

Paris, le 1^{er} avril 2015

12-14 rue Charles Fourier

75013 PARIS

Tel 01 48 05 47 88

Fax 01 47 00 16 05

Mail : contact@syndicat-magistrature.org

site : www.syndicat-magistrature.org

Observations sur le projet de loi « *relatif au renseignement* » présenté en conseil des ministres

Le projet de loi relatif au renseignement est présenté comme répondant au double objectif d'améliorer la détection des menaces pesant sur la sécurité nationale, en particulier terroristes, et de garantir un cadre juridique protecteur des libertés individuelles, à la mise en œuvre des techniques de renseignement. Il prétend mettre en conformité la France avec les standards démocratiques en la matière, par la constitution d'un cadre normatif équilibré entre performance des services spéciaux, assurant la sécurité des citoyens, et effectivité du contrôle, protégeant leur vie privée et leurs libertés. C'est pourtant bien plus à la reconnaissance de pouvoirs accrus pour les services qu'à la protection des libertés des citoyens que s'atèle ce projet, ainsi qu'en témoigne son exposé des motifs.

Depuis l'arrêt Klass contre Allemagne de 1978, la jurisprudence européenne rappelle aux États qu'ils ne disposent pas d'une latitude illimitée pour assujettir à des mesures de surveillance secrète les personnes soumises à leur juridiction et prendre « n'importe quelle mesure jugée par eux appropriée », sous peine « de saper, voire de détruire, la démocratie au motif de la défendre », la défense de l'Etat de droit ne pouvant se passer d'un examen attentif des moyens choisis.

Alors que cette logique devrait prévaloir et placer au cœur du débat démocratique la protection des individus contre les abus de la puissance publique, car tel est le sens de la notion de sûreté telle que conçue par les rédacteurs de la Déclaration des droits de l'homme et du citoyen de 1789, c'est d'abord à la protection des agents des services de renseignement que ce texte œuvre. Alors que les citoyens sont, en matière de renseignement, les cibles potentielles de la surveillance étatique, la garantie de leurs libertés n'est que secondairement l'objet de ce texte. Le renversement des principes est aussi choquant que fièrement assumé. C'est ainsi que l'exposé des motifs pose d'abord que « les agents des services spécialisés de renseignement (...)

demeurent exposés à des risques pénaux injustifiés. En deuxième lieu, l'absence de règles claires (...) favorise les suspicions infondées sur l'activité des services spécialisés et fragilise leur action ». Sans ciller, le gouvernement offre un blanc-seing à des services au moment même où il présente un texte dont l'objet rappelle à lui seul combien ils fonctionnent depuis plusieurs années dans la plus grande illégalité... La protection des libertés de tout un chacun n'est visée qu'enfin : « en troisième lieu, l'insuffisance de la loi limite l'étendue du contrôle exercé sur les services spécialisés : ce qui n'a pas de fondement légal n'a pas de contrôle organisé, ce qui n'est pas acceptable dans une société démocratique attachée à la protection des libertés constitutionnellement garanties. »

Cet ordre des priorités constitue une juste présentation du texte, dont les dispositions combinées légalisent tout un panel de techniques de surveillance, certaines préexistantes « notamment en matière d'interceptions des correspondances et d'accès administratif aux données de connexion », d'autres nouvelles « notamment en ce qui concerne certaines techniques de sonorisation de lieux, de captation de données ou de localisation en temps réel d'objets ou de personnes ». Voilà l'objet réel de ce texte : légaliser au profit de services au fonctionnement par essence occulte des prérogatives très larges, permettant une surveillance étendue et renforcée dans l'espace virtuel et dans l'espace physique, tout en organisant un système de contrôle a priori dérisoire et a posteriori illusoire. Le président de la CNCIS, M. Delarue, la CNIL, le Conseil national du numérique ou le commissaire aux droits de l'homme du Conseil de l'Europe ne s'y sont pas trompés et expriment aujourd'hui leurs vives inquiétudes.

La cause des services du renseignement n'était pas absente du débat politique : la loi de 1991 sur les interceptions de sécurité a initié une dynamique en réponse aux exigences de la Cour européenne des droits de l'Homme. Les lois qui ont suivi ont systématiquement eu pour effet ou pour objet, d'abord de réorganiser les services spécialisés, puis d'accroître leurs pouvoirs. Les derniers textes adoptés, loi de programmation militaire du 18 décembre 2013 (et son article 20) et la loi du 13 novembre 2014 ont ainsi, au prétexte d'une nécessaire adaptation aux nouvelles technologies comme aux nouvelles menaces, ouvert un cycle de renforcement des pouvoirs du renseignement.

Le législateur a fait le choix du contre-pied : traditionnellement désignés avec méfiance par une classe politique qui voit dans les services des renseignements une menace potentielle, ceux-ci sont aujourd'hui entièrement dédouanés, les dérives anciennes ou récentes oubliées. Un postulat pourtant dangereux au stade du processus législatif : si la défiance totale ne saurait être la règle, il appartient néanmoins en cette matière de déployer la plus grande vigilance. Gérard Soulier souligne, dans l'ouvrage Raisonner la raison

d'Etat coordonné par Mireille Delmas Marty, combien il est fondamental que les dérives potentielles des services ne soient pas écartées des débats démocratiques. S'il importe selon lui de ne pas empêcher de manière absolue les mesures de surveillance, mais bien de « les reconnaître, les réglementer, en limitant les possibilités et en organisant un contrôle », il faut se garder de « s'en remettre finalement à une pratique correcte des agents de l'Etat, lorsque c'est d'eux justement que l'on peut redouter un glissement vers les méthodes de l'Etat policier ».

Alors qu'aux termes mêmes de l'exposé des motifs du projet de loi, la prégnance des enjeux soulevés par le renseignement appelle un « consensus social exprimé par la représentation nationale », qui devrait naturellement se traduire par un examen approfondi du texte par les assemblées, le gouvernement choisit de soumettre le texte aux parlementaires selon la procédure d'urgence, au prétexte que le temps serait compté dans la lutte contre le terrorisme. Ce, malgré les nombreux textes ayant affiché cet objectif au cours des 18 derniers mois, et surtout, en dépit de l'irréductibilité du projet à la lutte contre le terrorisme. Ni les citoyens, ni les parlementaires ne doivent s'y tromper : ce projet concerne la surveillance, bien au-delà de la lutte anti-terroriste. Porteur d'une vision globale du renseignement, enraciné dans une réflexion de longue haleine, ce texte méritait assurément un examen approfondi, seul à même de créer les conditions d'un débat serein, s'agissant de la protection des libertés individuelles. C'est hélas la procédure accélérée qui a été choisie. Le fond répond ainsi à la forme : pour une loi au contenu restrictif de libertés et corrodant les conditions d'existence de la démocratie, une procédure antidémocratique.

Malgré le consensus politique en faveur de l'adoption de ce texte, chacun se réfugiant derrière l'argument sécuritaire, le Syndicat de la magistrature ne se résigne pas. Il dénonce l'extension du champ des activités de renseignement et la légalisation de techniques de surveillance intrusives (I) sans contre-pouvoir réel, le contrôle organisé étant aussi dérisoire a priori qu'illusoire a posteriori (II)

I. Une extension dangereuse du champ d'action et des pouvoirs du renseignement

A. Un champ d'intervention des activités de renseignement toujours plus étendu

1. les dangers d'une définition large

La vocation annoncée de ce texte à constituer une grande loi sur le renseignement trouve son expression dans la définition de principes

directeurs du fonctionnement des services de renseignement, des missions qui leur sont confiées mais également des motifs pouvant justifier le recours à des techniques policières intrusives. Ce souci de définir plus clairement des missions de services agissant par principe dans l'opacité peut paraître louable. L'exposé des motifs évoque ainsi la double fonction de « connaissance et d'anticipation », constituant le cœur de l'activité des services spécialisés, et entend définir les contours de cette mission. Mais la définition extensive des finalités du renseignement adoptée dès l'article 1 du projet contrevient évidemment à l'objectif affiché d'un meilleur encadrement de l'activité de ces services.

Le renseignement n'est une activité légitime que si elle se borne à la collecte d'information dans un domaine strictement défini comme ayant trait à la sécurité nationale à l'exclusion de toute dimension susceptible d'en faire un instrument politique placé entre les mains du gouvernement. Cette exigence s'impose d'autant plus lorsque ces services se voient dotés de pouvoirs particulièrement intrusifs, susceptibles de porter une atteinte grave aux libertés de l'ensemble des citoyens. Le projet de loi crée un article L 811-3 du code de la sécurité intérieure qui liste les « intérêts publics » pouvant fonder l'usage de pouvoirs de police exorbitants. Loin de reprendre les motifs énoncés à l'article L241-2 du code de la sécurité intérieure régissant actuellement le recours aux interceptions de sécurité, le projet de loi adopte une vision dangereusement extensive, par l'adjonction de motifs supplémentaires et de rédactions nouvelles de missions anciennes. Cette nouvelle définition est loin d'être anodine.

Les intérêts publics listés pèchent d'abord par leur définition vague et les contradictions qui peuvent les traverser. C'est le cas des « intérêts économiques et scientifiques essentiels de la France » et des « intérêts essentiels de la politique étrangère et l'exécution des engagements internationaux de la France ». Dans ce cadre flou, confier aux services des pouvoirs intrusifs à des fins de collecte d'information mais aussi d' « entrave des menaces et des risques » pour la protection de ces intérêts n'est pas anodin. En effet, c'est de permettre à la puissance publique de contrer ou de déstabiliser en secret des actions, qui peuvent être tout aussi contraires aux intérêts économiques ou de politique étrangère que vitales dans une démocratie : il en est ainsi des actions visant à mettre à jour les pratiques illégales ou amORALES d'entreprises nationales (de l'énergie, la distribution de l'eau, les nouvelles technologies ou l'armement...) ou à contester des choix de politique étrangère. À défaut de protection réelle des lanceurs d'alerte, la reconnaissance extensive de pouvoirs au profit des services spécialisés dans ces domaines, qui va de pair avec la volonté de sanctuariser le secret des affaires et le secret de la défense nationale, est préoccupante.

Le maintien de la prévention de la criminalité et de la délinquance organisée dans les activités des services de renseignement, qui constitue une des premières activités des services, interroge dans la mesure où le projet fait l'impasse sur une question pourtant fondamentale : la frontière entre les activités relevant de la police administrative et celles ayant trait à la police judiciaire.

Le projet de loi ajoute enfin un nouvel intérêt public justifiant le recours à des techniques policières intrusives : « *la prévention des violences collectives de nature à porter atteinte à la paix publique* ». C'est dans ce dernier « intérêt public » que se niche l'extension la plus inacceptable des pouvoirs des services de renseignement. En effet, ce critère autoriserait à n'en pas douter les services spécialisés à opérer des formes intrusives de surveillance sur l'ensemble des mouvements et mobilisations de nature politique. La potentialité de violences collectives concerne en effet toute manifestation ou tout rassemblement de personnes. Nul doute que les services sont déjà présents dans les manifestations comme dans les lieux de mobilisation (telles les ZAD actuelles) et même dans les quartiers populaires périphériques. Mais donner une assise textuelle contribue à légitimer et normaliser ces pratiques, tout en décuplant les moyens de fichage et de surveillance de mouvements politiques. Ce texte autoriserait ainsi, lors d'une manifestation publique, à capter, par le dispositif de l'IMSI catching, l'ensemble des données de connexion téléphonique, ou à écouter les réunions préparatoires à des mobilisations politiques par le biais d'une sonorisation.

Le Syndicat de la magistrature dénonce toute forme de renseignement à caractère politique et exige que le critère de « violences collectives de nature à porter atteinte à la paix publique », extensif et imprécis, et dont l'objectif politique est à peine voilé, soit retiré du projet de loi.

L'analyse des intérêts publics le démontre donc bien : ce texte ne se borne pas à donner des moyens à la prévention du terrorisme, qui ne constitue que l'une des missions assignées aux services de renseignement.

Et tout comme le champ d'intervention du renseignement déborde la seule question terroriste, le projet de texte s'étend bien au-delà du seul renseignement antiterroriste. Aussi, l'article 12 du projet est-il consacré à la surveillance des personnes détenues, aux fins de prévenir les évasions et d'assurer la sécurité et le bon ordre des établissements. Ce critère classique en matière pénitentiaire fonde aujourd'hui un projet d'extension du renseignement pénitentiaire, qui se voit confier, sous le seul et très insuffisant contrôle du procureur de la République, des pouvoirs de détection,

d'interruption et de brouillage des communications émises sur des téléphones portables ou ordinateurs, mais aussi un pouvoir de captation des données techniques de connexion par le mécanisme de l'IMSI catching, très intrusif car non ciblé. Pour le Syndicat de la magistrature, le fait que la détention de téléphones portables soit à ce jour interdite en détention ne saurait autoriser toutes les mesures de surveillance. Il n'est ainsi pas acceptable que l'administration pénitentiaire, ainsi consacrée au rang des services de renseignement, puisse mettre en œuvre sans contrôle précisément organisé la captation de ces données (données techniques de connexion notamment et données informatiques contenues dans les systèmes de traitement automatisés de données).

2. L'absence de contrôle des « débordements » du renseignement

N'appréhendant le champ d'intervention du renseignement que sous l'angle de son extension, le projet fait l'impasse sur la frontière entre les activités de renseignement et les activités de police judiciaire. Il n'est question ni des « débordements » du renseignement (la poursuite de collecte de renseignement après constatation d'une infraction ou en parallèle d'une enquête judiciaire), ni des retards dans la judiciarisation des affaires (ouverture d'une enquête judiciaire sur la base de renseignements). Il s'agit pourtant d'enjeux majeurs de la protection des libertés et du contrôle de services dont le fonctionnement est par essence occulte.

Il convient de rappeler qu'une enquête judiciaire n'intervient pas nécessairement après les faits, elle peut être ouverte avant qu'une infraction soit commise, pour peu que l'infraction (potentiellement en préparation) soit déterminée. En deçà, le renseignement intervient en collectant des informations non spécifiques. Le renseignement a vocation à réunir des informations générales, la police judiciaire à investiguer sur des faits particuliers contrevenant à la loi pénale.

La frontière devrait être claire dès lors que L'article 40 du code de procédure pénale impose à « toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit, d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs ». Pourtant, la pratique des services spécialisés peut contrevenir à cette obligation, lorsqu'il n'est pas dans leur intérêt de judiciariser une affaire pour des raisons diverses tenant aux stratégies desdits services. Ce retard dans la judiciarisation a été dénoncé par de nombreux professionnels sans trouver de réponse dans le projet de texte présenté.

Et trop d'affaires judiciaires se trouvent nourries par des informations obtenues par les services de renseignement et introduites dans les procédures judiciaires par le biais de procès-verbaux – anonymes – de renseignement. Des pratiques qui suspendent l'application des règles de la procédure pénale, seules de nature à assurer le respect des droits de la défense.

Malgré ces dérives connues, le projet n'élabore aucun dispositif sérieux de contrôle de la frontière entre renseignement et police judiciaire. Pour le Syndicat de la magistrature, le contrôle sur l'usage des techniques devrait évidemment inclure un contrôle sur le cadre légal opportun. Si les éléments déjà recueillis permettent d'identifier une ou plusieurs infractions déterminées, en préparation même à un stade embryonnaire, une enquête judiciaire devra être ouverte pour mettre en œuvre ces pouvoirs. Le contrôle devra également empêcher les services de poursuivre leur action en parallèle d'une enquête judiciaire.

Dès lors néanmoins que le renseignement, cantonné à une mission de recueil d'information, n'a pas vocation à disparaître, il doit être encadré. Mais loin de prévoir un tel contrôle, le projet de loi consacre en réalité des pratiques particulièrement intrusives et attentatoires aux libertés individuelles, sans assurer de contrôle réel.

B. Les pouvoirs exorbitants des services de renseignement entérinés

1. La disproportion des mesures de surveillance ciblées

Les accès administratifs aux données de connexion

Le projet approfondit dangereusement les dispositifs introduits par la loi de programmation militaire du 18 décembre 2013 sur l'accès administratif aux données de connexion¹.

Il crée un accès en temps réel des services spécialisés aux réseaux des opérateurs : l'article L 851-3 du CSI introduit par le projet donne le pouvoir

¹ Dont le périmètre est très large puisque peuvent être recueillies les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, recensés l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, localisés les équipements terminaux utilisés, et listées les communications entrantes et sortantes d'un abonné, ainsi que la durée et la date des communications.

aux services spécialisés d'opérer du recueil d'informations directement sur les réseaux des opérateurs, « *pour les seuls besoins de la prévention du terrorisme* » et concernant « *des personnes préalablement identifiées comme présentant une menace* ». Le glissement du « recueil auprès des opérateurs » vers la ponction directe sur les réseaux est d'autant plus préoccupant que les critères sont peu restrictifs. Il n'est en effet requis aucun « risque imminent » d'action terroriste pour mettre en œuvre cette modalité dérogatoire de recueil.

La géolocalisation :

L'utilisation de balises ou de tout autre dispositif de géolocalisation en temps réel d'une personne, d'un véhicule ou d'un objet est également légalisée par l'article L 851-6. La démarche est loin d'être anodine : il est de notoriété publique que les services font déjà usage de cette technique intrusive. Mais, si le Syndicat de la magistrature n'est pas, par principe, hostile à toute forme de surveillance, il exige que le cadre soit strictement défini. Tel n'est assurément pas le cas lorsque l'objectif de « *prévention des atteintes aux intérêts publics mentionnés à l'article L 811-3* » constitue la seule condition du recours à cette technique intrusive, sans autre garantie.

Malgré son caractère particulièrement intrusif, cette technique compte au nombre de celles qui peuvent être mises en œuvre sans autorisation préalable, au seul motif de « *l'urgence liée à une menace imminente* » (laquelle ne se limite pas à la menace terroriste, il faut le rappeler!) ou du « *risque très élevé de ne pouvoir effectuer l'opération ultérieurement* » catégorie encore plus floue et susceptible d'interprétation large. Il faut d'ailleurs ici encore répéter que si la menace imminente en question est la commission d'une infraction, le cadre de l'enquête judiciaire autorise aujourd'hui le recours à la géolocalisation dans des conditions larges et néanmoins soumises à un contrôle juridictionnel préalable.

Le Syndicat de la magistrature conteste le régime ainsi fixé pour la pose de balise tant en raison d'un encadrement textuel insuffisant que de l'autorité décisionnaire choisie.

Les interceptions de sécurité

Le texte élargit encore le champ des interceptions de sécurité régi par la loi de 1991, par la référence aux intérêts publics listés au nouvel article L 811-3 : les écoutes administratives trouveront ainsi à s'appliquer bien au-delà du seul champ de la prévention du terrorisme. Le nouvel article L 852-1 du CSI procède à une extension dangereuse des « cibles » d'interception des

correspondances émises par voie de communications électroniques : l'*entourage* (notion très floue) des personnes visées peut être écouté si « *elles sont susceptibles de jouer un rôle d'intermédiaire, volontaire ou non, pour le compte de celle-ci ou de fournir des informations* ». Cette définition est si lâche que c'est bien le principe des écoutes des proches des « cibles » qui est ainsi entériné, ouvrant la voie à une surveillance sans discernement de la population. Le texte n'offre en réalité aucun encadrement lorsqu'il permet d'écouter les personnes susceptibles de servir d'intermédiaire de manière « non volontaire » ou de simplement « fournir des informations ». Ce critère pourra viser indifféremment tout l'entourage d'une personne suspectée, jusqu'à un degré de connaissance relativement faible. La surveillance ainsi mise en œuvre s'éloigne clairement d'une surveillance ciblée, pour s'étendre au-delà de seules personnes identifiées.

Ce cadre ne garantit aucunement l'équilibre nécessaire à la préservation des libertés : ces écoutes peuvent concerner tous types de professions (y compris des avocats ou des journalistes par exemple) et les critères retenus laissent entrevoir des possibilités d'écoutes à des fins politiques. Le quota d'interception demeure fixé par le Premier ministre et se situe hors du débat démocratique. S'il peut être admis que la détermination du nombre d'interceptions effectuées dans un même temps ne relève pas techniquement du domaine de la loi, ce choix n'en demeure pas moins contestable. Enfin, le texte prévoit que l'arrêté fixant le contingent et sa répartition entre les ministères est porté à la connaissance de la CNCTR (tout comme le nombre d'autorisations délivrées) : doit-on en conclure que ces éléments ne seront pas accessibles aux citoyens ?

Le Syndicat de la magistrature conteste tout à la fois le champ élargi permettant le recours aux interceptions, la désignation dans le texte de l' « entourage » selon une acception très large et l'absence de garanties procédurales. Ces garanties devraient tenir non seulement à l'indépendance de l'autorité prenant la décision de la mise sur écoute mais aussi à la constitution d'une protection spécifique pour les professions sensibles (notamment les avocats et journalistes).

La sonorisation et la captation d'images et de données informatiques

L'article 3 du projet de loi est tout entier consacré à la captation de données : il s'agit d'une disposition nouvelle accordant un pouvoir supplémentaire aux services de renseignement. Seul le principe de subsidiarité énoncé au nouvel article L 853-1 du CSI (si les moyens ne peuvent être recueillis par un autre moyen légalement autorisé) vient encadrer ce procédé très intrusif. En effet, cette méthode de surveillance contrevient à deux

principes fondamentaux : l'inviolabilité du domicile et la liberté de communication.

S'agissant de la sonorisation tout particulièrement, soulignons qu'elle constitue une atteinte plus grave encore que les interceptions de sécurité, dès lors que l'ensemble des conversations, discussions, jusqu'aux pensées exprimées à voix haute dans la solitude sont susceptibles d'être interceptées. Dans cette situation, le domicile perd sa dimension sacrée qui en fait le lieu par excellence de l'intimité et de la liberté quasi absolue. Le texte vise non seulement l'enregistrement audio, mais aussi la captation d'images, correspondant au placement de caméras à l'intérieur d'un domicile. L'ensemble des activités effectuées au sein du domicile sur un ordinateur ou un appareil similaire, sur internet ou sans connexion internet, peut être surveillé et intercepté en temps réel, le texte visant « *des données informatiques transitant par un système automatisé de données ou contenues dans un tel système* ». Ainsi, un texte (politique par exemple...) rédigé sur un traitement de texte, tout comme une conversation sur Skype, pourraient être espionnés en temps réel. Là encore, le texte ne limite aucunement le recours à cette mesure à la seule prévention du terrorisme.

Pour le Syndicat de la magistrature, de tels pouvoirs ne sont légitimes qu'à titre exceptionnel, dans des procédures judiciaires concernant des infractions graves et placées sous le contrôle d'un juge indépendant.

2. La danger de mesures de surveillance généralisées

L'accès administratif aux données

Le nouvel article L 851-4 du CSI est extrêmement inquiétant puisqu'il confie aux services le pouvoir « *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* ». Il s'agit de légaliser une pratique de surveillance non ciblée, consistant pour les opérateurs et fournisseurs d'accès à utiliser des matériels et logiciels fonctionnant sur la base d'algorithmes pour filtrer l'ensemble des données circulant sur les réseaux. Ce passage au tamis de la totalité des actions des internautes sera élaboré pour détecter des profils sur la base de leur connexion, du contenu qu'ils examinent ou de leur « cheminement » sur le net, une association de recherches internet par exemple.

Ces dispositions doivent alarmer les citoyens : ce texte donne des capacités de surveillance généralisée sans précédent aux services de renseignement et

aux prestataires privés chargés de la mise en œuvre de la technique. Valider l'utilisation d'algorithmes pour passer au tamis l'ensemble des flux internet, contenus et données de connexion, ouvre une brèche d'autant plus inquiétante que le cadre fixé est insuffisamment protecteur.

D'abord s'agissant des conditions de recours à cette technique de surveillance massive : l'existence d'une menace terroriste précise et imminente n'est pas la condition du recours temporaire à cette surveillance généralisée. A l'inverse, c'est la mise en œuvre de la technique qui doit révéler la menace.

C'est au titre de la prévention du terrorisme que les services pourraient recourir à cette technique (sur simple avis de la CNCTR, encore une fois) pour une durée de 30 jours renouvelable sans limitation. Rien n'empêchera une utilisation quasi permanente, puisque la prévention du terrorisme est une mission qui figure sans discontinuité à l'agenda des services de renseignement.

Ensuite parce que cette « garantie » de l'anonymat – qui serait levée par le seul Premier ministre en cas de menace avérée - n'en est en réalité pas une : les professionnels de l'internet rappellent eux que la combinaison d'un petit nombre de données suffit à identifier des personnes, démontrant le caractère illusoire de cette protection.

Enfin parce que les algorithmes utilisés (et susceptibles d'être modifiés durant le temps de la mise en œuvre de la technique) demeureront secrets, alors même qu'un contrôle aigu aurait vocation à leur être appliqué, si cette technique était validée.

Pour le Syndicat de la magistrature, ce cadre ne constitue aucunement un rempart contre des formes de surveillance généralisée. Non seulement les conditions du contrôle a priori pèchent par leur faiblesse, mais les conditions de recours à ces techniques sont loin d'être restrictives. Ces articles contreviennent ainsi au principe de proportionnalité. Nombreux sont les commentateurs spécialisés qui identifient dans ce procédé un mode opératoire proche de la surveillance de masse opérée par la NSA, consistant à placer sous contrôle une large partie du trafic internet à la recherche de comportements « suspects » ou de marqueurs faibles.

Le Syndicat de la magistrature rappelle son opposition à ces formes de surveillance généralisée.

L'IMSI catching

Afin qu'aucun espace de liberté ou d'intimité, aucun lieu de débat collectif ne puisse échapper aux services de renseignement, le projet légalise l'*IMSI catching* sous le nom savamment édulcoré de « dispositif technique de proximité ». Le procédé est ainsi décrit dans le rapport précité : « *(il) consiste à placer une fausse antenne relais à proximité de la personne dont on souhaite intercepter les échanges téléphoniques portables. Cette antenne capte les données transmises entre le téléphone portable et la véritable antenne relais (...) ce procédé est plus attentatoire aux libertés que la classique interception des télécommunications, notamment parce qu'il conduit à capter les conversations téléphoniques de l'ensemble des personnes se trouvant à proximité de l'antenne relais factice* ». Précision utile, le rayon de ce dispositif peut aller d'une centaine de mètres à près de deux kilomètres, selon la disposition des lieux et la densité des réseaux : les captations de données pourront donc concerner un grand nombre de personnes sur la seule base de leur proximité temporaire et fortuite avec une « cible » potentielle.

L'article L 851-7 du CSI ainsi créé par le projet autorise le recours à cette technique pour la totalité des « *intérêts publics mentionnés à l'article L 811-3* » : il ne se borne aucunement à la prévention du terrorisme ou à l'imminence d'un attentat. La durée classique d'autorisation de mise en œuvre d'une technique est de 4 mois renouvelables, et est même portée à 6 mois. Elle peut être donnée « *au bénéfice d'un service et porter sur des lieux et une période déterminée* ». La procédure spécifique de motivation spéciale et d'avis exprès de la CNCTR ne suffit évidemment pas à encadrer ce pouvoir.

Une dérogation supplémentaire est prévue par le texte (point III) : « *pour la prévention d'un acte de terrorisme* », la captation peut porter non seulement sur les données de connexion mais aussi sur le contenu des correspondances émises ou reçues par un équipement terminal (une antenne relais). Le texte ne requiert pas même l'imminence d'un acte de terrorisme ou d'une menace spécifiquement désignée. Et l'installation peut se faire sans autorisation préalable selon les conditions de l'article L851-6 2ème alinéa.

Pour le Syndicat de la magistrature, le procédé de l'*IMSI catching* est si intrusif qu'il n'a vocation à être utilisé qu'exceptionnellement dans le cadre de procédures judiciaires concernant des infractions graves à la loi pénale. Il ne saurait être utilisé dans le renseignement, a fortiori au regard de son champ d'intervention élargi.

Ces pouvoirs sont complétés par la généralisation du recueil des informations concernant les déplacements de l'ensemble des citoyens. Dans le

prolongement du décret du 26 septembre 2014, adopté dans le plus grand secret, qui a créé le fichier PNR-API français actant la surveillance de tous les citoyens prenant l'avion en France, l'article 9 du projet entérine un contrôle généralisé des déplacements de tous. Ainsi, en application de l'article L 561-26 du code monétaire et financier, les services spécialisés pourront *« demander à toute entreprise de transport terrestre, ferroviaire, maritime ou aérien ou opérateur de voyage ou de séjour les éléments d'identification des personnes ayant payé ou bénéficié d'une prestation ainsi que les éléments d'information relatif à la nature de cette prestation et, s'il y a lieu, aux bagages et marchandises transportés »*.

Comment considérer sérieusement que ce texte vient encadrer les pouvoirs des services de renseignement, quand il leur confie en réalité, sur des critères si peu restrictifs, des pouvoirs exorbitants et particulièrement intrusifs ! La CNIL elle-même a dénoncé dans ces nouvelles techniques (sonde, dispositif de détection de « signaux faibles » et « IMSI catcher ») un *« profond changement de nature dans les mesures de surveillance légalement autorisées. 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 »* La critique, quoi que mesurée dans les termes, doit être entendue pour ce qu'elle est : une alerte face à une possible mutation de notre société vers une surveillance généralisée.

Elle est d'autant plus pertinente que le projet de loi procède à cette extension du champ d'intervention et des pouvoirs des services sans élaborer un réel contrôle du recours à ces techniques intrusives.

II. Un encadrement insuffisant des pouvoirs de renseignement

Le déséquilibre dont souffre ce projet tient tout à la fois à la faiblesse de l'institution de contrôle créée (la CNCTR) et par les insuffisances du contrôle juridictionnel a posteriori confié au Conseil d'Etat.

A. La CNCTR, une commission faible

1) Le contrôle a priori très insuffisant

Alors même qu'il ambitionne de mettre notre droit en conformité avec les exigences démocratiques, le projet maintient le Premier ministre au cœur du système de renseignement actant une logique de pouvoir d'Etat au détriment de la soumission à l'Etat de droit. C'est ce que prévoit l'article L 821-1 en confiant le pouvoir décisionnel au Premier ministre, lequel n'est aucunement tenu de suivre l'avis purement consultatif confié à la Commission nationale de contrôle des techniques de renseignement qu'il crée et qui se substitue à l'actuelle CNCIS.

Cette commission, dont la composition est prévue par l'article L 831-1, de nature administrative, est formée de neuf membres. Quatre d'entre eux sont des juges, dont deux conseillers d'état et deux juges judiciaires, magistrats ou anciens magistrats de la Cour de cassation. Quatre sont des parlementaires, députés et sénateurs désignés par les présidents de leurs assemblées respectives. Le neuvième membre est un technicien, « personnalité qualifiée pour sa connaissance en matière de communications électroniques, nommé sur proposition du président de l'autorité de régulation des communications électroniques et des postes. »

La nomination politique de près de la moitié de la commission contredit son caractère affiché d'indépendance. En effet, si cette composante donne une apparence « démocratique » à la commission, elle la place en réalité en situation de dépendance par rapport au pouvoir politique. Cette composante de la commission ne sera qu'insuffisamment contrebalancée par la présence de quatre juges, même si le président de la commission est désigné parmi eux. Il convient de rappeler à nouveau que c'est au juge judiciaire que revient la mission constitutionnelle de gardien des libertés individuelles, mission dont découle son statut d'indépendance totale vis à vis du pouvoir. C'est pourquoi le Syndicat de la magistrature considère que seule une commission largement composée de magistrats, et parmi eux, d'une majorité de juges judiciaires, ainsi que de personnalités qualifiées nommées selon des procédures de nature à exclure toute relation de dépendance politique peut prétendre à une indépendance réelle, et être à même de mener à bien un contrôle efficace.

La mise en œuvre des techniques de recueil des renseignements sera autorisée par le premier ministre, sans que l'avis de la CNCTR s'impose à lui. Selon les articles L 821-1 à L 821-6, la demande d'autorisation, est communiquée au président de la commission ou, à défaut, à un membre de la commission désigné par lui, qui rend un avis dans les 24h, sauf s'il y a un doute sur la validité de la demande, auquel cas la commission se réunit pour rendre un avis dans les 3 jours. A défaut d'avis rendu dans les délais, l'avis est réputé rendu. Si la commission estime qu'une autorisation a été donnée illégalement, elle adresse au premier ministre et au service de renseignement

concerné une recommandation tendant à l'interruption de la technique. Si cette recommandation n'est pas suivie d'effet, la majorité absolue des membres de la commission peut saisir le Conseil d'Etat. En cas d'urgence absolue, le Premier ministre peut autoriser le service à mettre en œuvre une technique de renseignement sans avis préalable de la commission.

Ces modalités de fonctionnement ne peuvent satisfaire aux exigences d'un contrôle réel et indépendant de pouvoirs particulièrement attentatoires aux libertés individuelles. Tout d'abord, les avis et recommandations de la commission sont dépourvus de force obligatoire. L'avis préalable, comme la recommandation éventuellement formulée, ne lie pas le Premier ministre qui demeure toujours libre d'autoriser contre l'avis de la commission. Aussi, si l'on excepte la possibilité de saisir une juridiction, cette instance tient un rôle somme toute consultatif, qui ne peut évidemment constituer un contrôle suffisant eu égard au caractère extrêmement intrusif des mesures concernées.

A cet égard, il faut signaler que dans la pratique actuelle de la CNCIS, cette commission peut intervenir dans un cadre d'urgence et rendre un avis dans les deux heures, jour et nuit. Cela démontre qu'un tel dispositif est viable, à condition que les moyens humains permettent d'assurer la permanence utile, et qu'une volonté politique favorable à un contrôle plus efficace peut faire le choix de ne permettre en aucun cas de déroger à l'avis de l'autorité de contrôle.

Dans le même sens, le projet de loi prévoit le cas du silence de la commission : la carence de la CNCTR à se prononcer dans les délais prévus vaut consentement de sa part. Et là réside un vice essentiel du projet de loi : la commission fonctionne selon une logique inversée en termes de protection des libertés. Si la commission ne dit mot, elle admet une atteinte aux libertés ; c'est l'émission d'un possible frein à cette atteinte qui doit être explicite. De même, pour autoriser une mesure de renseignement, possiblement attentatoire aux libertés, un seul des membres de la commission peut se prononcer ; si à l'inverse il s'agit de d'émettre un avis négatif, alors la commission doit agir collectivement, et plus encore, si elle envisage de saisir le Conseil d'Etat, elle ne peut le faire qu'à la majorité absolue de ses membres. Il est aussi particulièrement notable qu'en matière de surveillance des communications émises ou reçues à l'étranger, la loi ne prévoit pas d'avis préalable de la CNCTR. Peut-on alors encore affirmer que ce texte a pour objet d'encadrer les activités, en dérogeant à un droit commun déjà si peu protecteur alors même que peuvent être impliqués des identifiants rattachables au territoire national lorsqu'ils sont interlocuteurs d'un identifiant étranger ? Le Syndicat de la magistrature entend dénoncer cette

ultime dérogation comme l'opacité dans laquelle un cadre juridique est susceptible d'être ultérieurement fixé par décret en Conseil d'Etat non publié.

Le Syndicat de la magistrature dénonce déclare très fermement son hostilité à cette vision minimaliste du contrôle a priori. Le gouvernement refuse d'envisager un dispositif réellement « garantiste ». Il exclut d'abord de manière contestable la compétence judiciaire selon une vision particulière de la distinction entre police administrative et police judiciaire. Il refuse ensuite d'envisager un système dans lequel une autorité indépendante (composée de magistrats judiciaires et administratifs, éclairés par des techniciens) aurait le pouvoir d'autoriser ou non le recours aux techniques intrusives. Ce mécanisme de véritable contrôle a priori serait pourtant seul à même d'assurer le caractère démocratique de l'intervention des services.

Enfin, au prétexte qu'il crée une commission – pourtant si faible – le projet ne pose aucune limite aux pouvoirs accordés aux services de renseignement : le Syndicat de la magistrature estime quant à lui que certains pouvoirs sont tellement attentatoires aux libertés que l'on ne doit pouvoir y recourir que dans le cadre d'une enquête judiciaire, celle-ci devant obligatoirement viser des personnes contre lesquelles il existe des raisons graves de soupçonner qu'elles ont ou vont commettre une infraction pénale lourde. C'est le cas des dispositifs de surveillance non ciblée et des dispositifs intrusifs tels que la sonorisation.

2. Faiblesse du contrôle diffus effectué par la commission

La commission est également chargée d'assurer un contrôle non juridictionnel a posteriori, selon des modalités régies par les articles L 822-1, L 822-2, L 822-4 et L 833-1 à L 833-6. La mission de la CNCTR est ainsi de « veiller à ce que les techniques de recueil du renseignement soient mises en œuvre sur le territoire national conformément aux dispositions » du livre VIII du CSI tel que prévu par le projet discuté. Son action doit être facilitée par tous les agents et les autorités publiques, et est permise par la communication de toutes les autorisations délivrées par le Premier ministre ou ses délégués, un droit d'accès aux autorisations, relevés, registres, données collectées, transcriptions et extractions effectués et mis à disposition par les services de renseignement, la possibilité d'obtenir sur demande à tout moment des informations sur les modalités d'exécution des autorisations en cours. Jusqu'à présent, l'ensemble des interceptions de sécurité était à disposition permanente de la CNCIS, puisque consigné dans ses locaux, permettant un contrôle effectif.

C'est l'article L 822-1 qui détermine les rôles et les responsabilités dans la mise à disposition des informations sur la base de laquelle le contrôle peut

s'exercer. Sous la responsabilité du Premier ministre, et selon des modalités qu'il lui appartient de définir par une voie non prévue par la loi, les services de renseignement eux-mêmes établissent un relevé de leur propre action, que l'on comprend être une forme de journal de bord. Aucun encadrement législatif n'est en mesure d'assurer que les documents ainsi fournis à la CNCTR épuisent l'activité réelle des services. Sans adopter une posture de défiance de principe, il importe toutefois de rester vigilant sur la possibilité de ce que des actes ne soient jamais soumis à la commission et que des informations recueillies dans des procédures autorisées soient soustraites de ces relevés.

Et même en retenant par principe la bonne foi des services de renseignement on s'aperçoit, là encore, que le contrôle ne peut trouver d'effet que si la CNCTR est suffisamment prompte à agir. En effet, l'autorité de contrôle n'est tenue par aucun délai pour agir dès lors que la phase de l'avis préalable est dépassée. Or, les techniques de recueil de renseignement n'ont vocation à se dérouler que pour un temps limité. Il en va de même pour la conservation des données recueillies, qui ne demeurent disponibles que dans un certain délai avant destruction. C'est donc au cours de ces délais que la commission est en mesure de se livrer aux vérifications utiles et à leur analyse, pour, le cas échéant recommander de mettre fin à la technique ou à la conservation. Le seul terrain d'influence de la commission est donc *in fine* celui d'une abréviation du travail en cours. Il convient de relever que la commission devra disposer de moyens humains conséquents, tant la célérité est la condition *sine qua non* de son action à tous égards.

Dépourvue de tout pouvoir d'interpellation publique en dehors de son rapport annuel dont l'expression demeurera limitée par les exigences du secret défense, la CNCTR aura pour seul recours réel la saisine du Conseil d'Etat, si ses avis et recommandations ne sont pas suivis d'effet. Or, cette modalité de contrôle a posteriori souffre elle-même de ses faiblesses.

B. Le contrôle juridictionnel largement illusoire

1. Une procédure insuffisamment protectrice des libertés

Un des aspects positifs du projet de loi réside dans la possibilité d'entrée en jeu du Conseil d'Etat. L'existence d'un recours, même très insuffisant, constitue une avancée dans un champ jusque là laissé à l'écart de tout contrôle juridictionnel. Mais cette introduction, telle que pensée dans le projet de loi, est si faible que sa portée est principalement symbolique.

La saisine du Conseil d'Etat est la sanction maximale que la CNCTR peut infliger aux services de renseignement ou au Premier ministre qui persistent à

contrevenir à ses recommandations. Elle peut le faire de son propre chef, dans le cas précédemment décrit, ou à la demande d'un justiciable. Comme le prévoit l'article L 841-1, le Conseil d'Etat peut également être saisi à titre préjudiciel par toute juridiction administrative ou judiciaire dans le cadre 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 une des parties.

Lorsqu'il s'agit d'une saisine à l'initiative d'un citoyen, la CNCTR agit comme un filtre, dans les conditions prévues par l'article L 821-6, impliquant l'émission d'une recommandation non suivie d'effet, et enfin d'une décision de saisine prise à la majorité absolue. Cet obstacle introduit lors de l'examen en Conseil d'Etat retarde d'autant l'accès au juge, alors même que la CNCTR ne dispose d'aucun pouvoir de contrainte dans ce cadre, comme c'est le cas dans les recours préalables classiques. Tout le dispositif est en réalité obéré par le secret qui entoure les techniques de renseignement, qui confère un caractère hasardeux aux demandes de justiciables, lesquels ne peuvent que soupçonner l'existence d'une surveillance mise en œuvre à leur encontre.

Le fonctionnement « à l'aveugle » pour les justiciables se poursuit tout au long de la procédure : la saisine de la CNCTR porte par définition sur des faits inconnus du requérant, qui est contraint de faire état d'indices ou d'impressions. La réponse donnée par cette administration ne l'éclairera que très partiellement : soit le Conseil d'Etat sera saisi, auquel cas le justiciable pourra déduire qu'il fait ou a fait l'objet d'une mesure de surveillance, soit la CNCTR lui indique qu'aucune irrégularité n'a été commise, ce qui peut signifier qu'il n'a été concerné par aucune surveillance, ou aussi bien que la mesure de surveillance qu'il a subie est jugée régulière. Le requérant pourra alors faire le choix de ne pas se fier à cet avis et de saisir le Conseil d'Etat. Il se trouvera certes devant cette juridiction mais sans élément tangible de connaissance sur sa situation relativement à d'éventuelles mesures de surveillance, et le demeurera jusqu'à la décision qui indiquera, ainsi que dispose l'article L 773-6 « qu'aucune illégalité n'a été commise, sans confirmer ni infirmer la mise en œuvre d'une technique », ou, dans les conditions prévues par l'article L 773-7, l'informer qu'une illégalité a été commise « sans faire état d'aucun élément protégé par le secret défense ». Si les considérations relatives au nécessaire secret devant protéger le renseignement sont audibles dans la logique du texte, le Syndicat de la magistrature entend dénoncer le caractère illusoire d'un recours ouvert en principe, mais en réalité soumis à un filtre administratif préalable, et surtout extrêmement difficile, voire impossible à soutenir compte tenu de l'obligation pour le requérant de le présenter les mains vides et sans possibilité d'une réelle défense. Il n'est en outre pas acceptable que le Conseil d'Etat ne puisse de lui-même déclassifier les

informations en cause pour informer parfaitement le citoyen victime d'une surveillance illégale des conditions dans lesquelles elle a été mise en œuvre.

Quand à la possibilité offerte au requérant d'obtenir réparation du préjudice subi du fait d'une mesure de surveillance illégale, elle est de pur affichage : le Conseil d'Etat ne peut indemniser un requérant à ce titre que s'il est saisi de conclusions en ce sens. Que pourraient donc contenir ces conclusions, qui ne sauraient déterminer avec précision de fait générateur (par hypothèse, la mesure de surveillance devant rester occulte en tout état de la procédure) ni de lien de causalité (qui ne peut être décrit qu'en fonction de son point de départ, ici inconnu) ni même de préjudice précisément déterminé, vu l'ignorance de la durée de la mesure et donc de ses effets préjudiciables éventuels ? Il ne fait nul doute qu'un citoyen pourra souffrir ou avoir souffert du fait d'une mesure de surveillance ; il ne fait nul doute non plus qu'il ne parviendra pas à en être dûment réparé.

Non seulement le requérant est contraint de former un recours en demeurant dans l'ignorance totale de sa situation, mais il le soutiendra dans les conditions très éloignées du « procès équitable » tel que l'entend la Cour européenne des droits de l'homme, et se trouvera face à l'Etat dans un position de complète inégalité des armes, et dans un cadre non respectueux du contradictoire, heureusement compensé par un très large office du juge.

C'est bien ici le périmètre du secret défense qui déterminera la réalité du contrôle a posteriori. Or, le texte ne donne au Conseil d'Etat aucun pouvoir d'appréciation sur la pertinence de la classification secret défense des informations qui lui sont soumises. Ainsi, la juridiction n'a pas de marge de manœuvre quant à la publicité des débats, l'article L 773-4 énonçant que le président « *ordonne* » le huis-clos lorsqu'est en cause le secret de la défense nationale. Dans les mêmes conditions, le contradictoire est exclu sans appréciation possible par le conseil : l'article L 773-5 prévoit ainsi que la formation chargée de l'instruction entend les parties séparément lorsqu'est en cause le secret de la défense nationale. Or, l'audition de l'administration dans un procès administratif n'est légitime que lorsque ses explications sont soumises au contradictoire. Si le citoyen requérant n'est pas mis en capacité de connaître ses arguments, ceux-ci ne devraient pas pouvoir être entendus par le Conseil d'Etat. La juridiction devrait alors se prononcer sur la base de la seule motivation écrite exigée de l'administration pour la mise en œuvre des techniques : ce n'est qu'à cette condition que cette exigence de motivation préalable constituera une réelle avancée.

Cette procédure a pour double effet négatif de renforcer le déséquilibre procédural au profit de la partie défenderesse, et d'amoindrir l'obligation de

motivation qui pèse sur elle. Pourquoi, en effet, prendre la peine de motiver suffisamment ses décisions quand on aura l'opportunité de les justifier a posteriori si elles sont remises en cause ?

2) l'insuffisance des sanctions

Enfin, si l'intervention du Conseil d'Etat dispose bien d'un véritable pouvoir de faire obstacle à la poursuite d'une technique illégale, on ne peut que déplorer, d'abord, que ce pouvoir se manifeste si tardivement, et d'autre part, qu'aucune autre sanction ne soit possible que l'annulation de l'autorisation.

De fait, la tardiveté de l'intervention du Conseil d'Etat réduit considérablement la portée de son contrôle. Nous l'avons déjà indiqué, les techniques de renseignement sont mises en œuvre pour une durée limitée. Or l'intervention du Conseil d'Etat, sur saisine d'un citoyen mais aussi de la CNCTR, n'est possible qu'après épuisement de la procédure prévue par l'article L 821-6, laquelle ne fixe aucun délai, et est concrètement, susceptible d'être longue. Et une fois le Conseil d'Etat saisi, celui-ci n'a pas de délai pour statuer. L'article L 841-1 prévoit un délai maximum d'un mois en cas de saisine à titre préjudiciel par une juridiction. Par extrapolation de cette disposition et par expérience des délais de traitement usuels de la haute cour, il n'est pas invraisemblable de penser que les délais de traitement des requêtes excéderont très largement la durée des mesures attaquées, ainsi que la durée de conservation des renseignements recueillis à ce titre, étant entendu que le texte ne prévoit pas d'extension de la conservation des données en cas de recours. Deux difficultés apparaissent : sans subsistance de preuves directes, seul le « journal de bord » du service de renseignement tiendra lieu de pièces, ce qui jette un doute sérieux sur la réalité du contrôle ; bien après que toute trace de la mesure a disparu, la seule sanction possible étant son annulation, et la destruction des renseignements irrégulièrement collectés, il sera certes fait droit à la requête du requérant, sans conséquence réelle toutefois lorsque la surveillance illégale aura cessé depuis longtemps.

A cet égard toutefois, l'allongement manifeste de la durée de conservation est préoccupant. Il est inacceptable que l'article L 822-2 permette, en cas de nécessité de décryptage, de ne faire courir le délai de conservation qu'à compter du déchiffrement, en laissant au service toute latitude sur la date d'exploitation des données. Alors que les délais de conservation actuels sont de 10 jours pour les interceptions de sécurité et d'une année maximum pour les métadonnées, le projet prévoit de fixer ce délai à un mois pour les écoutes, un an maximum pour les informations recueillies par d'autres techniques et à 5 ans les données de connexion. S'il était possible de s'interroger sur l'ambivalence de cette longue conservation, attentatoire aux

libertés mais pouvant assurer l'effectivité des recours, on ne peut qu'être très inquiets de cet allongement. En effet, face à un recours largement illusoire, prévoir de tels délais est particulièrement alarmant, et contraire aux principes fondamentaux dans la mesure où le recueil d'informations est significativement élargi par ces nouveaux pouvoirs.

Enfin, le Syndicat de la magistrature déplore l'absence de possibilités de sanctions au-delà de la simple annulation des actes. Fort heureusement, l'article L 773-7 prévoit que si l'illégalité constatée est susceptible de constituer une infraction, la formation de jugement saisit le procureur de la République, qui pourra s'en saisir à condition que le Premier ministre se prononce favorablement sur la déclassification des éléments du dossier. Cette disposition nécessaire est toutefois très insuffisante, d'une part en raison de l'obstacle possible de la classification au secret des documents nécessaires au traitement de l'affaire, et d'autre part parce qu'est laissée sans réponse toute une variété de situations excédant la simple irrégularité non fautive, mais ne pouvant emporter de qualification pénale. Quid, par exemple, d'irrégularités non fautives répétées du même agent ou du même service ? De la responsabilité partagée de nombreux agents donnant lieu à une irrégularité très grave, sans intention frauduleuse individuelle ?

Le contrôle des agents n'est pas au cœur du projet : ainsi l'article 10 du projet de loi prévoit-il une immunité pénale pour les agents des services qui auraient accédé ou se seraient maintenus frauduleusement dans un système de traitement automatisé de données « *pour assurer hors du territoire national la protection des intérêts publics* ». Singulier choix dans un domaine que l'on prétend encadrer juridiquement que de créer une immunité pénale, et donc, permettre aux agents concernés d'invoquer le fait justificatif de l'autorisation de la loi. Le Syndicat de la magistrature est hostile à toute forme d'immunité pénale au profit de ces services. Ils doivent demeurer comptables de leurs actes devant les tribunaux, lesquels pourront, lorsque cela est légitime, appliquer le fait justificatif de l'ordre de la loi.

A l'inverse, l'article 7 du projet étend à l'ensemble des techniques de renseignement la pénalisation de la révélation d'une mesure de surveillance, le refus de sa mise en œuvre ou de communiquer les informations. Jusqu'à présent, seules les interceptions de sécurité étaient concernées. Cette pénalisation, sans exception, est susceptible de porter une atteinte disproportionnée aux nécessités du débat démocratique. L'absence totale de dérogation à cette pénalisation aura des effets concrets : nul ne pourra informer les citoyens sur l'usage dévoyé qui pourrait avoir été fait des pouvoirs de surveillance. Cet article traduit encore une fois le refus français de consacrer un statut pour les lanceurs d'alerte.

Le projet évite en outre soigneusement de confier au Conseil d'Etat le soin de sanctionner l'usage de techniques policières par les services de renseignement alors que les conditions d'une intervention de police judiciaire étaient réunies. A défaut de prévoir un véritable contrôle a priori, le Conseil d'Etat devrait a minima pouvoir informer le Procureur de la République de l'interruption de la mesure et transmettre l'ensemble des éléments préalables à sa mise en œuvre pouvant justifier l'ouverture d'une enquête judiciaire.

Si le projet ne le prévoit pas explicitement, il appartiendra d'ailleurs au Conseil d'Etat de véritablement se saisir du texte pour exercer un tel contrôle dans le cadre de la saisine sur question préjudicielle par les juridictions pénales, afin que soient enfin sanctionnées les introductions occultes dans les procédures pénales d'informations obtenues illégalement par les services de renseignement.

Pour un véritable encadrement a priori des activités par une instance indépendante et qui n'exclue pas le juge judiciaire

Pour le Syndicat de la magistrature, l'activité des services de renseignement ne sera légitime que dans les conditions suivantes :

- Restreindre l'activité des services de renseignement à une fonction de connaissance et d'anticipation, dans un domaine strictement défini qui exclue la surveillance politique des activités militantes et le recueil d'information sur des actes délinquants ou criminels déterminés qui relèvent de la police judiciaire.
- Exclure certaines mesures ciblées du champ du renseignement et notamment la sonorisation de domicile ou de véhicule. Ces pratiques extrêmement intrusives ne peuvent trouver une légitimité que dans le cadre d'une information judiciaire sous le contrôle d'un juge indépendant, avec les garanties procédurales attachées à ce dispositif.
- Exclure l'ensemble des mesures de surveillance généralisée : IMSI catching, traitement automatisé de données de connexion. Du fait de leur caractère massivement intrusif, de telles pratiques ne peuvent trouver une légitimité que dans le cadre d'une information judiciaire, sous le contrôle d'un juge d'instruction indépendant.
- Refuser l'adjonction d'un régime de renseignement spécifique aux personnes détenus et fondé sur le seul risque d'évasion ou de trouble au bon ordre. Les personnes détenues n'ayant vocation à faire l'objet de surveillance qu'en

fonction des critères généraux énoncés par la loi.

- Refuser l'allongement de la durée de conservation des données recueillies dans le cadre de la mise en œuvre de techniques de renseignement.
- Confier le pouvoir d'autorisation des techniques d'investigation à une instance indépendante composée de juges administratifs et de juge judiciaires, ces derniers devant être majoritaires, accompagnés par des techniciens et excluant tout membre du pouvoir exécutif et du pouvoir législatif.
- Prévoir un recours juridictionnel a posteriori, dans des conditions assurant le respect du contradictoire et les conditions d'une défense réelle, notamment en réduisant le champ du secret défense.