité faisant l'objet de l'autorisation, celle-ci peut être accordée également pour ces personnes* ».

Il s'agit ici de permettre le placement sous écoute des proches d'une personne, au motif que celle-ci pourrait utiliser le téléphone de ce proche. Cette mesure, particulièrement intrusive, vise à contourner la jurisprudence de la CNCIS qui exige la mise en évidence d'un lien direct entre la personne placée sur écoute et l'intérêt à protéger.

L'USM estime que cette mesure ne peut s'envisager que dans les hypothèses les plus graves, telles que la prévention des actes de terrorisme, et serait inadmissible dans les autres hypothèses.

Cette question renvoie une nouvelle fois à celle des pouvoirs dévolus à la CNCTR et à l'efficience du contrôle exercé par cette commission.

Les alinéas suivants de l'article L852-1 reprennent les dispositions déjà existantes en matière d'interceptions de sécurité. L'USM n'a pas d'observations autres que celles qu'elle a déjà développées.

3. les dispositifs mobiles de proximité (IMSI-catchers)

L'article L851-7 prévoit la possibilité d'utiliser un dispositif technique de proximité pour la prévention de l'ensemble des atteintes aux intérêts publics visés à l'article L811-3 pour recueillir :

- les données techniques de connexion strictement nécessaires à l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur ;
- les données techniques relatives à la localisation des équipements terminaux utilisés.

L'autorisation est donnée par le Premier ministre, après avis du président de la CNCTR, dont il peut s'affranchir.

L'autorisation peut également être accordée à « un service et porter sur des lieux et une période déterminés », dans la limite de 6 mois. En ce cas, l'autorisation du Premier Ministre doit être spécialement motivée et prise sur l'avis exprès (et non « conforme ») de la CNCTR.

Il s'agit de l'utilisation du dispositif « IMSI Catcher », qui permet, selon la CNIL, « *de placer une fausse antenne relais à proximité de la personne dont on souhaite intercepter les échanges électroniques, afin de capter les données transmises entre le périphérique électronique et la véritable antenne relais* ». Seront également captées automatiquement, systématiquement et indistinctement les données des individus à proximité du dispositif, compte tenu de la portée de cette fausse antenne et de l'impossibilité technique de cibler un appareil précisément pour capter ses données.

Dans son avis rendu le 5 mars 2015 sur le projet de loi, la CNIL relève qu'il ne « *s'agit plus seulement d'accéder aux données utiles concernant une personne identifiée comme devant faire l'objet d'une surveillance particulière, mais de permettre de collecter, de manière indifférenciée, un volume important de données qui peuvent être relatives à des personnes tout à fait étrangères à la mission de renseignement (...) ce changement a des conséquences particulièrement graves sur la protection de la vie privée et des données personnelles. De telles mesures doivent dès lors être assorties de conditions de mise en œuvre plus précises et de nature à limiter les atteintes à ces droits fondamentaux, d'une part, et de modalités de contrôle effectives et adaptées à la nature de ces atteintes d'autre part. A cet égard, la Commission est particulièrement réservée sur l'application d'un seul régime d'autorisation (sonde et « signaux faibles ») et de la seule*

information du Premier Ministre et de la CNCTR s'agissant des IMSI Catcher. Si le contrôle de la CNCTR a toute sa pertinence pour le recours à des techniques ciblées sur des personnes préalablement identifiées, la commission estime que sa portée se trouve très fortement atténuée dans le cadre des techniques permettant la collecte d'informations de manière indifférenciée ».

Le fait que l'utilisation d'un tel dispositif soit subordonnée à son inscription dans un registre spécial tenu à la disposition de la CNCTR et ne puisse être mise en œuvre que par un agent individuellement désigné et dûment habilité n'est pas suffisamment protecteur des libertés individuelles.

Pour l'USM, ces dispositions sont de nature à porter atteinte aux libertés individuelles de nombre d'individus sans lien avec les personnes visées par le renseignement et doivent donc pouvoir n'être utilisées que dans des cas très limités, et non dans l'ensemble des cas visés par l'article L811-3 du CSI.

Aussi, à défaut d'un contrôle par l'autorité judiciaire, il est impératif que l'avis de la CNCTR, préalable à la décision du Premier ministre, doive lier celui-ci.

Enfin, la durée de 6 mois prévue pour autoriser l'utilisation de ce système par un service sur des lieux et une période déterminés est trop longue. Au regard de la gravité de l'atteinte aux libertés induite par un tel dispositif, une réduction drastique de cette durée doit être prévue.

Pour la prévention d'un acte de terrorisme, l'article L851-7 III prévoit la mise en œuvre de ce dispositif pour intercepter directement des correspondances émises ou reçues par un équipement terminal (téléphone ou internet), pour la durée strictement nécessaire. L'autorisation est donnée dans la limite de 72 heures, renouvelables.

Un strict contrôle préalable doit être instauré, ici encore, s'agissant de l'interception des correspondances non seulement des individus surveillés dans le cadre de la prévention du terrorisme mais également de toutes les personnes qui se trouveraient géographiquement à proximité.

Comme pour la géolocalisation (ci-dessous), l'article L851-7 IV prévoit qu'en cas d'urgence liée à une menace imminente ou à un risque très élevé de ne pouvoir effectuer l'opération ultérieurement, le dispositif d'IMSI Catcher puisse être mis en œuvre sans autorisation préalable. Le Premier ministre et la CNCTR doivent alors informer sans délai et le Premier Ministre peut alors donner son autorisation dans un délai de 48 heures.

L'USM s'oppose à de telles dispositions, dès lors que la définition de l'urgence est trop large et le délai laissé au Premier ministre pour prendre sa décision trop long. Un tel dispositif, attentatoire au secret des correspondances et à la vie privée de nombreuses personnes simultanément et indistinctement, ne peut être mis en œuvre que dans des situations particulièrement exceptionnelles, après autorisation expresse de l'autorité judiciaire.

L'USM regrette que le projet de texte ne prévoie pas de dispositions relatives à la procédure de suivi des demandes et des conditions et durée de conservation des informations ou documents transmis. L'article L851-9 du CSI, reprenant les dispositions de l'article L246-4 alinéa 2 du CSI,

renvoie en effet à un décret en Conseil d'Etat pour fixer les modalités d'application de ces dispositifs de renseignement.

4. la géolocalisation

L'article L851-6 créé par le projet de loi permet la géolocalisation en temps réel d'une personne, d'un véhicule ou d'un objet, dans tous les cas prévus par l'article L811-3 du CSI, sur simple autorisation du premier ministre, après avis du président de la CNCTR, avis qui ne le lie pas.

L'USM s'insurge contre la possibilité de mise en œuvre d'une telle technique, dans des conditions aussi larges.

L'USM rappelle que deux arrêts de la Cour de Cassation du 22 octobre 2013 se fondant sur l'article 8 de la CEDH ont entraîné l'adoption en urgence d'une loi sur la géolocalisation dans un cadre judiciaire début 2014.

La loi du 28 mars 2014 a limité l'utilisation de la géolocalisation à certaines enquêtes (1° Enquête ou instruction relative à un délit prévu au livre II ou aux articles 434-6 et 434-27 du code pénal, puni d'un emprisonnement d'au moins trois ans ; 2° Enquête ou instruction relative à un crime ou à un délit, à l'exception de ceux mentionnés au 1° du présent article, puni d'un emprisonnement d'au moins cinq ans ; 3° procédure d'enquête ou d'instruction de recherche des causes de la mort ou de la disparition prévue aux articles 74, 74-1 et 80-4 ; 4° procédure de recherche d'une personne en fuite prévue à l'article 74-2).

Cette loi du 28 mars 2014 prévoit, dans le cadre d'une enquête de flagrance ou préliminaire, l'autorisation préalable du procureur de la République pour une durée maximale de 15 jours consécutifs, à l'issue desquels l'autorisation du JLD est nécessaire pour une durée d'un mois renouvelable, et dans le cadre d'une instruction, une autorisation par le juge d'instruction pour une durée maximale de 4 mois renouvelables.

Alors que les conditions de mise en œuvre de la géolocalisation sont particulièrement encadrées dans un cadre judiciaire, lorsque des indices permettent de soupçonner l'existence d'une infraction, l'absence totale de réel contrôle de la géolocalisation administrative est extrêmement préoccupante.

En réalité, cette technique pourra être utilisée, sur simple autorisation du premier ministre, après avis non obligatoire de la CNCTR, pour localiser en temps réel un chercheur si le gouvernement estime que les intérêts scientifiques essentiels de la France sont en jeu.

L'USM est donc particulièrement hostile à ces dispositions.

En cas d'urgence liée à une menace imminente ou à un risque très élevé de ne pouvoir effectuer l'opération ultérieurement, le dispositif apparaît, plus encore, attentatoire aux libertés individuelles.

En effet, dans ces conditions, alternatives et non cumulatives, l'article L851-6 alinéa 2 du CSI prévoit que la géolocalisation pourra être mise en œuvre sans autorisation préalable. Sont seulement prévues une information sans délai du Premier ministre et de la CNCTR et une autorisation du Premier Ministre dans les 48 heures. A défaut d'autorisation, la destruction des renseignements collectés serait ordonnée.

Ici encore, les dispositions légales sont insuffisamment protectrices des libertés individuelles. Dans l'ensemble des cas visés à l'article L811-3, si les agents de renseignements estiment que le risque de ne pouvoir mettre en œuvre la géolocalisation ultérieurement est très élevé, ils pourront s'affranchir de toute autorisation pendant 48 heures.

L'USM rappelle que dans le cas des enquêtes judiciaires, les conditions permettant la géolocalisation sans autorisation préalable en cas d'urgence sont infiniment plus strictes et pour une durée plus limitée. L'article 230-35 du code de procédure pénale exige une urgence « *résultant d'un risque imminent de dépérissement des preuves ou d'atteinte grave aux personnes ou aux biens* ». L'OPJ doit alors informer « *immédiatement, par tout moyen* », le procureur de la République ou le juge d'instruction qui peut ordonner mainlevée de la géolocalisation.

Par ailleurs, l'article L853-2 prévoit, lorsque les renseignements relatifs aux finalités prévues à l'article L. 811-3 ne peuvent être recueillis par un autre moyen légalement autorisé, la possibilité de s'introduire dans un véhicule ou dans un lieu privé à la seule fin de mettre en place, d'utiliser ou de retirer les dispositifs de géolocalisation.

Dans un cadre judiciaire, des conditions strictes sont posées, puisqu'une autorisation écrite du Procureur ou du juge d'instruction est nécessaire, que la procédure est différente selon le quantum de la peine encourue pour l'infraction et qu'un contrôle renforcé est prévu lorsque l'introduction est envisagé dans un lieu d'habitation (une autorisation du JLD est alors nécessaire).

L'absence de distinction du contrôle selon l'intérêt public protégé ou le lieu privé dans lequel l'introduction est nécessaire est particulièrement problématique.

Surtout, le rôle de la CNCTR est très insuffisamment renforcé en la matière.

En effet, l'article L853-2 prévoit que :

- l'autorisation du Premier ministre doit être spécialement motivée,
- cette autorisation ne peut être accordée que sur avis exprès de la CNCTR,
- lorsque l'avis n'est pas rendu par le Président de la commission mais par un membre désigné par lui, celui-ci ne peut être que l'un des membres issus de la cour de cassation ou du conseil d'Etat
- l'autorisation est accordée pour une durée maximale de 30 jours, renouvelable dans les mêmes conditions de forme et de durée que l'autorisation initiale
- le dispositif est mis en œuvre sous le contrôle de la CNCTR, à laquelle le service rend compte, et qui peut à tout moment demander l'interruption du dispositif et la destruction des éléments collectées
- lorsque la modalité a été autorisée après avis défavorable de la CNCTR ou que le premier ministre n'a pas donné suite à ses recommandations, le Conseil d'Etat est saisi à la demande d'au moins deux membres de la Commission.

Ce renforcement n'est que de façade puisque selon le dernier alinéa de cet article L853-2, lorsque l'autorisation ne concerne pas un lieu privé à usage d'habitation, et en cas « d'urgence absolue » l'autorisation peut être délivrée sans avis préalable de la commission.

Malgré l'apparence de contrôle renforcé, l'USM déplore que :

- L'avis de la CNCTR ne lie pas le Premier ministre.

- L'avis de la CNCTR puisse être rendu par un seul de ses membres. Une délibération collégiale doit être prévue.
- L'autorisation soit accordée pour une durée assez longue. S'agissant d'un dispositif particulièrement attentatoire au secret des correspondances et à la vie privée, une durée très courte doit être prévue.
- Aucun compte rendu du résultat des investigations ne soit nécessaire avant d'envisager le renouvellement du dispositif.
- La juridiction de recours ne soit pas automatiquement saisie si le Premier ministre n'a pas suivi une recommandation de la CNCTR ou a autorisé le dispositif contre l'avis de la commission.
- Le Premier ministre puisse prendre une décision sans le moindre avis préalable en cas d'urgence absolue. La notion d'urgence absolue est extrêmement large et devrait être très strictement précisée.

Il est inconcevable que les dispositions permettant une géolocalisation par des agents de renseignement, en dehors de toute infraction soupçonnée, soient particulièrement moins protectrices des libertés individuelles que celles applicables à la géolocalisation judiciaire.

5. l'enregistrement des paroles ou images d'une personne et la captation de ses données informatiques

L'article L853-1 autorise l'utilisation de dispositifs techniques permettant :

- la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel, ou d'images dans un lieu privé.

- la captation, la transmission et l'enregistrement de données informatiques transitant par un système automatisé de données ou contenues dans un tel système.

Il s'agit ainsi de permettre d'écouter et enregistrer des conversations, de prendre des photos y compris dans des lieux privés et de capter les consultations de sites internet....

Le texte fixe une condition préalable à l'autorisation d'utiliser ces techniques : les renseignements relatifs aux finalités prévues à l'article L811-3 ne doivent pas pouvoir être recueillis par un autre moyen légalement autorisé.

Si cette condition est évidemment importante, elle ne paraît pas suffisante, au regard du caractère trop large des domaines d'application possible de ces techniques et toujours faute de réel contrôle préalable.

Par dérogations aux règles générales fixées par le projet de loi, l'autorisation n'est pas délivrée pour une durée de 4 mois mais pour une durée de 2 mois, renouvelable.

L'article L853-2 permet, lorsque les renseignements relatifs aux finalités prévues à l'article L. 811-3 ne peuvent être recueillis par un autre moyen légalement autorisé, la possibilité de s'introduire dans un véhicule ou dans un lieu privé à la seule fin de mettre en place, d'utiliser ou de retirer les dispositifs (micro, caméra).

Il permet également, pour la captation, la transmission et l'enregistrement de données informatiques transitant par un système automatisé de données ou contenues dans un tel système, et « l*orsque 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 concrètement de permettre l'introduction directement dans les opérations informatiques en cours, par exemple dans une discussion par « chat »...

L'absence de distinction des modalités du contrôle selon l'intérêt public protégé, le lieu privé dans lequel l'introduction est nécessaire, ou l'introduction dans un système informatique est particulièrement problématique.

Surtout, le rôle de la CNCTR est certes renforcé, mais de manière insuffisante.

En effet, l'article L853-2 prévoit que :

- l'autorisation du Premier ministre doit être spécialement motivée
- cette autorisation ne peut être accordée que sur avis exprès de la CNCTR
- lorsque l'avis n'est pas rendu par le Président de la commission mais par un membre désigné par lui, celui-ci ne peut être que l'un des membres issus de la cour de cassation ou du conseil d'Etat
- l'autorisation est accordée pour une durée maximale de 30 jours, renouvelable dans les mêmes conditions de forme et de durée que l'autorisation initiale.
- le dispositif est mis en œuvre sous le contrôle de la CNCTR, à laquelle le service rend compte, et qui peut à tout moment demander l'interruption du dispositif et la destruction des éléments collectées
- lorsque la modalité a été autorisée après avis défavorable de la CNCTR ou que le premier ministre n'a pas donné suite à ses recommandations, le Conseil d'Etat est saisi à la demande d'au moins deux membres de la Commission.

Ce renforcement n'est que de façade puisque selon le dernier alinéa de cet article L853-2, lorsque l'autorisation ne concerne pas un lieu privé à usage d'habitation, et en cas « d'urgence absolue » l'autorisation peut être délivrée sans avis préalable de la commission.

Malgré l'apparence de contrôle renforcé, l'USM déplore que :

- L'avis de la CNCTR ne lie pas le Premier ministre.
- L'avis de la CNCTR puisse être rendu par un seul de ses membres. Une délibération collégiale doit être prévue.
- L'autorisation soit accordée pour une durée assez longue. S'agissant d'un dispositif particulièrement attentatoire au secret des correspondances et à la vie privée, une durée très courte doit être prévue.
- Aucun compte-rendu du résultat des investigations ne soit nécessaire avant d'envisager le renouvellement du dispositif.
- La juridiction de recours ne soit pas automatiquement saisie si le Premier ministre n'a pas suivi une recommandation de la CNCTR ou a autorisé le dispositif contre l'avis de la commission.
- le Premier ministre puisse prendre une décision sans le moindre avis préalable en cas d'urgence absolue. La notion d'urgence absolue doit être strictement précisée.

6. les interceptions de communications électroniques émises ou reçues de l'étranger : une absence totale de contrôle

L'article L854-1 I issu du projet de loi régit les mesures prises pour assurer la surveillance et le contrôle des transmissions émises ou reçues à l'étranger.

Le projet de loi se limite à prévoir que l'interception des communications et l'exploitation qui pourrait en être faite sont soumises à autorisation du Premier ministre.

Le texte renvoie à des décrets en Conseil d'Etat pour préciser les modalités de mise en œuvre de la surveillance (décret qui ne serait pas publié), définir les conditions d'exploitation de conservation et de destruction des renseignements collectés et préciser la procédure de délivrance des autorisations d'exploitation des correspondances. Tout juste précise-t-il que ce décret en Conseil d'Etat sera pris après avis de la CNCTR.

L'article L854-1 II prévoit les modalités de conservation et de destruction des communications, sous le contrôle de la CNCTR, lorsque ces communications « renvoient à des numéros d'abonnement ou à des identifiants techniques rattachables au territoire national ». Ces modalités seront celles prévues aux articles L822-2 à L822-4.

L'article L854-1 III prévoit la compétence de la CNCTR, sur réclamation de toute personne y ayant un intérêt ou sa propre initiative, pour s'assurer que les techniques de renseignement respectent les conditions fixées, en faire rapport au premier ministre (qui répond dans les 15 jours).

Ainsi, le projet de loi n'apporte aucune précision quant aux modalités de contrôle des interceptions de communications électroniques dès lors qu'elles auront été émises ou reçues de l'étranger.

Il résulte donc de cet article une absence totale de contrôle des dispositifs de renseignement en la matière. Pire, est légalisée l'absence totale de garanties, même minimales, et de contrôle.

L'USM s'insurge sur ces dispositions qui ne répondent absolument pas aux règles de prévisibilité de la loi ni à la nécessaire protection des libertés individuelles.

IV. Dispositions particulières (surveillance des détenus, protection des agents, extension des pouvoirs de Tracfin), et recodification

1. La surveillance des détenus

L'article 12 relatif à la surveillance des détenus introduit deux nouveaux articles dans le code de procédure pénale.

L'article 727-2 permet à l'administration pénitentiaire de disposer des prérogatives nécessaires à la détection, au brouillage et à l'interruption des correspondances illicites émises ou reçues par la voie des communications électroniques ou radioélectriques par une personne détenue, notamment les communications téléphoniques, les échanges de messages écrits ainsi que des communications par talkie-walkie.

Cet article autorise également l'administration pénitentiaire à utiliser un dispositif permettant de recueillir les données de connexion ou celles relatives à la géolocalisation des équipements utilisés.

La miniaturisation constante des matériels de téléphonie, combinée à l'allègement imposé des fouilles effectuées par les personnels de l'administration pénitentiaire sur le détenu et sa famille lors des parloirs, ont conduit à une augmentation sensible du nombre de téléphones portables illicitement introduits en maison d'arrêt ou en centre de détention, étant précisé que ces téléphones disposent le plus souvent de connexion internet.

La mise en œuvre de dispositifs techniques de nature à rendre inutilisables les matériels introduits illicitement en maisons d'arrêt ne peut que satisfaire l'USM.

Une réflexion quant à la tarification faite aux détenus lors de l'utilisation des téléphones fixes mis à leur disposition par l'administration pénitentiaire pourrait aussi être utile. En effet, nombre de détenus sanctionnés disciplinairement ou pénalement pour avoir détenu ces appareils de communications illicites en milieu carcéral justifient cette détention au regard de considération purement économiques. Dans les établissements pour exécution de peine, l'accès aux téléphones fixes est permis, contrairement aux maisons d'arrêt dans le cadre de la détention provisoire.

Le second paragraphe du projet d'article 727-2 du code de procédure pénale dispose que, sous le contrôle du Procureur de la République territorialement compétent, l'administration pénitentiaire pourrait recueillir les données techniques de connexion des équipements terminaux utilisés et procéder à leur localisation.

L'introduction en milieu carcéral d'objets illicites, en particulier de matériels de téléphonie, est constitutif d'une infraction pénale tant pour la personne qui introduit l'objet que pour le détenu qui les reçoit. Ce dernier, sans préjudice de sanctions disciplinaires, peut être poursuivi en qualité de complice d'introduction ou de receleur de l'objet illicitement introduit.

Cette possession illicite des équipements terminaux, notamment de téléphones portables, en ce qu'elle permet à elle seule la constatation des infractions précédemment évoquées, relève déjà du dispositif général de la géolocalisation active prévue par les articles 230-32 du code de procédure pénale.

Le dispositif actuel est garant des libertés individuelles en ce que la mise en œuvre du dispositif de géolocalisation prévoit, non pas un simple contrôle du procureur de la république, mais une autorisation préalable. Cette autorisation est valable 15 jours consécutifs, pouvant le cas échéant être prolongée par le juge des libertés et de la détention pour une durée d'un mois renouvelable.

L'opération de géolocalisation est donc conduite sous le contrôle du magistrat qui l'a ordonné ou renouvelée (article 230-37).

Force est de constater que le projet de texte envisagé aurait pour effet de mettre en place un régime dérogatoire de géolocalisation des terminaux de communication possédés par les détenus, régime dérogatoire que rien ne justifie.

Il serait d'ailleurs surprenant que le régime mis en œuvre pour géolocaliser le téléphone portable d'une personne recherchée pour avoir commis un crime soit plus protecteur que pour un détenu détenant un téléphone portable illégalement dans sa cellule sans avoir commis d'autres infractions.

L'amélioration des textes existants en la matière est cependant souhaitable. Il serait ainsi possible d'étendre la liste des lieux pour lesquels une autorisation peut être donnée pour mettre en place ou retirer un moyen technique de localisation en temps réel, liste prévue par l'article 230-4 du Code de procédure pénale, en y ajoutant les lieux de détention.

L'article 727-3 issu du projet de loi permettrait sous le contrôle du parquet d'accéder aux données informatiques contenues dans les systèmes de traitement automatisé de données que possèdent illicitement les personnes détenues.

Là encore, si des terminaux illicites sont découverts, les OPJ, sur autorisation du parquet, peuvent déjà faire toutes les réquisitions utiles permettant d'accéder aux données informatiques et détecter toute connexion à un réseau non autorisé.

Si cet article, dont la plus-value est incertaine, avait vocation à demeurer, il conviendrait donc de l'améliorer en instaurant un accord préalable du parquet pour la mise en œuvre des techniques d'accès aux données et non un simple contrôle *a posteriori*.

Le projet d'article 727-3 du code de procédure pénale permettrait enfin une possible rétention du matériel illicite jusqu'à son éventuelle restitution au détenu au moment de sa libération.

Il semble préférable de prévoir que, de manière systématique, s'agissant d'objets irrégulièrement introduits dans des lieux de détention, lesdits objets soient systématiquement confisqués, comme c'est actuellement le cas.

2. La protection des agents :

2.1 : renforcement de leur anonymat

L'USM n'a pas d'objection à faire valoir sur ces dispositions.

2.2 : exonération de poursuites pénales

L'article 10 du projet de loi prévoit que les dispositions pénales réprimant les atteintes aux systèmes de traitement automatisé de données ne sont pas applicables aux mesures mises en œuvre pour assurer hors du territoire national la protection des intérêts mentionnés à l'article L811-3 du CSI par les agents habilités.

Sous réserve de la mise en place de dispositifs réels de contrôles préalablement à la mise en œuvre des techniques de renseignement, l'USM n'a pas d'observations particulières sur ce point.

3. Renforcement des pouvoirs de TRACFIN

Il s'agit de confier à TRACFIN des prérogatives dont disposent les autres services de renseignements (accès aux fichiers voyageurs des compagnies aériennes) et qui paraissent nécessaires au plein exercice de ses missions.

L'USM n'a donc pas d'objection à faire valoir sur ces dispositions.

4. Dispositions diverses et recodification

Les articles 5, 6, 7, 8, 11, 13, 14, 15, 16 correspondants à des mesures de recodification ou d'adaptation, l'USM n'a pas d'observation à formuler.