

RÉPUBLIQUE FRANÇAISE

**LE DÉFENSEUR
DES DROITS**



Paris, le 2 avril 2015

Avis du Défenseur des droits n° 15-04

Le Défenseur des droits,

Vu l'article 71-1 de la Constitution du 4 octobre 1958 ;

Vu la loi organique n°2011-333 du 29 mars 2011 relative au Défenseur des droits ;

Auditionné le 2 avril 2015 par la Commission des Lois de l'Assemblée nationale sur le projet de loi relatif au renseignement.

Le Défenseur des droits a émis l'avis ci-joint.

Le Défenseur des droits

Jacques TOUBON

Le Constituant a confié au Défenseur des droits la mission générale « *de veiller au respect des droits et libertés par les administrations de l'État* » (article 71-1 de la Constitution) et, plus particulièrement, « *de veiller au respect de la déontologie par les personnes exerçant des activités de sécurité sur le territoire de la République* » (4° de l'article 4 de la loi organique n° 20111-333 du 29 mars 2011).

Le Défenseur des droits approuve la démarche du gouvernement visant à élaborer « *un cadre légal général aux activités des services de renseignement, alliant détermination des principes, définition des techniques et renforcement du contrôle* ». Sur ce dernier point, l'exposé des motifs précise que « *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* ».

Eu égard à l'objet de sa mission, le Défenseur des droits, qui prend pour acquise la nécessité d'adopter des outils de renseignement mieux adaptés à la réalité opérationnelle et aux besoins de la lutte contre le terrorisme, souhaite émettre une série d'observations portant, d'une part, sur le champ d'application de la loi, d'autre part, sur les modalités du contrôle opéré par la Commission nationale de contrôle des techniques de renseignement, enfin sur la mise en œuvre du contrôle juridictionnel.

1. La clarté et la précision de la loi quant à son champ d'application et sa portée

Les techniques de renseignement qui pourraient être mises en œuvre sont plus nombreuses et plus intrusives que celles qui existent déjà à l'heure actuelle.

Outre que le recours aux techniques de renseignement prévues par le projet de loi doit être limité à ce qui est strictement nécessaire et approprié à la réalisation des objectifs poursuivis, la loi doit répondre à l'exigence de prévisibilité posée notamment par l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH), lequel protège le droit au respect de la vie privée et de la correspondance.

Cela signifie que la loi doit être d'une clarté et d'une précision suffisantes pour fournir aux individus une protection adéquate contre les risques d'abus de l'exécutif dans le recours aux techniques de renseignement.

La nature des mesures susceptibles d'être mises en œuvre dans le cadre du projet de loi sur le renseignement implique des exigences fortes en matière de prévisibilité de la loi.¹

¹ Voir, à cet égard, la jurisprudence de la Cour européenne des droits de l'homme, notamment les arrêts suivants : *Amann c. Suisse* [GC], no 27798/95, § 50, CEDH 2000-II; *Malone c. Royaume-Uni*, 2 août 1984, série A no 82 ; *Kruslin c. France*, 24 avril 1990, série A no 176-A (concernant des écoutes et d'autres formes d'interception d'entretiens téléphoniques) ; *Klass et autres c. Allemagne*, 6 septembre 1978, série A n° 28.

Si la Cour européenne des droits de l'homme conçoit que l'exigence de prévisibilité ne saurait signifier qu'il faille permettre à quelqu'un de prévoir si et quand ses communications risquent d'être interceptées par les autorités, afin qu'il puisse régler son comportement en conséquence, **la loi doit user de termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions, elle habilite la puissance publique à opérer pareille atteinte secrète, et virtuellement dangereuse, au droit au respect de la vie privée et de la correspondance.**

Les ingérences dans le droit au respect de la vie privée sont d'une telle gravité qu'elles doivent reposer sur **des dispositions claires et détaillées, d'autant que les procédés techniques se diversifient et se perfectionnent.**

Les mêmes exigences sont posées par la jurisprudence de la Cour de justice de l'Union européenne (CJUE). Elles sont rappelées dans l'arrêt récent *Digital Rights Ireland* du 8 avril 2014 censurant la Directive 2006/24/CE du 15 mars 2006 sur les communications électroniques.²

La Cour y rappelle que les ingérences portées aux droits au respect de la vie privée et à la protection des données personnelles (protégés par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne) doivent reposer sur des dispositions claires et précises, permettant de garantir qu'elles sont effectivement limitées au strict nécessaire.³

a) La nécessité de préciser davantage les motifs d'intérêt public pouvant justifier une mise en œuvre des techniques de renseignement (Article 1^{er} du PL – L.811-3)

Le projet de loi énumère 7 motifs d'intérêt public (L.811-3).⁴ Il prévoit un champ d'intervention très large aux activités de renseignement.

Le champ d'application de la loi ne s'applique pas seulement aux actes de terrorisme mais aussi à des actes relevant de la criminalité et de la délinquance organisées ou à des « violences collectives ». Le champ d'application de la loi est donc très large et, eu égard à son objet, mérite d'être précisé.

Afin de circonscrire plus précisément ce champ, il serait nécessaire de définir par la loi chaque motif d'intérêt public de manière précise et restrictive. Il serait opportun à

² Directive sur la conservation des données générées ou traitées dans le cadre de la fourniture des services de communications électroniques accessibles au public ou de réseaux publics de communications. Ce texte oblige les fournisseurs de services de communications électroniques de conserver des données afin de les rendre accessibles aux autorités nationales compétentes, à des fins de prévention, de recherche, de détection et de poursuite des infractions graves. CJUE, *arrêt Digital Rights Ireland Ltd contre Minister for Communications, Marine and Natural Resources et autres (C-293/12) et Kärntner Landesregierung et autres (C-594/12)*, 8 avril 2014.

³ Arrêt précité, § 65.

⁴ 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 ; 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.

cet égard de faire explicitement référence aux avis et recommandations de la Commission nationale des interceptions de sécurité (CNIS) relatifs à la définition et l'interprétation des motifs d'intérêt public prévus par la loi du 10 juillet 1991, plusieurs d'entre eux ayant été repris dans le projet de loi (sécurité nationale, sauvegarde des éléments essentiels du potentiel scientifique et économique de la Nation, prévention du terrorisme, prévention de la criminalité et de la délinquance organisées et prévention de la reconstitution ou du maintien de groupement dissous).⁵

Par ailleurs, s'agissant du nouveau motif « *la prévention des violences collectives de nature à porter gravement atteinte à la paix publique* », celui-ci est trop imprécis.

Anticipant une évolution du nombre de motifs légaux, la CNIS soulignait dans son dernier rapport la nécessité de maintenir des définitions précises et restrictives, afin de respecter le caractère exceptionnel des raisons pouvant autoriser le recours à une mesure de surveillance.

Enfin, il y a lieu de rappeler que, pour être compatibles avec la CEDH, les mesures d'ingérence dans l'exercice des droits doivent être « prévues par la loi », c'est à dire, comportant des garanties minimales quant aux finalités poursuivies, aux catégories de personnes visées, aux durées d'exécution de ces mesures, etc⁶ ...

b) La nécessité de préciser les catégories de personnes susceptibles d'être visées par les activités de renseignement (article 1^{er} du PL – L.821-2, article 2 du PL – L.851-4 et 852-1, article 9 du PL, para. 3, 561-26)

Le projet de loi ne contient aucune précision sur les personnes qui pourraient faire l'objet de mesures de renseignement et ne définit pas les motifs pouvant justifier leur mise en place.

Ce dispositif apparaît en contradiction avec la jurisprudence européenne qui impose à la loi de contenir des dispositions précises sur les catégories de personnes pouvant potentiellement faire l'objet d'une mesure attentatoire au droit au respect de leur vie privée, les critères objectifs permettant d'identifier ces personnes et les motifs justifiant cette mesure.⁷

Dans son arrêt du 8 avril 2014 (*Digital Rights Ireland*)⁸, la CJUE a censuré la Directive 2006/24/CE « *Communications électroniques* » car elle concernait de manière globale l'ensemble des personnes faisant usage de services de communications électroniques, s'appliquant à des personnes pour lesquelles il n'existait aucun indice de nature à laisser croire que leur comportement puisse avoir un lien avec des infractions graves.⁹

⁵ Voir notamment les rapports d'activité de la CNIS.

⁶ Voir également CEDH, *Klass* précité et *Liberty et autres c. Royaume Uni*, 1^{er} juillet 2008.

⁷ Voir, par exemple, CEDH, *Kruslin*, précité.

⁸ CJUE, *arrêt Digital Rights Ireland Ltd (C-293/12) contre Minister for Communications, Marine and Natural Resources et autres et Kärntner Landesregierung (C-594/12) et autres*, 8 avril 2014.

⁹ CJUE, *arrêt Digital Rights Ireland Ltd*, précité, § 58.

C'est ce que rappelait également le rapport d'information de l'Assemblée nationale de 2013 sur l'évaluation du cadre juridique applicable aux services de renseignement, soulignant que l'absence de cette garantie pouvait justifier une condamnation de la Cour de Strasbourg : « *La loi doit indiquer les catégories de personnes susceptibles de faire l'objet de moyens spéciaux d'investigation ainsi que les cas dans lesquels la mise en œuvre de ces moyens est possible (...)* ». ¹⁰

Par ailleurs, à l'instar de la CNIL ¹¹ et de l'Ordre des avocats de Paris, il y a lieu de souligner le fait que le projet de loi ne prévoit aucune disposition concernant certaines professions (parlementaires, magistrats, avocats, journalistes...) alors que celles-ci bénéficient d'une protection au regard du droit interne et du droit européen.

S'agissant des journalistes, le code de procédure pénale (CPP) en application de la loi du 29 juillet 1881 sur la liberté de la presse interdit la transcription des correspondances avec un journaliste permettant d'identifier une source. ¹² Il convient également de rappeler que l'article 10 de la CEDH accorde à la presse et à la confidentialité des sources journalistiques une protection extrêmement étendue. ¹³

Quant aux parlementaires, le CPP prévoit qu'aucune interception ne peut avoir lieu sur la ligne d'un député ou d'un sénateur sans que le président de l'assemblée à laquelle il appartient en soit informé par le juge d'instruction. ¹⁴

Quant aux avocats, ils exercent une mission fondamentale, la défense des justiciables. Le secret professionnel des avocats, notamment les échanges avec leurs clients, est protégé par l'article 66-5 de la loi du 31 décembre 1971. L'article 100-5 du CPP alinéa 3 prohibe d'ailleurs la transcription des correspondances avec un avocat relevant de l'exercice des droits de la défense. ¹⁵

Il y a également lieu de rappeler que l'article 8 de la CEDH accorde une protection renforcée aux échanges entre les avocats et leurs clients, essentielle pour l'exercice de leur mission. La protection du secret professionnel est également le corollaire du droit qu'a le client d'un avocat de ne pas contribuer à sa propre incrimination. ¹⁶

Si le droit interne peut prévoir des ingérences à ce droit (perquisitions, saisies, écoutes), elles doivent être strictement nécessaires et proportionnées, et impérativement assorties de garanties particulières, les avocats occupant une position centrale dans l'administration de la justice.

Celles-ci peuvent impliquer que soient prises les mesures suivantes : une autorisation de mise en œuvre par le juge et qui soit motivée, informer et faire

¹⁰ Assemblée nationale, Commission des lois constitutionnelles, de la législation et de l'administration générale de la République, Rapport d'information de mai 2013 de la sur l'évaluation du cadre juridique applicable aux services de renseignement, présenté par Messieurs Urvoas et Verchère.

¹¹ CNIL, avis du 5 mars 2015.

¹² Article 100-5 du CPP.

¹³ Article protégeant la liberté d'expression. Voir, notamment, CEDH, *Goodwin c. Royaume-Uni*, arrêt du 27 mars 1996, § 39.

¹⁴ Article 100-7 du CPP.

¹⁵ Voir également Article 727-1 du CPP.

¹⁶ *Michaud c. France*, no 12323/11, 6 décembre 2012 et *André et autre c. France*, no 18603/03, § 41, 24 juillet 2008

intervenir le cas échéant le bâtonnier de l'Ordre des avocats dont relève l'avocat,¹⁷ mettre en place un contrôle efficace et accessible pour contester les mesures.¹⁸ A cet égard, il y a lieu de souligner que l'article 100-7 du CPP prévoit qu'aucune interception ne peut avoir lieu sur une ligne dépendant du cabinet d'un avocat ou de son domicile sans que le bâtonnier en soit informé par le juge.

En restant muet sur la situation de ces professions dites « à risque », le projet de loi semble contrevenir à la protection qui leur est garantie par les normes précitées.

C'est ce que reprochait la CJUE à la directive 2006/24/CE du 15 mars 2006 sur les communications électroniques dans son arrêt du 8 avril 2014 (*Digital Rights Ireland Ltd*). Le texte ne prévoyait aucune exception quant à son champ d'application, de sorte qu'il s'appliquait même à des personnes dont les communications étaient soumises, selon les règles du droit national, au secret professionnel.¹⁹

Dès lors, concernant les professions précitées, des garanties devront être inscrites dans la loi.

c) La nécessité de limiter l'accès aux techniques de renseignements à un nombre restreint de services et d'agents (Article 1^{er} du PL – 811-4)

Aux termes de l'article L.811-4, un décret en Conseil d'Etat sera pris pour désigner « *ceux des services autres que les services spécialisés de renseignement* » relevant des trois ministères qui pourraient être autorisés à recourir aux techniques de renseignement.

Ces dispositions permettraient donc à d'autres services que les services de renseignement de recourir aux techniques spéciales de renseignement. Or, en raison du caractère exceptionnel de ces mesures, **le recours à ces techniques devrait être ouvert à un nombre restreint de services dont seule la loi pourrait modifier la liste.**

d) Eclaircir l'articulation entre le projet de loi et les procédures judiciaires subséquentes (créer un nouvel article)

Compte tenu de la nature des mesures mises en œuvre, l'agent chargé du recueil de renseignements doit être tenu de mettre fin à la phase de police administrative dès lors qu'il ne s'agit plus de prévention mais de recherche ou de poursuites des preuves d'une infraction, et qu'il entre de ce fait dans une phase d'enquête de police judiciaire ; l'absence de garanties en matière de droits fondamentaux dans le texte actuel requiert d'amender la loi pour prévoir un critère objectif contraignant l'agent à mettre fin à la phase de police administrative et à engager la phase de police judiciaire qui comporte les garanties et contrôles nécessaires au respect des libertés individuelles – l'article 66 de la constitution est le fondement de cette exigence du contrôle judiciaire en matière de libertés fondamentales.

¹⁷ *André et autre*, précité.

¹⁸ *Pruteanu c. Roumanie*, n° 30181/05, §§ 48 et suivants.

¹⁹ CJUE, *arrêt Digital Rights Ireland Ltd (C-293/12 ; C-594/12) et autres*, 8 avril 2014, § 58.

Prévoir explicitement le recours de la Commission nationale de contrôle des techniques de renseignement (CNCTR) à l'article 40 du code de procédure pénale (CPP) pourrait être un moyen de contrôle efficace. La rédaction actuelle de l'article L.822-6 qui fait référence à l'article 40 précité est trop large et imprécise et ne permet concrètement aucun recours sur ce fondement surtout si les agents sont officiers de police judiciaire, ces derniers pouvant attendre avant d'informer le Procureur de la République (article 12 du CPP).

Compte tenu de l'absence de précisions du projet de loi sur l'articulation qui sera faite entre la phase administrative de surveillance et la procédure judiciaire, notamment les conséquences que peuvent avoir le projet de loi sur les procédures pénales subséquentes, d'autres questions se posent que l'on pourrait synthétiser autour de ces trois interrogations :

- ***quelles garanties existent pour s'assurer que le recours aux techniques de renseignements par la voie administrative ne soit pas un moyen pour contourner la procédure pénale ?***
- ***dans la mesure où le projet de loi légalise les moyens de recueillir des renseignements par la police administrative, les éléments recueillis pourront-ils concrètement servir de fondement à l'ouverture d'une procédure pénale à l'encontre d'un individu ? Dans l'affirmative, une autre série de questions se posent sur le respect effectif des droits de la défense de ce dernier, notamment - le droit d'accès par lui-même ou son représentant à ces éléments de renseignement qui seraient devenus des éléments de preuve et - le droit de disposer d'un recours effectif pour contester la régularité de la mesure de surveillance administrative litigieuse devant le Conseil d'Etat, sachant que le projet de loi ne leur autorise pas l'accès aux pièces ?***
- ***quelles seraient les éventuelles conséquences d'une décision du Conseil d'Etat constatant l'irrégularité de la mise en œuvre d'une technique de surveillance à l'égard d'une procédure pénale dans laquelle des renseignements recueillis auraient été versés au dossier ?***

Face à ces interrogations, au regard de la jurisprudence du Conseil constitutionnel, on peut estimer que les informations et éléments recueillis dans le cadre d'une enquête administrative ne sauraient constituer des éléments de preuve régulièrement exploitables dans le cadre d'une procédure pénale. En effet, le juge constitutionnel a jugé que « *le principe du contradictoire et le respect des droits de la défense impliquent en particulier qu'une personne mise en cause devant une juridiction répressive ait été mise en mesure, par elle-même ou par son avocat, de contester les conditions dans lesquelles ont été recueillis les éléments de preuve qui fondent sa mise en cause ; qu'en permettant ainsi qu'une condamnation puisse être prononcée sur le fondement d'éléments de preuve alors que la personne mise en cause n'a pas*

été mise à même de contester les conditions dans lesquelles ils ont été recueillis, [les dispositions attaquées] méconnaissent les exigences constitutionnelles qui résultent de l'article 16 de la Déclaration de 1789 »²⁰.

e) La conservation des données

Enfin, on soulignera que la durée de conservation des renseignements recueillis peut varier entre 30 jours et 5 ans, selon les techniques de renseignement (L.822-2). Outre que ces durées sont supérieures à celles prévues par la loi de 1991 et que plusieurs dérogations sont prévues pour prolonger la conservation ces données, il y a lieu de se demander si ces durées ne sont pas excessives au regard de la finalité poursuivie par la mesure et des exigences posées par la jurisprudence européenne, notamment par l'arrêt de la CJUE *Digital Rights Ireland* précité.

2. Le contrôle de la demande d'autorisation et de la mise en œuvre des techniques de renseignement

Compte tenu du caractère intrusif et attentatoire au droit au respect de la vie privée des mesures prévues par le projet de loi, les moyens de contrôle administratif et juridictionnel doivent être proportionnés.

A. Le contrôle administratif par la CNCTR

L'instauration d'une demande d'avis préalable à une autorité indépendante est à saluer. A cet égard, la CNIS souligne que ce dispositif de contrôle « *est plus efficace du point de vue de la protection des libertés publiques* »²¹.

Cependant, afin de permettre à cette commission d'exercer pleinement sa mission de contrôle de légalité, proportionnalité et de subsidiarité des demandes d'autorisation et de la mise en œuvre des mesures autorisées, en conformité avec les exigences posées par la jurisprudence européenne sur le droit au respect de la vie privée, **il serait nécessaire de renforcer ses pouvoirs tout en lui allouant les moyens humains et techniques nécessaires et de lui permettre d'exercer un contrôle immédiat et sans restriction**. Il y a lieu de rappeler que, dans son rapport sur le numérique et les droits fondamentaux de 2014, le Conseil d'Etat allait dans ce sens et proposait de « [doter la CNIS] de moyens humains renforcés sur le plan quantitatif et qualitatif, avec des compétences de haut niveau en matière d'ingénierie des communications électroniques, d'informatique et d'analyse des données ».

a) Le projet de loi prévoit que le contrôle a priori n'est pas systématique²² (Article 1^{er})

En effet, en cas d'urgence absolue, le Premier ministre pourra autoriser la mise en œuvre d'une technique de renseignement sans avis préalable de la Commission (L.821-5).

²⁰ CC, décision n° 2014 – 693 DC, 25 mars 2014, cdt 25 et 26.

²¹ CNCIS – 22e rapport d'activité 2013-2014.

²² Par exemple, en cas d'urgence absolue (L.821-5).

Il est surprenant qu'une telle dérogation soit prévue alors que pour la CNIS, celle-ci a été écartée, le Premier ministre ayant qualifié la pratique du contrôle *a priori* de « *pratique la mieux à même de répondre à l'objectif de protection efficace des libertés poursuivie par le législateur* ». ²³ La CNIS souligne que ce contrôle permet un dialogue utile avec les services demandeurs et une meilleure prise en compte par ceux-ci, dès le stade préparatoire, des éléments de la « jurisprudence » de la Commission .

Dès lors, **même en cas d'urgence absolue, l'avis préalable de la CNCTR devrait être sollicité, ses moyens devant lui permettre de faire face à de telles sollicitations.**

b) La nature de l'avis préalable de la Commission (Article 1^{er})

L'avis de la Commission ne semble être que consultatif. Le Premier ministre peut en effet autoriser la mise en œuvre d'une technique de renseignement malgré un avis défavorable de la Commission (L.821-3, 821-6).

En cas d'avis défavorable de la Commission non suivi par le Premier ministre, la procédure prévoit qu'elle puisse saisir le Conseil d'Etat mais à deux conditions (1- que les recommandations formulées par la Commission ne soient pas suivies par le Premier ministre ou que les mesures prises soient insuffisantes ; 2- qu'il y ait une majorité absolue des membres de la commission pour la saisine du Conseil d'Etat) (L.821-6).

En cas d'avis défavorable non suivi par le Premier ministre, afin de procéder sans délai à un contrôle juridictionnel de légalité et de proportionnalité des mesures mises en œuvre, la saisine du Conseil d'Etat par la CNCTR devrait être possible sans condition, le cas échéant, via une procédure de référé.

L'avis exprès de la Commission n'est pas non plus une condition préalable à la mise en œuvre du dispositif, l'avis étant « *réputé rendu* » en cas de dépassement des délais fixés par la loi (L.821-3).

Outre qu'il serait préférable qu'un avis exprès soit rendu avant la délivrance de l'autorisation par le Premier ministre, l'effectivité du contrôle *a priori* de la commission implique que celle-ci puisse matériellement exercer ces contrôles. Or, le projet de loi prévoit qu'elle doit statuer dans délais de 24 heures ou 3 jours en cas de doute sur la validité de la demande (L.821-3). Ces délais sont trop brefs. La CNIS dispose de plus de temps (48 heures et 7 jours). ²⁴

Pour effectuer un contrôle efficace en amont de la procédure, la CNCTR doit pouvoir être matériellement en mesure d'opérer les contrôles nécessaires (légalité, proportionnalité et subsidiarité).

c) La nature du contrôle

Le contrôle *a priori* opéré par la CNCTR portera sur la légalité de la demande d'autorisation de mise en œuvre d'une technique de renseignement, en particulier

²³ CNIS – 22e rapport d'activité 2013-2014, p.72.

²⁴ CNIS – 22e rapport d'activité 2013-2014, p.80, L.243-8 du code de la sécurité intérieure.

sur sa proportionnalité et sur sa subsidiarité (s'assurer de l'absolue nécessité de recourir à la mesure).

Le projet de loi précise que la demande d'autorisation doit être **écrite et motivée** (L.821-2). Ainsi que la CNIS le souligne, la qualité de la motivation de la demande est primordiale : « c'est la qualité de la motivation des demandes qui va mécaniquement induire la possibilité puis la qualité de ce contrôle ».

Dès lors, afin de permettre un contrôle exhaustif de la légalité de la demande d'autorisation par la CNCTR, la motivation de la demande devra être **suffisante, pertinente et sincère**. C'est ce qu'impose déjà la CNIS dans sa jurisprudence. Il serait opportun de faire explicitement référence à celle-ci afin de fixer les exigences relatives à la motivation de la demande.

d) Le contrôle a posteriori

Pour être suffisamment protecteur, le contrôle *a posteriori* effectué par la CNCTR doit être efficace. Pour cela, la Commission doit pouvoir exercer pleinement ses missions en ayant accès **sans restriction et sans délai** à l'ensemble des renseignements recueillis.

Or, il semble que ses pouvoirs soient affaiblis par rapport à ceux de la CNIS.²⁵ La CNCTR devrait en effet demander à chaque service de renseignement d'avoir accès aux registres et données, ce qui rendra impossible un contrôle « *en temps réel* » (Article 1^{er} du PL, L.822-1).

La CNCTR devrait pouvoir exercer **un contrôle immédiat** compte tenu du fait que certaines données collectées pourraient être détruites dans le délai d'un mois (L.822-2 II).

Enfin, compte tenu de la possibilité d'autoriser la mise en œuvre rapide des techniques de renseignement très intrusives sur plusieurs mois, **il faudrait permettre à la CNCTR de saisir directement le Conseil d'Etat et demander à celui-ci de statuer dans un bref délai. Il pourrait être utile de recourir à la procédure de référé (L.773-2)**. Cela constituerait une garantie supplémentaire qui permettrait de ne pas laisser perdurer des situations qui seraient illégales.

B. Le contrôle juridictionnel par le Conseil d'Etat (Articles 4 et 5 du PL)

Le Défenseur des droits se félicite de l'intervention d'un contrôle juridictionnel, naturellement confié au Conseil d'Etat, juge administratif suprême des activités des administrations.

Cependant, au vu des règles procédurales dérogatoires applicables lorsqu'est en cause le secret de la défense nationale (L.773-1 et suivants), de nombreuses questions subsistent à ce stade de l'élaboration du projet de loi quant au caractère effectif de la voie de recours ainsi prévue et des garanties que la CEDH fixe en

²⁵ La CNIS accède, semble-t-il, aux renseignements recueillis par les services de renseignements via le groupement interministériel de contrôle.

contrepartie des restrictions apportées aux droits de la défense pour assurer, malgré tout, les conditions d'un procès équitable²⁶.

La Cour de Strasbourg conçoit que le droit à un procès pleinement contradictoire peut être restreint dans la mesure strictement nécessaire à la sauvegarde d'un intérêt public important tel que la sécurité nationale ou la nécessité de garder secrètes certaines méthodes policières de recherche des Infractions. Toutefois, elle estime que l'équité du procès impose que toutes les difficultés causées à la défense par une limitation de ses droits doivent être suffisamment compensées par la procédure suivie devant les autorités judiciaires, notamment par l'existence des garanties suivantes : le caractère non absolu de l'interdiction de divulgation des renseignements recueillis, la possibilité pour l'organe de contrôle de divulguer les documents et les informations pertinents au plaignant lorsque celui-ci a obtenu satisfaction, l'accès sans restriction des victimes potentielles à l'organe de contrôle sans avoir à surmonté un obstacle probatoire.²⁷

Le projet de loi ne présente pas ces garanties. Il n'offre pas de contrepoids suffisant aux restrictions apportées à l'exercice des droits.

On relèvera tout d'abord les difficultés procédurales attachées à ce que ce recours puisse être effectivement exercé, les mesures de surveillance des services de renseignement étant par nature secrètes et la faculté de justifier d'un intérêt direct et personnel, hypothétique.

Comment s'insurger contre une erreur fondée sur l'homonymie ?

Par ailleurs, on s'interrogera sur la faculté qu'aura le potentiel requérant soupçonnant d'être surveillé d'exercer utilement ce recours - en l'absence d'informations lui permettant de contester la légalité et la proportionnalité de la mesure, lesquelles ne ressortiront pas de la décision de la CNCTR qui ne sera pas motivée (celle-ci se bornant à au réclamant qu'elle « *a procédé aux vérifications nécessaires* » (L.833-3), - sans instruction écrite, et - sans avoir accès aux pièces du dossier. Dans l'étude d'impact du projet de loi, il est admis que le contentieux aura lieu sans décision, sans instruction écrite et contradictoire et que le requérant ne pourra pas soulever les moyens pertinents et devra se reposer sur le Conseil d'Etat qui « pourrait relever tout moyen d'office ».²⁸

Les pièces versées à la procédure seront en revanche à la disposition de la juridiction et de la partie adverse (et de la Commission si elle intervient). Or, le principe de l'égalité des armes garanti par l'article 6 de la CEDH implique que la partie puisse présenter sa cause « *dans des conditions qui ne la placent pas dans une situation défavorable par rapport à son adversaire* ».²⁹

Par ailleurs, outre les incertitudes sur le déroulement de l'audience et la forme que prendra la décision du Conseil d'Etat, mais aussi les conditions de sa motivation et de sa notification au réclamant en cas de constat d'illégalité de la mesure contestée, on relève que l'annulation et la destruction des renseignements recueillis

²⁶ Voir, par exemple, CDH, Kennedy c. Royaume Uni, 18 mai 2010.

²⁷ CEDH, précité, §§ 184 et suivants.

²⁸ Etude d'impact,

²⁹ CEDH, Foucher c. France, 18 mars 1997, § 34.

irrégulièrement ne seront pas ordonnés automatiquement mais laissés à l'appréciation de la juridiction (L.773-7, « elle *peut* annuler (...) »). Là encore se pose la question de l'effectivité d'un tel recours qui est supposé mettre fin à la violation du droit au respect de la vie privée (annulation de l'autorisation) et redresser la situation (destruction des données et indemnisation).

Dans une récente affaire relative à l'interception des conversations téléphoniques d'un avocat, la Cour européenne des droits de l'homme a rappelé qu'un recours « efficace » au sens de l'article 8 de la CEDH doit permettre la réalisation d'un contrôle de la légalité des enregistrements litigieux et à aboutir, le cas échéant, à une décision ordonnant la destruction de ceux-ci.³⁰



Dans le cadre de ses différentes missions, en application de l'article 33 de la loi organique du 29 mars 2011 permet au Défenseur des droits peut, de sa propre initiative, à la demande d'une partie ou à la diligence de la juridiction concernée, présenter des observations ou être entendu.

Le présent projet de loi ne saurait remettre en cause ou entraver ces prérogatives.

Concernant leur mise en œuvre, aucun principe de droit ne vient s'opposer à ce qu'à titre individuel, le Défenseur des droits lui-même ou certains de ces agents expressément identifiés, soient habilités au secret de la défense nationale, à l'instar des membres du Conseil d'Etat qui seront expressément désignées pour connaître de ces contentieux.

³⁰ *Pruteanu c. Roumanie*, précité, § 55.