Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PROJET DE LOI

relatif au renseignement

ETUDE D'IMPACT

NOR : PRMX1504410L/Bleue-1

18 MARS 2015

SOMMAIRE

INTRODUCTION

La recherche du renseignement constitue un impératif majeur pour la sécurité de la France, de sa population et de son territoire.

Le caractère nécessairement confidentiel du renseignement ne doit pas pour autant permettre une absence d'encadrement rigoureux dont les conséquences peuvent être préjudiciables. Les récents événements qui se sont déroulés sur le territoire national ont mis en exergue les limites du dispositif actuel (partie I) et la nécessité pour les services de renseignement de disposer d'un cadre juridique unifié conférant aux agents des moyens efficaces.

Les évolutions législatives proposées ont donc pour objectifs de :

- donner aux services spécialisés de renseignement des moyens d'action adaptés à la diversité de leurs missions et à l'évolution tant des techniques que des menaces ;
- renforcer la sécurité juridique de leur action ;
- adapter le contrôle de ces services pour asseoir la légitimité de leur action et garantir une meilleure protection des libertés individuelles (partie II).

Partie 1 - Etat des lieux et diagnostic

1.1. Etat des lieux et application de la législation relative au renseignement

1.1.1. Etat des lieux

1.1.1.1. Origine des dispositions relatives au renseignement

La loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques constitue le socle de l'encadrement de la mise en œuvre des techniques de renseignement. Codifiée dans le code de la sécurité intérieure, elle crée un régime général permettant l'autorisation de mise en œuvre des interceptions de sécurité hors la décision d'un juge judiciaire et sous le contrôle d'une nouvelle autorité administrative indépendante : la commission nationale de contrôle des interceptions de sécurité (CNCIS).

L'article 6 de la loi « anti-terroriste » du 23 janvier 2006 (codifié dans le code des postes et communications électroniques – article L.34-1 et suivants) a étendu les modalités d'accès aux données de connexion par les services de renseignement sous le contrôle d'une personnalité qualifiée.

L'article 20 de loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale (LPM) a procédé à l'unification des régimes d'accès administratifs aux données de connexion, sans modifier les dispositions relatives aux interceptions de sécurité. Il a également introduit un régime propre à la géolocalisation en temps réel grâce aux informations fournies par les réseaux ou services de communications électroniques. Toutefois, cette loi n'a pas permis de répondre à l'ensemble des besoins opérationnels qui supposent l'adoption de nouvelles dispositions législatives pour sécuriser encore davantage l'ensemble des pratiques de géolocalisation dans un cadre administratif.

1.1.1.2. Etat actuel de la législation

En l'état du droit, les services de renseignement ne disposent que de moyens limités : les interceptions de sécurité, l'accès aux données de connexion ainsi qu'un accès limité à certains traitements de données à caractère personnel.

1.1.1.2.1. Les interceptions de sécurité

Depuis l'ordonnance du 12 mars 2012 qui a présidé à la codification de la loi de 1991, les interceptions de sécurité sont régies par les articles L. 241-1 à L. 245-3 du code de la sécurité intérieure.

Ces interceptions s'inscrivent dans le cadre de finalités limitativement énumérées par l'article L. 241-2 : la recherche « *des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de l'article L. 212-1* ».

L'autorisation prévue à l'article L. 241-2 du code de la sécurité intérieure est accordée par décision écrite et motivée du Premier ministre ou de l'une des deux personnes spécialement déléguées par lui. Elle est donnée sur proposition écrite et motivée du ministre de la défense, du ministre de l'intérieur ou du ministre chargé des douanes, ou de l'une des deux personnes que chacun d'eux aura spécialement déléguées. Le Premier ministre, en l'occurrence le groupement interministériel de contrôle (GIC), organise la centralisation de l'exécution des interceptions autorisées.

Cette autorisation est donnée pour une durée maximum de quatre mois. Elle cesse de plein droit de produire effet à l'expiration de ce délai. Elle ne peut être renouvelée que dans les mêmes conditions de forme et de durée. Le nombre d'autorisations en vigueur au même moment est contingenté.
La mise en œuvre de ces interceptions s'effectue sous le contrôle d'une autorité administrative indépendante, la commission nationale de contrôle des interceptions de sécurité (CNCIS). La décision motivée du Premier ministre mentionnée à l'article L. 242-1 est communiquée dans un délai de quarante-huit heures au plus tard au président de la Commission nationale de contrôle des interceptions de sécurité. Si celui-ci estime que la légalité de cette décision n'est pas certaine, il réunit la commission, qui statue dans les sept jours suivant la réception par son président de la communication mentionnée au premier alinéa. Au cas où la commission estime qu'une interception de sécurité a été autorisée en méconnaissance des dispositions du présent titre, elle adresse au Premier ministre une recommandation tendant à ce que cette interception soit interrompue. Elle porte également cette recommandation à la connaissance du ministre ayant proposé l'interception et du ministre chargé des communications électroniques.

La commission peut adresser au Premier ministre une recommandation relative au contingent et à sa répartition mentionnés à l'article L. 242-2. Le Premier ministre informe sans délai la commission des suites données à ses recommandations.

Par ailleurs, de sa propre initiative ou sur réclamation de toute personne y ayant un intérêt direct et personnel, la commission peut procéder au contrôle de toute interception de sécurité en vue de vérifier si elle est effectuée dans le respect des dispositions du code de la sécurité intérieure
Si la commission estime qu'une interception de sécurité est effectuée en violation des dispositions du code de la sécurité intérieure, elle adresse au Premier ministre une recommandation tendant à ce que cette interception soit interrompue.

La CNCIS effectue un contrôle rigoureux de la proportionnalité de la demande, en particulier lorsque le motif de prévention du terrorisme est avancé. Dans ce domaine, la définition retenue par la CNCIS est celle du droit pénal : la commission intentionnelle d'actes en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur. Dès lors, la surveillance de mouvements extrémistes ne relève pas nécessairement de la prévention du terrorisme. Comme l'indique la CNCIS dans son 20ème rapport, « *le prosélytisme religieux, comme l'expression d'opinions extrêmes, dès lors qu'elles ne tombent pas sous le coup de la loi, ne justifient pas, en tant que tels, une demande d'interception, s'ils ne comportent aucune menace immédiate pour l'ordre public républicain, matérialisée par exemple par un appel ou un encouragement à la violence* ».

La motivation de la demande doit donc répondre à trois critères. Elle doit être suffisante, pertinente et sincère. Le service doit ainsi identifier précisément la cible et son implication personnelle dans des agissements en rapport avec le motif avancé. Il s'agit alors de permettre à la CNCIS d'évaluer la proportionnalité entre l'atteinte projetée à la vie privée et la gravité de la menace. Le respect de ce principe la conduit d'ailleurs, comme l'exige la loi, à exclure des transcriptions résultant de l'interception de sécurité les parties des conversations qui n'apportent aucune information pertinente au regard de la finalité poursuivie par la surveillance. La Commission vérifie également que la demande ne poursuit pas d'autres buts que celui affiché pour justifier cette surveillance.

La rigueur de ces conditions ainsi que l'existence d'un quota d'interceptions autorisées, fixé par le Premier ministre, expliquent le nombre limité de cas de mise en œuvre de ces techniques de renseignement. En 1991, il s'établissait à 1180 puis à 1840 en 2009 avant de faire l'objet d'une revalorisation à 2190 en 2014. Les interceptions sont réparties entre les ministères de la Défense (285), du Budget (120) et de l'Intérieur (1785), ce dernier bénéficiant de plus de trois-quarts du total. La relative faiblesse du chiffre peut surprendre au regard du nombre de téléphones en usage sur le territoire national ou de celui des réquisitions judiciaires (650 000 réquisitions en 2012 dont 35 000 interceptions judiciaires), mais le législateur avait souhaité, par l'instauration de ce contingent, préserver le caractère exceptionnel de telles interceptions et, par là même, les libertés publiques. Sa mise en œuvre visait également à inciter les services à interrompre le plus rapidement possible les écoutes devenues inutiles, afin de pouvoir en solliciter de nouvelles[1].

Il convient par ailleurs de relever que la commission a fait évoluer sa jurisprudence, en admettant que le contingent devait porter non plus sur des lignes téléphoniques mais bien sur des personnes et donc sur l'ensemble des modes de communications qu'elles utilisent[2].
.

1.1.1.2.2. L'accès aux données de connexion

Antérieurement à la loi de programmation militaire du 18 décembre 2013, l'accès aux données de connexion par les services de renseignement relevait d'un double régime.

- *Le régime juridique antérieur à la loi du 18 décembre 2013*

L'accès aux données de connexion dans un cadre administratif préventif était régi par deux fondements juridiques distincts, en fonction des finalités :

<u>- La loi du 10 juillet 1991 relative au secret des correspondances émises par voie électronique (codifiée dans le code de la sécurité intérieure)</u>

L'article 22 de la loi du 10 juillet 1991, codifié à l'article L. 244-2 du code de la sécurité intérieure, prévoyait expressément l'accès aux données techniques de connexion dans le but de réaliser une interception de sécurité.

---

[1] Rapport de la délégation parlementaire au renseignement, relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2014 par M. Jean-Jacques URVOAS.

[2] Rapport de la délégation parlementaire au renseignement, relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2014 par M. Jean-Jacques URVOAS.

La procédure passait et passe encore par le groupement interministériel de contrôle (GIC), relevant du Premier ministre. Elle est placée sous le contrôle de la Commission nationale de contrôle des interceptions de sécurité (CNCIS).

De longue date, les services des ministères de l'intérieur et de la défense utilisaient ce fondement et cette procédure aussi bien pour les demandes d'accès « autonomes » aux données de connexion, c'est-à-dire non suivies d'interceptions de sécurité, que pour les demandes d'accès « préparatoires », lorsque les données de connexion recherchées visaient à identifier des personnes ou numéros nécessaires à la mise en œuvre d'une interception de sécurité. L'accès « autonome » aux données de connexion était accepté par la CNCIS sur le fondement d'une interprétation extensive de cette procédure.

- L'article 6 de la loi « anti-terroriste » du 23 janvier 2006 (codifié dans le code des postes et communications électroniques – article L.34-1 et suivants)

La loi « anti-terroriste » du 23 janvier 2006 avait créé une procédure spécifique d'accès aux données de connexion en matière de prévention du terrorisme.

Elle permettait aux services de police et de gendarmerie d'exiger des opérateurs de communications électroniques la transmission des données de connexion. Les services adressaient les demandes à une « personnalité qualifiée ». Celle-ci était placée auprès du ministre de l'intérieur, mais désignée et contrôlée par la CNCIS, autorité administrative indépendante. Après avoir vérifié le bien-fondé de la demande, la personnalité qualifiée délivrait une autorisation de transmission de la demande à l'opérateur concerné. La CNCIS effectuait aussi un contrôle *a posteriori*.

L'article 6 de la loi du 23 janvier 2006 prévoyait une procédure de demande et de contrôle formalisés. Validé par le Conseil constitutionnel, il constituait une base juridique incontestable, protectrice des agents des services demandeurs comme des opérateurs de communication électronique.

Mais cet article ne constituait qu'une base juridique partielle au regard des missions des services de renseignement : adopté à titre temporaire seulement (3 ans renouvelés deux fois par le Parlement, qui devaient expirer le 31 décembre 2015), il était limité à la seule finalité anti-terroriste, soit une fraction seulement des compétences de la DCRI, et, même au sein de la prévention du terrorisme, il ne couvrait que les services du ministère de l'intérieur (et non la DGSE, la DPSD ou TRACFIN).

- *Le défaut d'encadrement législatif de la géolocalisation en temps réel*

Les services de police et de gendarmerie avaient également recours à la géolocalisation en temps réel de terminaux téléphoniques ou informatiques.

Si elle acceptait le recours à cette prestation depuis 2010, la CNCIS considérait qu'elle reposait sur une base juridique trop fragile, eu égard à la jurisprudence de la Cour européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH) sur les mesures de surveillance attentatoires à la vie privée. En effet, la CEDH analysait ces mesures comme des ingérences d'une autorité publique dans la vie privée, ingérences qui méconnaissent l'article 8 de la Convention sauf lorsqu'elles sont explicitement prévues par la loi, clairement énoncées, nécessaires à la poursuite d'un ou plusieurs buts légitimes énoncés et

proportionnées au motif de sécurité poursuivi. C'est pourquoi, après avoir décidé d'y mettre fin au 31 décembre 2012, la CNCIS avait accepté de proroger sa doctrine constructive jusqu'au 31 décembre 2013, en contrepartie de l'engagement du gouvernement de proposer une modification rapide de la loi.

- *Le régime juridique actuel*

L'article 20 de la loi de programmation militaire a procédé à l'unification des deux régimes d'accès administratifs aux données de connexion, sans modifier les dispositions relatives aux interceptions de sécurité[3]. Il a également introduit un régime propre à la géolocalisation en temps réel grâce aux informations fournies par les réseaux ou services de communications électroniques.

Cet article a ajouté un sixième chapitre au titre IV du livre II du code de la sécurité intérieure, lequel titre régit la pratique des interceptions de sécurité et, désormais, l'accès « administratif » aux données de connexion.

- *Définition des données de connexion*

En application du nouveau régime juridique et comme cela était déjà le cas sous l'empire du régime précédent, l'accès aux données de connexion ne permet pas de connaître le contenu des échanges effectués par les personnes surveillées.

Les services de renseignement peuvent accéder, en vertu de ce dispositif , aux informations et documents concernant les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communication électronique, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, aux données relatives à la localisation des équipements terminaux utilisés ainsi qu'aux données techniques relatives aux communications d'un abonné portant sur la liste des numéros appelés et appelant, la durée et la date des communications.

Il ne s'agit donc que de la collecte de toutes les « traces » d'une connexion ou d'un appel, des factures détaillées dont dispose chaque abonné. Jamais l'accès au contenu d'une connexion ou d'un appel n'est permis.

La loi du 18 décembre 2013 n'a donc pas créé de nouveaux moyens mais a unifié et clarifié le droit, condition indispensable pour un contrôle démocratique[4].

- *Les conditions de mise en œuvre*

La loi encadre très strictement les conditions de mise en œuvre de cet accès. Les demandes écrites et motivées des agents sont soumises à une « personnalité qualifiée » qui, placée auprès du Premier ministre mais œuvrant sous le contrôle de la CNCIS, s'assure de la légalité de la demande. La demande doit s'inscrire dans le cadre des finalités définies par l'article L. 241-2 du code de la sécurité intérieure : la sécurité nationale, la sauvegarde des éléments

---

[3] L'article L. 244-2 a donc été conservé mais a retrouvé la portée qui était la sienne à l'origine : permettre l'accès aux données de connexion dans le seul objectif de permettre une interception de sécurité ultérieure.

[4] Rapport de la délégation parlementaire au renseignement, relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2014 par M. Jean-Jacques URVOAS.

essentiels du potentiel scientifique et économique de la France, la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous.

Parallèlement, la personnalité qualifiée vérifie la proportionnalité de la demande déposée.

Enfin, la personnalité qualifiée informe la CNCIS de ses décisions afin que celle-ci puisse exercer ses pouvoirs de contrôles énumérés par les articles L. 243-8 à L. 243-12 du code de la sécurité intérieure.

- *Les conditions particulières de la transmission des données de connexion en temps réel*

Le régime d'autorisation et de contrôle de la transmission en temps réel des données de connexion – notamment les données de géolocalisation – est aligné sur celui des interceptions de sécurité. Pour qu'une telle opération soit autorisée, elle devra être sollicitée par les ministres compétents auprès du Premier ministre, lequel consultera la CNCIS qui exercera alors le même type de contrôle, exigeant et minutieux, qu'en matière d'interceptions de sécurité.

1.1.1.2.3. La mise en œuvre de traitements de données à caractère personnel et l'accès à des traitements mis en œuvre par d'autres services de l'Etat

Les services de renseignement peuvent mettre en œuvre les traitements nécessaires à l'exploitation des données qu'ils collectent au cours de leurs investigations. En application du III de l'article 26 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, les textes portant création de ces fichiers ont été dispensés de publication par un décret du 27 juin 2008. Tel est le cas du fichier relatif à la centralisation du renseignement intérieur pour la sécurité du territoire et des intérêts nationaux (CRISTINA) mis en œuvre par la DGSI, du « *fichier de la DGSE* », du « *fichier du personnel de la DGSE* » ou du fichier de personnes étrangères de la direction du renseignement militaire.

Par ailleurs, les services de renseignement peuvent également accéder à des traitements mis en œuvre par d'autres services de l'Etat. Conformément à l'article L. 222-1 du code de la sécurité intérieure, pour les besoins de la prévention des atteintes aux intérêts fondamentaux de la Nation et des actes de terrorisme, les agents individuellement désignés et dûment habilités de ces services peuvent, dans les conditions fixées par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, avoir accès aux traitements automatisés suivants :

1° Le fichier national des immatriculations ;
2° Le système national de gestion des permis de conduire ;
3° Le système de gestion des cartes nationales d'identité ;
4° Le système de gestion des passeports ;
5° Le système informatisé de gestion des dossiers des ressortissants étrangers en France ;
6° Les données à caractère personnel, mentionnées aux articles L. 611-3 à L. 611-5 du code de l'entrée et du séjour des étrangers et du droit d'asile, relatives aux ressortissants étrangers qui, ayant été contrôlés à l'occasion du franchissement de la frontière, ne remplissent pas les conditions d'entrée requises ;
7° Les données à caractère personnel mentionnées à l'article L. 611-6 du même code.

Cette disposition, initialement limitée au 31 décembre 2012 puis dont l'effet a été prolongé au 31 décembre 2015 par la loi n°2012-1432 du 21 décembre 2012, a été pérennisée par la loi du 13 novembre 2014.

Enfin, les services de renseignement peuvent accéder aux données relatives aux déplacements internationaux, notamment aériens, des personnes. Il s'agit des données API (*advanced passenger information system*), qui portent sur l'identité des passagers et les informations relatives au document de voyage utilisé – passeport, carte nationale d'identité, visa, carte d'embarquement –, et des données PNR (*passenger name record*). Les données PNR sont recueillies, par les compagnies aériennes, au moment de la réservation du vol, contrairement aux données API, qui le sont seulement au moment de l'enregistrement du passager à l'aéroport. Les données PNR permettent d'anticiper les déplacements d'une personne identifiée par les services de renseignement et comportent des informations plus opérationnelles.

En France, les données API sont enregistrées, dans le cadre des finalités des articles L. 232-1 et L. 232-2 du code de la sécurité intérieure, au sein du traitement SETRADER, auquel les services de renseignement ont accès en application de l'article L. 232-2 du code de la sécurité intérieure. Ce fichier peut notamment faire l'objet d'une mise en relation avec le fichier des personnes recherchées (FPR).

Dans l'attente de l'adoption puis de la transposition d'une proposition de directive relative à l'utilisation des données PNR pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, l'article 17 de loi de programmation militaire (codifié à l'article L. 232-7 du code de la sécurité intérieure) a autorisé le gouvernement français, à titre expérimental (jusqu'au 31 décembre 2017) :

- à créer et à mettre en œuvre un traitement des données des passagers aériens (données de réservation (PNR) et données d'enregistrement (API)) collectées au cours des vols à destination et en provenance du territoire national, à l'exception des vols reliant deux points de la France métropolitaine,

- et ayant pour finalité la prévention et de la constatation des actes de terrorisme, des infractions mentionnées à l'article 695-23 du code de procédure pénale et des atteintes aux intérêts fondamentaux de la Nation, du rassemblement des preuves de ces infractions et de ces atteintes ainsi que de la recherche de leurs auteurs.

La mise en œuvre de ce traitement a nécessité l'adoption de deux actes réglementaires :

- le décret n° 2014-1095 du 26 septembre 2014 portant création d'un traitement de données à caractère personnel dénommé «système API-PNR France» pris pour l'application de l'article L. 232-7 du code de la sécurité intérieure
- le décret n° 2014-1566 du 22 décembre 2014 portant création d'un service à compétence nationale dénommé « Unité Information Passagers » (UIP)**,**
-

Enfin, en vertu de l'article L. 234-2 du code de la sécurité intérieure, les services ont accès au traitement des antécédents judiciaires dans le cadre d'enquêtes administratives ou pour l'exercice de missions ou d'interventions (L. 234-3).

En conclusion, la loi n'attribue que des moyens limités aux services de renseignement, notoirement insuffisants eu égard à la réalité de leur action quotidienne et à l'état de la menace. Les services spécialisés sont dès lors contraints de s'exposer à des risques importants pour continuer à remplir leur mission dans des conditions optimales.

1.1.2. Les limites de la législation relative au renseignement

La proposition de réformer l'architecture normative du renseignement a rencontré un écho favorable à l'occasion du conseil national du renseignement du 9 juillet 2014 présidé par le Président de la République. Il s'agit d'ailleurs d'une thématique récurrente dans les écrits consacrés à la politique publique du renseignement (Livres blancs sur la défense et la sécurité nationale de 2008 et 2013, rapports de la Délégation parlementaire au renseignement ou de parlementaires).

Cette réforme est d'autant plus incontournable qu'elle permettra de combler un retard préjudiciable[5]. La France demeure en effet la seule démocratie occidentale à ne pas bénéficier d'un cadre juridique cohérent en la matière, laissant de ce fait les services de renseignement dans une incertitude juridique et créant les conditions d'une condamnation de la France par la CEDH.

1.1.2.1. L'absence de définition des activités de renseignement

Le renforcement de la protection des libertés individuelles nécessite l'adoption d'un cadre législatif ayant pour objet d'encadrer l'ensemble des techniques de renseignement, les services habilités à les mettre en œuvre et sous quelles conditions.

1.1.2.2. Les pouvoirs de la CNCIS limités à certaines techniques de renseignement

Les moyens de la CNCIS, qui n'ont pas évolué depuis la loi du 10 juillet 1991, alors que son champ de compétence a été considérablement étendu par la création d'une procédure d'accès aux métadonnées, sont insuffisants.

Comme l'ont relevé tant la CNCIS elle-même au fil de ses rapports annuels qu'une mission d'information récente de l'Assemblée nationale, ces moyens ne sont manifestement pas suffisants pour assurer un contrôle effectif de la surveillance des communications. Pour les seules demandes d'accès aux métadonnées dans le cadre de la loi du 23 janvier 2006, la CNCIS est saisie de près de 600 décisions de la personnalité qualifiée chaque semaine.
L'octroi de moyens supplémentaires n'implique pas pour autant un changement de la nature de l'autorité chargée du contrôle. Trois modèles sont envisageables : le contrôle par une autorité judiciaire ; le contrôle par une émanation du Parlement ; le contrôle par une autorité administrative indépendante.

---

[5] Rapport de la délégation parlementaire au renseignement, relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2014 par M. Jean-Jacques URVOAS.

Si en France, le contrôle *a priori* par le juge est réservé aux interceptions judiciaires et est écarté pour les interceptions administratives pratiquées à des fins de prévention, il est appliqué à ces interceptions préventives aux États-Unis et, dans une certaine mesure, au Royaume-Uni. En France cependant, cette solution est exclue par la jurisprudence du Conseil constitutionnel, selon laquelle la réquisition et le traitement des «données de trafic», ayant pour finalité la prévention des actes de terrorisme, constituent de pures opérations de police administrative et ne peuvent en aucun cas relever de la compétence de l'autorité judiciaire.

Le deuxième type de contrôle existe depuis qu'une loi du 9 octobre 2007 a créé une délégation parlementaire au renseignement (DPR). La LPM du 18 décembre 2013 a accru ses pouvoirs en lui donnant un rôle de contrôle de l'action du gouvernement en matière de renseignement et non plus seulement de suivi de cette action. Toutefois, la jurisprudence du Conseil constitutionnel, selon laquelle le Parlement ne peut connaître d'opérations en cours, ne lui permet d'exercer son contrôle qu'*a posteriori*. La DPR ne pourrait donc pas reprendre les attributions de la CNCIS, qui contrôle les interceptions durant leur réalisation. Le modèle de contrôle par une AAI, pratiqué par la France depuis 1991, doit donc être maintenu tout en étant renforcé.

Le Conseil d'Etat, dans son rapport « Le numérique et les droits fondamentaux » propose ainsi de faire de la CNCIS une autorité de contrôle des services de renseignement, dotée 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.

De même, une amélioration de l'effectivité des voies de recours offertes au citoyen lorsque la mise en œuvre d'une technique de renseignement lui cause un préjudice constituerait un progrès notable de l'État de droit[6].

1.1.1.2.3. Un régime d'autorisation imparfaitement unifié

L'article 20 de la loi de programmation militaire a maintenu la «personnalité qualifiée », qui continuera à prendre des décisions en l'absence d'avis de la CNCIS et sans regard possible du Premier ministre ou de son délégué qui autorise les interceptions de sécurité. Par ailleurs, l'autorisation de la géolocalisation en temps réel relève d'un troisième régime. Le risque d'incohérence entre les différentes autorisations susceptibles d'être délivrées concernant un même objectif est donc important.

La CNCIS a fréquemment rappelé sa préférence pour la définition d'un régime unique dans le cadre de la loi du 10 juillet 1991, aujourd'hui titre IV du livre II du code de la sécurité intérieure, basé sur la quadruple distinction entre l'autorité qui demande, celle qui contrôle, celle qui autorise et celle qui met en œuvre. Il s'agirait d'assurer l'équilibre entre, d'une part, les impératifs de sécurité, et, d'autre part, la protection des droits et des libertés individuelles, en consacrant la séparation entre les services habilités relevant de ministères demandeurs et l'autorité de décision.

1.1.1.2.4. Le risque pénal des agents des services de renseignement

[6] « Le numérique et les droits fondamentaux ». Rapport du Conseil d'Etat. Etude annuelle 2014.

L'insécurité juridique pour les fonctionnaires du renseignement qui agissent sur le territoire national est aujourd'hui de moins en moins acceptée par les nouvelles générations de personnels, acteurs décisifs de cette fonction publique stratégique.

C'est pourquoi, afin de protéger les agents de ces services de renseignement, la loi devrait donc les autoriser à mettre en œuvre ces différentes techniques de renseignement. Leur responsabilité pénale ne pourrait être alors recherchée puisque, aux termes du premier alinéa de l'article 122-4 du code pénal, « *N'est pas pénalement responsable la personne qui accomplit un acte prescrit ou autorisé par des dispositions législatives ou réglementaires* ».

C'est le cas en matière d'enquête judiciaire : l'officier de police judiciaire et le juge d'instruction, lorsqu'ils mettent en œuvre des interceptions téléphoniques ou des sonorisation, ne commettent pas le délit d'atteinte à l'intimité de la vie privée prévu à l'article 226-1 du code pénal parce qu'ils agissent en application des articles 100 ou 706-96 du code de procédure pénale. Aucune immunité pénale n'est pourtant explicitement prévue, elle résulte directement et de manière suffisante de l'application de l'article 122-4 du code pénal.

Enfin, il est indispensable de renforcer la protection de l'anonymat des agents. Celle-ci est en effet malmenée à divers titres[7].

1.2. Cadre constitutionnel et conventionnel

1.2.1. Cadre constitutionnel

1.2.1.1 Les mesures de surveillance constituent des atteintes au droit au respect de la vie privée

Si, à l'origine, le Conseil constitutionnel a retenu une conception extensive de la liberté individuelle en y incluant les libertés fondamentales de la personne, telles que la liberté d'aller et de venir, l'inviolabilité du domicile, la liberté du mariage ou le respect de la vie privée, tel n'est plus le cas depuis 1999 (*décision n° 99-411 du 16 juin 1999, Loi portant diverses mesures relatives à la sécurité routière et aux infractions sur les agents des exploitants de réseau de transport public de voyageurs*).

Le droit au respect de la vie privée entre désormais dans le champ de la liberté personnelle proclamée par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789, laquelle implique notamment, le droit au secret des correspondances et à l'inviolabilité du domicile. (2013-357 QPC, 29 novembre 2013, cons. 6, JORF du 1er décembre 2013, p. 19603, texte n° 30, Rec. p. 1053 ; 2013-679 DC, 4 décembre 2013, cons. 38, JORF du 7 décembre 2013, p. 19958, texte n° 8, Rec. p. 1060).

1.2.1.2 En tant que telle, la protection de cette liberté n'est pas de la compétence exclusive du juge judiciaire

La compétence exclusive du juge judiciaire, prévue par l'article 66 de la Constitution, est désormais limitée à une définition plus étroite de la liberté individuelle, ne renvoyant plus qu'à la question de la privation de liberté (garde à vue, détention, rétention, hospitalisation

[7] Rapport de la délégation parlementaire au renseignement, relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2014 par M. Jean-Jacques URVOAS.

sans consentement).Le Conseil constitutionnel considère désormais que la liberté individuelle coïncide uniquement avec celle du droit à la sûreté, « celui-ci devant être entendu comme le droit de ne pas être arbitrairement détenu » (décision n° 2005-532 du 19 janvier 2006, Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers (Cons. 16).

Les techniques de renseignement, ne constituant pas des mesures privatives de liberté, y compris lorsqu'elles impliquent une intrusion dans un lieu privé, n'entrent donc pas dans le champ d'application de l'article 66 de la Constitution, de sorte que l'autorité judiciaire n'a pas compétence exclusive pour autoriser ou contrôler ces mesures de police.

De fait, si lorsqu'il s'agit de mesures de police judiciaire, celles-ci doivent être autorisées et mises en œuvre sous le contrôle de l'autorité judiciaire, tel n'est pas le cas des mesures prises dans le cadre de la police administrative, qui n'ont pas à être autorisées par le juge judiciaire, ainsi que l'a confirmé le Conseil constitutionnel dans sa décision *n° 2013-357 QPC du 29 novembre 2013, Société Wesgate Charles Ltd* [Visite des navires par les agents des douanes.

1.2.1.3 Les mesures envisagées doivent être conciliées avec d'autres droits et libertés garantis par la Constitution

De manière constante, le Conseil constitutionnel considère qu'il appartient au législateur d'assurer la conciliation entre, d'une part, la sauvegarde de l'ordre public, la recherche des auteurs d'infractions et la prévention du renouvellement des infractions ou encore la préservation des intérêts fondamentaux de la Nation, toutes nécessaires à la protection de droits de valeur constitutionnelle parmi les plus fondamentaux et, d'autre part, le respect de la vie privée et des autres droits et libertés constitutionnellement protégés.

Aussi, dans l'exercice de son pouvoir, « le législateur ne saurait priver de garanties légales des exigences constitutionnelles ».

Même si le juge n'a pas à autoriser la pénétration dans le domicile, dans le cadre d'une procédure administrative, le respect des exigences constitutionnelles résultant de l'article 2 de la DDHC suppose que cette intervention soit encadrée :

- Par le législateur, en application de l'article 34 de la Constitution, la loi devant être suffisamment précise pour ne pas encourir le grief d'incompétence négative,

- Les pouvoirs et conditions d'intervention devant être encadrés de manière suffisamment précise,

- Pour permettre, *in fine*, un contrôle effectif du juge, notamment de leur caractère nécessaire et proportionné,

- Indépendamment du contrôle exercé par la juridiction saisie, le cas échéant, dans le cadre des poursuites pénales ou de décisions administratives fondées sur les données collectées (*CC, 29 novembre 2013, Société Wesgate Charles Ltd précitée 2013-357 QPC ou 21 mars 2014 n° 2014-375 QPC* visites domiciliaires sur les lieux de travail)

1.2.1.4 L'encadrement envisagé doit être proportionné à l'atteinte, laquelle peut être différente selon la mesure de surveillance mise en œuvre

L'état de la législation permettant la collecte du renseignement en matière judiciaire et l'appréciation qu'en a fait le Conseil constitutionnel apportent quelques informations importantes quant au degré de précision et de contrôle que doivent comporter les mesures mises en œuvre, étant entendu que la présence de l'autorité judiciaire induite par la nature judiciaire des opérations n'a pas nécessairement à être transposée lorsque la mise en œuvre des techniques de renseignement découle d'une procédure administrative.

La loi n° 204-2004 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité a modernisé le cadre juridique de l'enquête en matière de délinquance organisée en introduisant dans le droit français les techniques spéciales d'enquête. Cette notion recouvre l'infiltration, les sonorisations et fixations d'images et la captation des données informatiques.

L'infiltration, prévue aux articles 706-81 à 706-87 du code de procédure pénale, est la possibilité, pour les officiers de police judiciaire ou agents de police judiciaire spécialement habilités, de surveiller des auteurs d'une infraction en se faisant passer auprès d'eux comme l'un de leurs co-auteurs, complices ou receleurs. L'infiltration, prévue pour durer pendant une période de quatre mois renouvelables, est autorisée par le procureur de la République ou, après avis de ce dernier, par le juge d'instruction. Cette autorisation permet aux agents infiltrés d'acquérir, détenir, transporter ou livrer des produits ou documents tirés de la criminalité organisée ainsi qu'à utiliser ou mettre à disposition des personnes se livrant à la criminalité organisée des moyens à caractère juridique ou financier ainsi que des moyens de transport ou d'hébergement.

Les sonorisations et fixations d'images de certains lieux et véhicules, prévues aux articles 706-96 à 706-102 du code de procédure pénale, permettent de surveiller, par un dispositif technique, les auteurs potentiels des infractions dont la preuve est recherchée alors qu'ils se trouvent dans des lieux ou véhicules privés. Cette technique d'enquête est utilisable dans le seul cadre de l'information judiciaire sur autorisation du juge d'instruction (et du juge des libertés et de la détention lorsque la mise en place du dispositif technique nécessite qu'il soit procédé à une perquisition de nuit dans un local d'habitation).

La captation des données informatiques, prévue par les articles 706-102-1 à 706-102-9 du code de procédure pénale, consiste en un dispositif technique permettant, sans le consentement des intéressés, de capter en temps réel des données informatiques utilisées ou saisies sur un ordinateur mais non encore diffusées. Il s'agit d'accéder, en tous lieux, à des données informatiques, de les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données. Cette technique d'enquête est utilisable dans le seul cadre de l'information judiciaire sur autorisation du juge d'instruction (et du juge des libertés et de la détention lorsque la mise en place du dispositif technique nécessite qu'il soit procédé à une perquisition de nuit dans un local d'habitation).

Ces techniques spéciales d'enquête ne s'appliquent que pour les infractions listées à l'article 706-73 du code de procédure pénale, soit la « grande » délinquance organisée.

Pour procéder à la mise en œuvre des sonorisations, captation d'images et captation de données informatiques, le juge d'instruction doit :

- solliciter l'avis préalable du procureur de la République ;
- rendre une ordonnance motivée qui devra expressément indiquer :
  - les éléments permettant d'identifier les véhicules ou les lieux privés ou publics visés ou la localisation exacte ou la description détaillée des systèmes de traitement automatisés de données ;
  - l'infraction motivant cette mise en place (autrement dit, l'une de celles visées à l'article 706-73, à peine de nullité) ;
  - la durée de la mesure (art. 706-98) ;
- délivrer une commission rogatoire spécifique.

L'obligation prévue de mentionner les éléments permettant d'identifier les véhicules ou les lieux privés ou publics visés par la mesure ou la description détaillée des systèmes de traitement automatisés de données est une garantie fondamentale de ce dispositif.

Les opérations relatives à la mise en œuvre de ces techniques obéissent à un certain formalisme.

Un procès-verbal des opérations prévues

Ce procès-verbal est établi par le juge d'instruction ou par l'officier de police judiciaire. Il doit indiquer chacune des opérations de mise en place. Il doit également indiquer les opérations de captation, de fixation et d'enregistrement sonore ou audiovisuel. Il doit enfin mentionner la date et l'heure auxquelles l'opération a commencé et celles auxquelles elle s'est terminée. Les enregistrements sont placés sous scellés fermés, ce qui implique un procès-verbal de saisie et de placement sous scellés.

Un procès verbal de transcription ou de description des opérations réalisées

En ce qui concerne les conversations, le texte vise une condition de fond classique de la retranscription à savoir que seul doit être retranscrit ce qui est « utile à la manifestation de la vérité ». S'il s'agit de captation d'image**,** la seule obligation est de procéder à la description de la scène enregistrée « utile à la manifestation de la vérité ». Les faits nouveaux devront être signalés par l'officier de police judiciaire au juge mandant par un procès-verbal spécifique de signalement, puis communiqués selon les dispositions du 3ème alinéa de l'article 80 au Parquet, lequel appréciera la suite à y donner. .

Les enregistrements sonores ou audiovisuels sont détruits, à la diligence du procureur de la République ou du procureur général, à l'expiration du délai de prescription de l'action publique. Il est dressé procès-verbal de l'opération de destruction.

A la suite de l'arrêt de la Cour européenne des droits de l'homme dans l'affaire Uzun et des arrêts de la Cour de cassation en date du 22 octobre 2013, la loi n°2014-372 du 28 mars 2014 relative à la géolocalisation a fourni un cadre juridique légal à la géolocalisation judiciaire en temps réel.

Les mesures de géolocalisation en temps réel peuvent être ordonnées dans un cadre plus large que celui réservé aux techniques spéciales d'enquête puisque la géolocalisation en temps réel est possible dans le cadre d'une enquête flagrante ou préliminaire, ainsi que dans le cadre d'une information judiciaire lorsque la procédure est relative à l'une des infractions suivantes :

- infraction punie d'au moins cinq ans d'emprisonnement ;
- délit prévu au livre II du code pénal et puni d'au moins trois ans d'emprisonnement ;
- délits d'évasion et de recel de criminel prévus aux articles 434-6 et 434-27 du code pénal (CPP).

Par ailleurs, il est également possible de recourir à la géolocalisation en temps réel dans les cadres procéduraux suivants :

- enquête ou information judiciaire en recherche des causes de la mort et des blessures (art. 74 et 80-4 du CPP) ;
- enquête ou information judiciaire en recherche des causes de la disparition (art. 74-1 et 80-4 du CPP) ;
- enquête en recherche d'une personne en fuite (art. 74-2 CPP).

L'article 230-32 du code de procédure pénale dispose qu'il peut être recouru à la géolocalisation *« d'une personne, à l'insu de celle-ci, d'un bien ou de tout autre objet* », dès lors que cette opération est *« exigée par les nécessités »* de la procédure.

Les objets susceptibles d'être géolocalisés n'étant pas limitativement énumérés, tout objet peut être géolocalisé soit par l'exploitation de sa technologie propre (téléphone portable, tablette, véhicule équipé d'un système GPS) soit par le biais de la pose d'une balise (moyen de transport, conteneur).

Par ailleurs, et à l'instar de ce qui existe en matière d'interceptions téléphoniques dans le domaine judiciaire, les mesures de géolocalisation ne sont pas limitées aux personnes soupçonnées d'avoir commis une infraction, mais peuvent être diligentées à l'encontre de tout individu (environnement familial ou amical du suspect notamment) dès lors que les nécessités de l'enquête l'exigent.

Concrètement, l'autorisation de géolocalisation prend la forme d'une décision écrite du procureur de la République et du juge des libertés et de la détention ou d'une commission rogatoire spéciale du magistrat instructeur. Cette autorisation doit faire état de tout élément permettant l'identification de l'objet géolocalisé. Les informations suivantes peuvent, par exemple, être mentionnées :

- le numéro d'immatriculation ou le modèle du véhicule lorsqu'un dispositif de géolocalisation est installé sur un moyen de transport ;
- le numéro de téléphone ou toute autre information (numéro IMSI[8] ou IMEI[9]) lorsqu'un terminal de télécommunication est géolocalisé.

Lorsque la mesure de géolocalisation requiert l'utilisation d'une balise, l'installation ou le retrait de ce dispositif peut nécessiter de s'introduire dans un espace privé, sans le consentement et en l'absence de l'occupant des lieux.

En cas d'urgence, l'officier de police judiciaire peut mettre en place ou prescrire d'initiative et sans autorisation préalable du procureur de la République ou du juge d'instruction une mesure de géolocalisation. Dans un tel cas de figure, le contrôle de l'autorité judiciaire s'exerce *a*

[8] International Mobile Subscriber Identity
[9] International Mobile Equipment Identity

posteriori. L'officier de police judiciaire doit informer immédiatement le procureur de la République ou le juge d'instruction de la mise en place de cette mesure, et le cas échéant de l'introduction dans un lieu privé. Cette information peut se faire par tout moyen (appel téléphonique, fax, courriel) et mention en est faite en procédure. Le procureur de la République ou le juge d'instruction peut alors immédiatement ordonner, sans formalisme particulier, l'interruption des opérations de géolocalisation. La validité de l'opération de géolocalisation décidée d'initiative en cas d'urgence par l'officier de police judiciaire est conditionnée par la prise d'une décision écrite en ce sens par l'autorité judiciaire compétente dans un délai de 24 heures. A défaut, les opérations de géolocalisation déjà réalisées doivent être considérées comme inexistantes et ne peuvent faire l'objet de retranscription et d'utilisation dans le cadre de la procédure.

Dans deux décisions (2014-693 DC, 25 mars 2014, cons. 13 à 15 et 17 sur la géolocalisation judiciaire ou 2004-492 DC, 2 mars 2004, cons. 62 à 66 pour mise en place de dispositifs techniques ayant pour objet, sans le consentement des intéressés, la captation, la fixation, la transmission et l'enregistrement de paroles ou d'images), le Conseil constitutionnel a donné des indications quant au contrôle du juge constitutionnel qui semble distinguer :

- Les mécanismes de surveillance n'impliquant pas d'acte de contrainte sur la personne visée ni d'atteinte à son intégrité corporelle, de saisie, d'interception de correspondance ou d'enregistrement d'image ou de son. L'atteinte à la vie privée qui en résulte consiste dans la surveillance par localisation continue et en temps réel d'une personne, le suivi de ses déplacements dans tous lieux publics ou privés ainsi que dans l'enregistrement et le traitement des données ainsi obtenues.

- Les mécanismes plus intrusifs impliquant la mise en place de dispositifs techniques ayant pour objet, sans le consentement des intéressés, la captation, la fixation, la transmission et l'enregistrement de paroles ou d'images, lesquels doivent être plus encadrés.

Par ailleurs, à l'aune de ces décisions, il semble résulter un ensemble minimal de pré requis tenant aux garanties procédurales que le législateur doit apporter pour concilier la sauvegarde de l'ordre public et le respect de la vie privée (que la technique résulte d'une procédure administrative ou judiciaire) :

- autorisation encadrée
- finalités limitées et caractère nécessaire et proportionné
- durée limitée
- relevé de la mise en œuvre des techniques de renseignement
- contrôle de l'autorité qui les a ordonnées
- contrôle *a posteriori*

1.2.1.5 L'encadrement doit être clair et précis afin d'être conforme au principe de légalité des délits et des peines

L'encadrement par la loi des techniques de renseignement ne permettra d'écarter le risque pénal des agents des services spécialisés de renseignement qu'à la condition de se conformer au principe de légalité des délits et des peines en étant le plus clair et précis possible.

Le Conseil d'Etat a eu plusieurs fois l'occasion de rappeler cette exigence. Par exemple, dans un avis rendu par l'Assemblée générale le 7 février 2013 et portant sur 5 propositions de loi

relatives à la fin de vie : *« Il n'existe aucun principe juridique qui s'oppose à ce que le législateur prévoie un dispositif civil, inscrit uniquement dans le code de la santé publique, et qui autorise certains actes auparavant sanctionnés par la loi pénale. Toutefois, pour qu'une telle cause objective d'irresponsabilité puisse constituer un fait justificatif recevable au regard de la loi pénale, il doit en emprunter les canons et obéir au premier de ces principes généraux constitutionnellement reconnus que constitue le principe de légalité des délits et des peines ».* Dans le même esprit, un avis rendu par la section sociale le 8 octobre 2013 et portant sur le projet de décret relatif aux expérimentations locales en matière de réduction des risques en direction des usagers de drogues indique qu'il « *appartient au Gouvernement, s'il veut mettre en œuvre ce projet, de proposer au Parlement le vote d'un dispositif législatif instituant, à titre expérimental, une dérogation limitée à la loi pénale, à condition que l'objet et les conditions de l'expérimentation soient définis de façon suffisamment précise et que le texte ne méconnaisse pas les autres exigences constitutionnelles et plus particulièrement, en l'espèce, le principe de légalité des délits et des peines qui s'applique tant aux textes instituant des incriminations qu'aux textes qui y dérogent* ».

Pour éviter l'arbitraire du juge quant à la mise en œuvre d'une exonération pénale, il importe que la loi soit suffisamment précise quant à la nature des techniques de renseignement autorisées, quant à la finalité poursuivie par ces techniques et quant aux conditions de leur mise en œuvre. Cette exigence de précision et de clarté permettra en outre de mieux cerner le champ de l'exonération de responsabilité pénale posée par le deuxième alinéa de l'article 122-4 du code pénal : « *n'est pas pénalement responsable la personne qui accomplit un acte commandé par l'autorité légitime, sauf si cet acte est manifestement illégal* ». En effet, plus la loi sera précise plus il sera aisé de distinguer ce qui est illégal de ce qui est manifestement illégal. Le caractère manifestement illégal de l'acte suppose la démonstration d'un abus d'autorité. Ce n'est donc pas l'illégalité de l'acte qui est sanctionnée mais l'usage du droit donné par la loi exercé à des fins manifestement étrangères aux objectifs assignés par la loi à ce droit.

Ainsi, quand bien même l'acte autorisant l'introduction dans le domicile ou autorisant l'interception des correspondances serait illégal parce disproportionné ou non nécessaire, la responsabilité pénale des agents des services spécialisés de renseignement ne pourrait être reconnue dès lors qu'une telle mesure est prévue par la loi.

En revanche, l'interception de correspondances à des fins privées ou pour des finalités manifestement non prévues par la loi serait manifestement illégale et la responsabilité des agents des services spécialisés de renseignement pourrait être reconnue.

1.2.2. Cadre conventionnel

Selon une jurisprudence constante de la Cour européenne des droits de l'homme, les écoutes téléphoniques, comme d'autres méthodes de surveillance secrète[10], constituent une ingérence dans le droit des personnes concernées au respect de leur vie privée, tel que protégé par l'article 8 de la CESDH.

> Article 8 : Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

[10] Comme les procédés de "*sonorisation*" (CEDH, 31 août 2005, Vetter c. France)

Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

Pour être compatibles avec la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, ces mesures doivent être prévues par la loi et nécessaires dans une société démocratique à la poursuite d'un but reconnu légitime.

1.2.2.1. Comme la Cour le rappelle régulièrement, les mots "prévue par la loi", au sens de l'article 8 § 2 signifient d'une part, que la mesure incriminée a une base en droit interne, mais également que la loi en cause est accessible à la personne concernée, prévisible pour la personne intéressée qui doit pouvoir en prévoir les conséquences pour elle, et sa compatibilité avec la prééminence du droit par exemple, 29 juin 2006, *Weber et Saravia c. Allemagne*, point 84).

L'accessibilité de la loi suppose, en premier lieu, que la loi soit publique et facile d'accès. Cette condition fait l'objet d'un examen attentif lorsque la portée d'une loi a été précisée par la jurisprudence ou lorsque l'application de la loi a été précisée par des normes administratives (*Kennedy c. Royaume-Uni du 18 mai 2010 :* pour considérer que la loi est accessible la Cour tient compte de l'élaboration d'un code de déontologie des services de renseignement, document public, qui peut être consulté sur Internet et que les services doivent respecter dans la mise en œuvre des mesures d'interception des communications).

La prévisibilité de la loi n'implique pas *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. Néanmoins, 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* (*Malone c. Royaume-Uni* du *2 août 1984)*

Le principe de prééminence du droit impose enfin que la loi définisse l'étendue et les modalités d'exercice des mesures de surveillance avec une précision et un encadrement suffisants. Puisque l'application de mesures de surveillance secrète des communications échappe au contrôle des intéressés comme du public, la loi irait à l'encontre de la prééminence du droit si le pouvoir d'appréciation accordé à l'exécutif ou à un juge ne connaissait pas de limites. En conséquence, la loi doit définir l'étendue et les modalités d'exercice d'un tel pouvoir avec une netteté suffisante pour fournir à l'individu une protection adéquate contre l'arbitraire pour fournir à l'individu une protection adéquate contre l'arbitraire (*Kruslin c/ France 1990 ; Kopp c. Suisse*, 25 mars 1998, § 72 ; *Valenzuela Contreras c. Espagne*, 30 juillet 1998, § 46*).*

Selon une jurisprudence constante illustrée notamment par les arrêts *Klass c. Allemagne* (1978) ou Liberty c/ Royaume Uni (2008), la mesure ne peut être regardée comme "*prévue par la loi*" que si la loi comporte les garanties minimales suivantes :

- les finalités poursuivies,
- la définition des catégories de personnes susceptibles de faire l'objet de mesures de surveillance,
- la fixation d'une limite à la durée d'exécution de la mesure,
- la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies,
- les précautions à prendre pour la communication des données à d'autres parties,
- les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des enregistrements.

Lorsque ces garanties ne sont pas définies par les textes, la Cour juge que l'ingérence n'est pas prévue par la loi.

Ainsi, avant la loi du 10 juillet 1991, le droit français ne comportait pas l'énoncé de ces garanties et la Cour avait jugé qu'aucun texte « *ne définit les catégories de personnes susceptibles d'être mises sous écoute judiciaire, ni la nature des infractions pouvant y donner lieu; rien n'astreint le juge à fixer une limite à la durée de l'exécution de la mesure; rien non plus ne précise les conditions d'établissement des procès-verbaux de synthèse consignant les conversations interceptées, ni les précautions à prendre pour communiquer intacts et complets les enregistrements réalisés, aux fins de contrôle éventuel par le juge - qui ne peut guère se rendre sur place pour vérifier le nombre et la longueur des bandes magnétiques originales - et par la défense, ni les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction desdites bandes, notamment après non-lieu ou relaxe. Les renseignements donnés par le Gouvernement sur ces différents points révèlent au mieux l'existence d'une pratique, dépourvue de force contraignante en l'absence de texte ou de jurisprudence* ». Elle en conclut que : « *le droit français, écrit et non écrit, n'indique pas avec assez de clarté l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités dans le domaine considéré. Il en allait encore davantage ainsi à l'époque des faits de la cause, de sorte que M. et Mme Huvig n'ont pas joui du degré minimal de protection voulu par la prééminence du droit dans une société démocratique* » (*Kruslin c/ France 1990*)

De même, s'agissant du système de surveillance des communications internationales anglais, la Cour a estimé que *« faute d'avoir défini avec la clarté requise l'étendue et les modalités d'exercice du pouvoir d'appréciation considérable conféré à l'Etat en matière d'interception et d'analyse des communications à destination ou en provenance de l'étranger, la loi en vigueur à l'époque pertinente n'offrait pas une protection suffisante contre les abus de pouvoir. En particulier, au rebours de ce qu'exige la jurisprudence de la Cour, aucune précision sur la procédure applicable à l'examen, la diffusion, la conservation et la destruction des données interceptées n'y figurait sous une forme accessible au public. Il s'ensuit que l'ingérence dans les droits des requérantes tels que garantis par l'article 8 n'était pas « prévue par la loi » (Liberty et autres c. Royaume Uni 2008* § 63*).*

En revanche, s'agissant du système de surveillance des communications internes anglais, la Cour a estimé que *la législation du Royaume-Uni en matière d'interception de communications internes, combinée avec les précisions apportées par la publication du code de déontologie, décrit avec une clarté suffisante les procédures applicables à la délivrance et au fonctionnement des mandats d'interception ainsi que le traitement, la divulgation et la destruction des informations interceptées. Elle observe en outre qu'aucune lacune importante dans l'application et le fonctionnement du régime de surveillance n'a été établie et estime donc que l'ingérence est prévue par la loi (Kennedy c. Royaume Uni 2010)*

De même, s'agissant du système de surveillance allemand, la Cour juge que *« les dispositions litigieuses de la loi G 10, envisagées dans leur contexte législatif, renferment les garanties minimales contre une ingérence arbitraire, telles que définies dans la jurisprudence de la Cour, et donnent donc aux citoyens une indication adéquate sur les circonstances et les conditions dans lesquelles les autorités publiques étaient autorisées à recourir à des mesures de surveillance, ainsi que sur l'étendue et les modalités d'exercice par les autorités de leur pouvoir discrétionnaire* (*Weber et Saravia c. Allemagne 2006)*

1.2.2.2 L'ingérence doit être nécessaire dans une société démocratique à la poursuite d'un but légitime

En matière de renseignement, la Cour tient compte de deux faits importants:

- les progrès techniques réalisés en matière d'espionnage et parallèlement de surveillance ;

- le développement du terrorisme en Europe au cours des dernières années. Les sociétés démocratiques se trouvent menacées de nos jours par des formes très complexes d'espionnage et par le terrorisme, de sorte que l'État doit être capable, pour combattre efficacement ces menaces, de surveiller *en secret* les éléments subversifs opérant sur son territoire.

La Cour admet donc que l'existence de dispositions législatives accordant des pouvoirs de surveillance secrète de la correspondance, des envois postaux et des télécommunications est, devant une situation exceptionnelle, nécessaire dans une société démocratique à la sécurité nationale et/ou à la défense de l'ordre et à la prévention des infractions pénales *(Klass et autres c/ Allemagne).* Ainsi, la Cour rappelle invariablement que, lorsqu'elle doit mettre en balance l'intérêt de l'Etat à protéger la sécurité nationale au moyen de mesures de surveillance secrète et la gravité de l'ingérence dans l'exercice par un requérant de son droit au respect de sa vie privée, les autorités nationales disposent d'une ample marge d'appréciation pour choisir les moyens de sauvegarder la sécurité nationale (voir, notamment, *Klass et autres*, précité, § 49, *Leander*, précité, § 59, et *Malone*, précité, § 81).

Néanmoins, les autorités doivent mettre en œuvre des garanties adéquates et suffisantes contre les abus car un système de surveillance secrète destiné à protéger la sécurité nationale crée un risque de saper, voire de détruire, la démocratie au motif de la défendre (*Klass et autres*, précité, §§ 49-50, *Leander*, précité, § 60, *Camenzind c. Suisse*, 16 décembre 1997, § 45, *Recueil* 1997-VIII, et *Lambert*, précité, § 31).

Cette appréciation dépend de toutes les circonstances de la cause, par exemple la nature, l'étendue et la durée des mesures éventuelles, les raisons requises pour les ordonner, les autorités compétentes pour les permettre, les exécuter et les contrôler, et le type de recours fourni par le droit interne (*Klass et autres*, précité, § 50).

S'agissant plus précisément du contrôle (de la nécessité et de la proportionnalité de l'ingérence), la Cour admet que la surveillance peut subir un contrôle à trois stades: lorsqu'on l'ordonne, pendant qu'on la mène ou après qu'elle a cessé.

S'agissant des deux premières phases, la nature et la logique mêmes de la surveillance secrète commandent d'exercer à l'insu de l'intéressé non seulement la surveillance comme telle, mais aussi le contrôle qui l'accompagne (*Klass et autres c/ Allemagne*).

Toutefois, puisque l'intéressé sera le plus souvent empêché d'introduire un recours effectif ou de prendre une part directe à un contrôle quelconque, il se révèle indispensable que les procédures existantes procurent en soi des garanties appropriées et équivalentes, sauvegardant les droits de l'individu et que l'ingérence de l'exécutif dans les droits d'un individu soit soumise à un contrôle efficace.

Si elle reconnaît que le contrôle juridictionnel offre, en principe, les meilleures garanties d'indépendance, d'impartialité et de procédure régulière, elle admet la possibilité qu'un tel contrôle soit exercé par une autorité administrative indépendante au regard de l'effectivité du contrôle dont elle dispose (autorisation, contrôle tout au long de l'exécution de la mesure, possibilité d'être saisi par tout individu se croyant surveillé) ce contrôle étant alors apte à limiter à ce qui était « nécessaire dans une société démocratique », l'ingérence résultant de la législation incriminée (*Klass et autres précité, §§ 53-60*).

En sens inverse, la Cour a considéré que l'ingérence, quoique prévue par la loi, avait outrepassé ce qui est nécessaire dans une société démocratique en raison de l'impossibilité dans laquelle s'était trouvé le requérant de contester la régularité des écoutes pratiquées sur la ligne d'un tiers (*Lambert c. France du 24 août 1998).* De même, dans une autre affaire, elle précise que le fait que les écoutes litigieuses aient été ordonnées par un magistrat et réalisées sous son contrôle ne suffit pas à justifier l'absence de voie de recours ouverte au bénéfice du requérant (*Matheron c. France du 29 mars 2005)*.

De même, la CEDH a considéré que la seule possibilité d'un pourvoi en cassation et l'absence d'un recours au fond contre une autorisation de perquisition délivrée par un juge ne permet pas un examen des éléments de fait fondant la décision litigieuse d'autant que la décision litigieuse, même si elle est délivrée par un juge, n'a pas permis à la personne de se faire entendre puisqu'il ignorait l'existence d'une procédure intentée à son encontre dans un arrêt *(Ravon et autres c. France du 21 février 2008).*

1.2.2.3 Le droit au procès équitable peut être concilié avec les exigences de protection de la sécurité nationale

Article 6-1 Toute personne a droit à ce que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable, par un tribunal indépendant et impartial, établi par la loi, qui décidera, soit des contestations sur ses droits et obligations de caractère civil, soit du bien-fondé de toute accusation en matière pénale dirigée contre elle. Le jugement doit être rendu publiquement, mais l'accès de la salle d'audience peut être interdit à la presse et au public pendant la totalité ou une partie du procès dans l'intérêt de la moralité, de l'ordre public ou de la sécurité nationale dans une société démocratique, lorsque les intérêts des mineurs ou la protection de la vie privée des parties au procès l'exigent, ou dans la mesure jugée strictement nécessaire par le tribunal, lorsque dans des circonstances spéciales la publicité serait de nature à porter atteinte aux intérêts de la justice.

La Cour rappelle que le principe de l'égalité des armes – l'un des éléments de la notion plus large de procès équitable – exige que chacune des parties se voie offrir une possibilité

raisonnable de présenter sa cause dans des conditions qui ne la placent pas dans une situation défavorable par rapport à son adversaire (voir, par exemple, *Jespers c. Belgique*, n° 8403/78, décision de la Commission du 15 octobre 1980, Décisions et rapports (DR) 27, p. 61 ; *Foucher c. France*, 18 mars 1997, § 34, *Recueil* 1997-II ; et *Bulut c. Autriche*, 22 février 1996, § 47, *Recueil* 1996-II).

Toutefois, la Cour a jugé que, même dans les instances impliquant une décision sur une accusation en matière pénale relevant de l'article 6, 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, la nécessité de garder secrètes certaines méthodes policières de recherche des infractions ou la protection des droits fondamentaux d'autrui. En ce qui concerne les dispositions limitant la communication des informations interceptées, la Cour rappelle que le droit à la divulgation des preuves pertinentes n'est pas absolu. Les intérêts de la sécurité nationale ou la nécessité de garder secrètes certaines méthodes d'enquête en matière pénale doivent être mis en balance avec le droit général à une procédure contradictoire (voir, *mutatis mutandis*, *Edwards et Lewis c. Royaume-Uni* [GC], n^{os} 39647/98 et 40461/98, § 46, CEDH 2004-X).

De même, l'obligation de tenir des audiences n'est pas absolue. Il existe des affaires dans lesquelles il n'est pas nécessaire de tenir audience et que les tribunaux peuvent trancher équitablement et raisonnablement sur la base des observations des parties et d'autres écrits. Les circonstances pouvant justifier que l'on se dispense d'une audience découlent essentiellement de la nature des questions dont la juridiction interne compétente est saisie (voir *Jussila c. Finlande* [GC], n° 73053/01, §§ 41-42, CEDH 2006-XIII).

Enfin, la sécurité nationale peut justifier l'exclusion du public d'une procédure, l'étendue de l'obligation de motivation peut varier selon la nature de la décision et se détermine à la lumière des circonstances de la cause, l'organe de contrôle pouvant à bon droit se borner à informer le requérant qu'aucune décision n'a été rendue, selon un mécanisme de non confirmation, non infirmation (voir *Ruiz Torija c. Espagne*, 9 décembre 1994, § 29, série A n° 303-A).

Toutefois, si l'on veut garantir un procès équitable à l'accusé, toutes difficultés causées à la défense par une limitation de ses droits doivent être suffisamment compensées par la procédure suivie devant les autorités judiciaires (voir, par exemple, *Doorson c. Pays-Bas*, 26 mars 1996, § 70, *Recueil* 1996-II ; *Jasper c. Royaume-Uni* [GC], n° 27052/95, §§ 51-53, 16 février 2000 ; et *A. et autres c. Royaume-Uni* [GC], n° 3455/05, § 205, 19 février 2009).

Ainsi, lorsque la procédure juridictionnelle porte sur des mesures de surveillance secrète, si la Cour admet qu'il est nécessaire de dissimuler des informations sensibles et confidentielles, et que, par voie de conséquence, les restrictions apportées à la procédure sont justifiées, elle regarde toutefois si considérées globalement, les restrictions en question étaient disproportionnées ou attentatoires au droit du requérant à un procès équitable. Ainsi, dans le système anglais des interceptions nationales (*Kennedy c. RU 2010*), elle constate que les garanties suivantes sont de nature à offrir un contrepoids suffisant :

- La saisine très large par toute personne *soupçonnant* la mise en œuvre d'une technique de renseignement (absence d'obstacle probatoire à surmonter)
- Le caractère indépendant et impartial de l'organe de contrôle
- Le fait qu'il dispose d'un droit de communication total

- le caractère absolu ou non de l'absence de contradictoire ou la possibilité d'y déroger
- Le fait que les informations produites à la juridiction de contrôle sont susceptibles de contenir des éléments extrêmement sensibles, surtout du point de vue de la politique gouvernementale de « non-confirmation et de non-dénégation ».
- Le fait que la décision de tenir audience relève du pouvoir discrétionnaire du juge, rien ne l'empêchant de tenir audience chaque fois qu'il considère que pareille mesure est utile à l'examen de l'affaire.
- Le fait que lorsque le juge donne gain de cause à un plaignant, il lui est loisible de divulguer les documents et les informations pertinents en application de l'article 6.4 de son règlement (paragraphe 84 à 87).
- Les pouvoirs effectifs de l'organe de contrôle : possibilité d'annuler un mandat d'interception, d'ordonner la destruction des informations interceptées, d'octroyer une indemnité.

Compte tenu de la nécessité de garantir l'efficacité du dispositif de surveillance secrète et de son importance pour la lutte contre le terrorisme et les infractions graves, la Cour considère que les restrictions apportées aux droits du requérant dans le cadre de la procédure suivie dans le système anglais étaient à la fois nécessaires et proportionnées et qu'elles n'ont pas porté atteinte à la substance même des droits de l'intéressé au titre de l'article 6-1.

Au total, pour la Cour européenne des droits de l'homme :

- si les ingérences dans la vie privée que constituent les mesures de surveillance sont justifiées par les finalités de préservation de la sécurité nationale et de protection des intérêts fondamentaux de l'Etat,

- elles doivent être strictement définies de manière à être accessibles, prévisibles et permettre un contrôle effectif par un organe impartial et indépendant, nonobstant les aménagements de procédure rendus nécessaires par la matière.

1.3. Etat de la législation relative au renseignement au sein des pays membres de l'Union européenne

1.3.1 Le modèle britannique

Initiée notamment en réaction aux condamnations de la CEDH, l'instauration d'un cadre juridique pour les services de renseignement britanniques trouve ses origines en 1989 avec le British Security Service Act. Par la suite, le législateur britannique a entendu donner une légitimité très forte aux services de renseignement en prévoyant leur existence et en définissant leur mission par la loi.

1.3.1.1 Présentations des différents services de renseignement britannique organisés autour d'organes gouvernementaux de coordination

1.3.1.1.1 Les principaux organes gouvernementaux de coordination

Le Committee on intelligence services (CIS): Ce comité est composé du Premier ministre, des ministres des affaires étrangères, de l'intérieur, de la défense et des finances. Leur mission est de définir les grandes lignes de la politique en matière de renseignement.

Comité interministériel du renseignement : Équivalent du Secrétariat général de la défense et de la sécurité nationale français, ce comité est rattaché au Cabinet office (bureau du conseil des ministres) chargé d'aider le premier ministre et le gouvernement britannique. Ce comité établit les plans de renseignement, coordonne les activités des services et centralise pour le gouvernement les rapports sur l'activité des services.

Le Joint intelligence committee JIC (en français : Comité conjoint du renseignement) dépend du cabinet office. Il établit quotidiennement pour le Premier ministre du Royaume-Uni une synthèse des informations des services de renseignement britannique (MI-5, MI-6, GCHQ) : il fixe et contrôle leurs objectifs. Le JIC coordonne chaque semaine une réunion interdépartementale en deux parties : la première réunit correspondants des ministères des Affaires étrangères et de la Défense, directeurs des services de renseignements, représentants de leurs homologues australien, canadien et néo-zélandais et des États-Unis dans le cadre de l'UKUSA (=United Kingdom-United States communications intelligence Agreement, traité signé secrètement le 5 mars 1946 entre le Royaume-Uni et les Etats-Unis, rejoints par la Canada, l'Australie et la Nouvelle-Zélande). . La seconde est uniquement britannique et dédiée aux sujets nationaux. Le président du JIC dirige le joint intelligence organisation (JIO) composé d'analystes du renseignement qui effectue, en coordination avec les trois services de renseignement, l'analyse des renseignements bruts fournis par ces derniers.

1.3.1.1.2 Pluralité des services de renseignement

Le British Security Service (« military intelligence » section 5 communément appelé MI-5) : Le British Security Service Act définit des bases statutaires du MI-5, service à compétence intérieure sous l'autorité du Ministère de l'intérieur, équivalent de la DGSI. Le MI5 enquête sur les menaces en matière de sécurité intérieure et collecte le renseignement en matière de contre-terrorisme, de contre-espionnage, de protection du patrimoine. Il conseille le gouvernement sur les menaces et aide les autres organisations pour répondre aux menaces et est en charge de démasquer les menaces sur le territoire national. Enfin, le MI5 doit concourir à la sauvegarde du « bien-être économique » du pays.

Le Secret intelligence service –SIS- (ex « military intelligence » section 6 communément appelé MI-6) : L'intelligence service act de 1994 a défini les compétences du SIS, service de renseignement compétent à l'étranger, comparable à la DGSE, mais sous l'autorité du Ministère des affaires étrangères. Le SIS recueille pour le Gouvernement britannique des renseignements secrets et mène des opérations secrètes outre-mer. L' « Intelligence Services Act 1994 » établit le périmètre de ces activités et ordonne au SIS de collecter le renseignement et d'exécuter d'autres tâches relatives aux activités et intentions de certains individus à l'étranger. La collecte de renseignements par le SIS s'accorde aux exigences et priorités établies par le « Joint Intelligence Committee » (Commission Mixte au Renseignement) et approuvées par le Gouvernement britannique. Afin de répondre à ces obligations, le SIS se sert de sources humaines et techniques et collabore étroitement avec un grand nombre de services de renseignement et de sécurité étrangers. En outre, le SIS coopère étroitement avec les autres services de renseignement et de sécurité britanniques : le Service de Sécurité et le GCHQ, les Forces Armées, le Ministère de la Défense, le Foreign and Commonwealth Office (le ministère des affaires étrangères), le Home Office (ministère de l'intérieur), la HM Revenue and Customs (direction générale des impôts et de la douane) et

d'autres ministères britanniques et organisations chargés de l'application de la loi. Le SIS a pour but de protéger le pays de toute attaque terroriste extérieure au pays et de conduire des activités d'espionnage à l'extérieur du Royaume-Uni, contrairement au MI5 chargé de la sécurité à l'intérieur des frontières.

Le Governement communication headquarters (GCHQ) : Le GCHQ littéralement « Quartier général des communications du gouvernement » est le service civil de renseignement technique placé sous la responsabilité du secrétaire d'Etat britannique aux affaires étrangères et du Commonwealth. La mission du GCHQ consiste dans la collecte du renseignement technique. Son rôle est de fournir au gouvernement et aux forces armées britanniques des informations collectées grâce aux techniques de renseignement d'origine électromagnétique**.** Le GCHQ constitue le plus grand service d'interception des communications occidental après la NSA américaine, avec laquelle il entretient des relations étroites. L'*Investigatory Powers tribunal* a d'ailleurs admis, par un jugement du 6 février 2015, la conformité au regard de la Convention européenne des droits de l'homme, du nouveau régime encadrant le partage d'informations entre la NSA et le GCHQ.

Il dispose de personnels formant un groupe intitulé Joint internet age capabilities (JIAC) dont la mission est d'améliorer la proximité entre les techniciens et les opérationnels, d'automatiser les procédures avec les services opérationnels et de trouver de nouvelles méthodes permettant de tirer un profit optimal des technologies émergentes. Enfin, ce groupe travaille à la mise en place d'un réseau commun au sein de la communauté du renseignement pour améliorer le partage de données entre service (projet « Secret intelligence network »).

Le MI5 collabore étroitement avec le GCHQ dont les missions ont été définies par l'Intelligence service act. Chacune des bases de données de ces services leur est mutuellement accessible. Les nécessités d'ordre économique et opérationnel ont poussé la communauté anglaise du renseignement à passer de l'ère du « need to know » au « need to share »

1.3.1.2 Le cadre légal d'autorisation des moyens de recueil de renseignement

1.3.1.2.1 Un mécanisme d'autorisation reposant sur les ministres de tutelle : le « warrant »

Le British Security Service (MI-5) n'ayant pas de compétence judiciaire, il ne peut accomplir, à la différence de la DGSI, aucun acte judiciaire (perquisitions...). Il ne dispose donc pour l'accomplissement de sa mission que de prérogatives qui lui sont conférées sous le contrôle du ministre de l'intérieur britannique. Concernant le SIS et le GCHQ, ces autorisations relèvent pour leur part du Ministère des affaires étrangères.

En application des textes en vigueur, les services doivent donc adresser à leur ministre de tutelle une demande détaillant l'ensemble des actions qui devront être conduites pour acquérir le renseignement, afin de se voir délivrer un « warrant ». Ainsi, un même warrant pourra par exemple comprendre une autorisation pour fouiller un domicile, y poser des micros. Le travail des juristes du service demandeur consiste donc à anticiper toutes les actions que les directions opérationnelles pourraient être amenées à réaliser (*par exemple, si au cours de la fouille domiciliaire est trouvé un ordinateur, le warrant devra avoir prévu cette éventualité afin de permettre la copie des données qu'il contient*).

Le système britannique offre ainsi un cadre combinant une réelle couverture juridique aux services de renseignement tout en préservant la nécessaire souplesse à leur activité

opérationnelle. Il s'appuie sur une forte responsabilité de l'exécutif, en l'occurrence les ministres de tutelle, qui sont seuls responsable de la délivrance des autorisations d'opérations (« warrant ») aux services. La « Regulation of Investigation power act» de 2000 (dite RIPA 2000) a complété le régime juridique pour ce qui est des actions intrusives.

La législation (*Intelligence Service act 1994, British security service act* et *RIPA 2000*) ne réglemente pas en tant que tel l'usage de telle ou telle technique mais raisonne davantage par rapport à la nature de l'atteinte à la vie privée qu'elle représente (ex : accès au domicile, filature, interceptions des communications). Un warrant peut ainsi intervenir dans n'importe quel domaine de la vie privée. Cette approche a permis à la législation anglaise de s'adapter aux évolutions technologiques, sans qu'il soit nécessaire de mettre à jour les textes trop fréquemment.

Il revient au service de convaincre son ministre de tutelle du bien fondé et de la légalité de la mesure. Ainsi, le ministre doit s'assurer en particulier de la nécessité, de la proportionnalité des moyens mis en œuvre mais aussi de l'absence de moyen alternatif pour aboutir aux objectifs recherchés. Dans certains cas, comme l'accès aux données techniques de connexion ou la filature d'un individu, l'autorisation d'un « senior member » du service suffit. En dehors du territoire britannique, le ministre chargé de la politique étrangère peut délivrer un warrant qui a pour conséquence d'exonérer de sa responsabilité pénale une personne qui, dans le cadre du warrant, accomplit des actes qui s'avéreraient normalement contraires à la législation britannique. Les actes qui seront accomplis doivent être nécessaires pour l'accomplissement normal des taches de l'Intelligence Service » et « des arrangements satisfaisants » existent pour assurer que rien ne sera fait pour aller au-delà de ce qui est nécessaire à l'accomplissement normal des taches de l'Intelligence Service.

Le signataire du warrant est normalement le ministre lui-même, le pouvoir politique endossant l'entière responsabilité de l'autorisation (ou du refus d'autorisation).Le warrant est délivré pour une durée de six mois renouvelable.

1.3.1.2.2 Le contrôle de l'activité des services de renseignement prend trois formes :

1.3.1.2.2.1 Les commissionners

Afin de contrôler les autorisations délivrées, ont été institués l'*Intelligence services commissionner* et l'*Interception of communication commissionner.*

L'intelligence service commissionner, nommé par le Premier ministre parmi les personnalités occupant ou ayant occupé de hautes fonctions judiciaires pour une durée de trois ans renouvelable, contrôle « ex post » la légalité des « warrants » délivrés par chacun des ministres concernés, afin de s'assurer de leur légalité. Les contrôles sont effectués par voie de sondage et sur son initiative. Il contrôle également l'exécution des warrants par les services et se rend aux sièges des services pour examiner les dossiers en échangeant avec les membres des services. Il peut exiger tous documents et informations qu'il estime nécessaires pour l'accomplissement de sa mission. Il établit annuellement un rapport à destination du Premier ministre, que ce dernier transmet à chaque chambre du parlement et publie.

L'*Interception of communication commissionner* détient des compétences comparables en matière d'interceptions de communications.

1.3.1.2.2.2. L'investitagory power tribunal

La RIPA 2000 a institué l'*Investigatory Powers tribunal qui est* un tribunal chargé de recevoir les plaintes des citoyens à l'encontre des services de renseignement quant à l'application de cette loi. Dans ce cadre, les *commissionners* apportent leur aide au tribunal qui remet un rapport au ministre concerné. Si la plainte est reconnue fondée, le procédé incriminé est suspendu, la production détruite et le plaignant indemnisé.

Les sept membres de cette juridiction sont nommés par le Reine pour cinq ans, sur proposition du Gouvernement qui sélectionne des juristes confirmés.

1.3.1.2.2.3 Le contrôle parlementaire

Le Royaume-Uni n'a pas institué un véritable contrôle parlementaire des services de renseignement mais a créé un comité dépendant du Premier ministre et composé de parlementaires. En effet, le Premier ministre choisit librement les neuf membres de *l'Intelligence Service Commitee* au sein des deux chambres (après consultation du chef de l'opposition). Selon la loi de 1994, le comité s'intéresse au budget, à la bonne administration et à la politique des trois principaux services de renseignement. L'ISC ne dispose d'aucune compétence s'agissant du DIS (*Defense intelligence staff*, le service de renseignement militaire), ou les organes de l'exécutif traitant du renseignement (le *Joint intelligence committee*, le *National security council*...).L'*Intelligence Service Communitee* publie un rapport annuel et peut publier des rapports spéciaux. Ce fut notamment le cas en septembre 2003 concernant l'Irak ou en 2005 après les attentats de Londres. Le *justice and security act 2013* a renforcé le contrôle du Parlement sur les services de renseignement. La loi a notamment étendu les attributions de l'ISC afin qu'il puisse en certaines circonstances traiter des aspects opérationnels. L'ISC a tenu sa première audition publique en novembre 2013 durant laquelle les trois directeurs des services de renseignement ont témoigné.

A l'occasion de l'affaire Kennedy c. Royaume Uni (2010), la Cour a relevé que ce système offrait de garanties suffisantes en termes d'accessibilité et de prévisibilité (identification des personnes potentiellement concernées, durée de conservation raisonnable, divulgation sélective, destruction maîtrisée, contrôle effectif).

Par suite, elle a estimé que la législation du Royaume-Uni en matière d'interception de communications internes, combinée avec les précisions apportées par la publication du code de déontologie, décrit avec une clarté suffisante les procédures applicables à la délivrance et au fonctionnement des mandats d'interception ainsi que le traitement, la divulgation et la destruction des informations interceptées. Elle observe en outre qu'aucune lacune importante dans l'application et le fonctionnement du régime de surveillance n'a été établie et que le contrôle est effectif.

1.3.2 Le modèle italien

1.3.2.1 Les services de renseignement organisés autour de l'organe gouvernemental du département de renseignement et de sécurité

Jusqu'en 2007, l'Italie ne disposait pas de législation spécifique propre aux services de renseignement, leur conférant des pouvoirs et des instruments opérationnels. Toutefois en 2007, il est apparu nécessaire d'adapter l'arsenal législatif, d'une part pour faire face à

l'importance de la menace terroriste à laquelle étaient confrontés les services, et d'autre part pour introduire un mécanisme de transparence envers le parlement. C'est dans ce contexte qu'a été adoptée la loi du 3 août 2007 relative au « Système du renseignement pour la sécurité de l'Etat et la réforme du secret ».

1.3.2.1.1 Présentation des différents services de renseignement organisés autour d'organes de coordination gouvernementaux DIS et CISR

Le Département de renseignement pour la sécurité (DIS) :
Pour exercer leurs fonctions, le Président du conseil des Ministres et l'Autorité déléguée font appel au DIS pour s'assurer de l'uniformité dans la programmation de la recherche de renseignement du système de renseignement pour la sécurité ainsi que dans les analyses et dans les activités opérationnelles des services de renseignement pour la sécurité. Il coordonne toutes les activités de renseignement pour la sécurité en contrôlant les activités menées par l'AISE et par l'AISI et demeure constamment informé des opérations menées par les services de renseignement pour la sécurité. Le DIS transmet au Président du conseil des ministres les rapports et analyses fournis par le système du renseignement pour la sécurité. Il recueille les informations, analyses et les rapports provenant des services de renseignement pour la sécurité, les forces armées et de police, des administrations de l'Etat et des organismes de recherche même privés. Compte tenu des attributions exclusives de l'AISI et de l'AISE, il élabore des analyses stratégiques ou relatives à des cas particuliers, il formule des avis de prévisions sur la base des analyses thématiques de l'AISE et de l'AISI. Il élabore en accord avec l'AISE et l'AISI le plan d'acquisition des ressources humaines.

Le comité interministériel pour la sécurité de la république (CISR) a été créé par la loi du 3 août 2007 et placé auprès de la Présidence du Conseil des ministres avec des fonctions de consultation, de proposition, de définition et de délibération, sur les orientations et les finalités générales de la politique de renseignement pour la sécurité. Il délibère sur la répartition des ressources financières entre le DIS et les services de renseignement pour la sécurité ainsi que sur les budgets prévisionnels et définitifs. Présidé par le Président du conseil des ministres, le comité est composé de l'autorité déléguée, des ministres des affaires étrangères, de l'intérieur, de la défense, de la justice, de l'économie et des finances.

L'Agence de renseignement et de sécurité interne (AISI) est compétente pour rechercher et élaborer dans son domaine de compétence tous les renseignements utiles pour la défense de la sécurité intérieure de la République, contre toute menace, toute activité subversive et toute forme d'agression criminelle ou terroriste. Elle a la charge des activités de renseignement pour la sécurité à l'intérieur du territoire national afin de protéger les intérêts politiques, militaires, économiques et industriels de l'Italie. L'AISI a également en charge, à l'intérieur du territoire national, la recherche et la lutte contre les activités d'espionnage dirigées contre l'Italie ainsi que les activités visant à porter atteinte aux intérêts nationaux. Elle peut effectuer des opérations à l'étranger mais seulement en collaboration avec l'AISE et lorsque ces opérations sont strictement liées aux activités de l'AISI sous la supervision du DIS (cf *infra*).

L'Agence de renseignement externe (AISE) est compétente pour rechercher et élaborer tous les renseignements utiles à la défense de l'indépendance, l'intégrité et la sécurité de la république contre la menace provenant de l'extérieur. L'agence est en particulier compétente pour les activités de lutte contre la prolifération de matériels stratégiques ainsi que des activités de recherche de renseignement à l'extérieur du territoire national pour assurer la sécurité et la protection des intérêts politiques militaires économiques et scientifiques et industriels de l'Italie. Elle a également la tache de repérer et lutter à l'extérieur du territoire

national contre les activités d'espionnage dirigées contre l'Italie et les activités visant à porter atteinte aux intérêts nationaux. Elle peut effectuer des opérations sur le territoire national seulement en collaboration avec l'AISI lorsque ces opérations sont strictement liées à des affaires qu'il traite l'étranger. La loi de 2007 prévoit que l'AISE est responsable devant le Président du Conseil des ministres et informe en temps utiles et en permanence le Ministre de la défense, le Ministre des affaires étrangères et le Ministre de l'intérieur en ce qui concerne leurs domaines de compétences.

1.3.2.1.2 Le cadre légal d'autorisation des opérations spéciales

La loi de 2007 prévoit que le directeur du service demande au Président du Conseil l'autorisation de mener, contre un ou plusieurs objectifs, des opérations spéciales au cours desquelles pourront être accomplies des actions délictuelles.

La demande d'autorisation :
La demande d'autorisation est très détaillée et doit être motivée. Elle doit ainsi successivement présenter : la phase opérationnelle (l'objectif recherché sur tel ou tel domaine opérationnel), la description des opérations et les finalités opérationnelles de celles-ci, la description des objectifs suivis (personnes physiques ou morales), l'indication des conduites adoptées (intrusion, surveillances techniques...) et leur qualification pénale, la description du caractère proportionnel et indispensable de celles-ci eu égard au résultat recherché, l'indication des dommages prévisibles aux intérêts privés, du contexte territorial et de la durée prévisible de l'opération, des frais prévisibles engendrés par l'opération ainsi que la mention des services partenaires. Enfin, la demande manuscrite se termine par la formule d'autorisation de procéder aux opérations et doit être signée par le directeur du service concerné.

Le Président du Conseil, plus généralement le Ministre délégué ad hoc, examine si la ou les opérations sollicitées respectent bien les exigences de la loi de 2007. Si tel est le cas, il donne son autorisation aux opérations spéciales et par là même aux conduites délictueuses qui en découlent. La requête signée (dont la loi ne précise pas précisément comment elle doit être rédigée) est gardée par le DIS, autorité de tutelle du service, pour une période prolongée. Cette demande d'autorisation peut viser une action immédiate, brève, engendrant un délit spécifique (autorisation « spot »), mais elle peut plus généralement viser une série de conduites délictueuses planifiées.

Les autorisations d'urgence pour contraintes exceptionnelles :
Quel que soit l'objet de la demande initiale, il y a toujours la possibilité de demander verbalement au directeur du service une autorisation d'urgence pour faire face aux contraintes opérationnelles non prévues *ab initio*. Dans ce cas, le directeur du service dispose d'un délai de 24 heures pour obtenir ratification a posteriori de l'opération par le Président du Conseil. La demande d'autorisation doit par ailleurs mettre en exergue le caractère proportionné des conduites envisagées par rapport au but poursuivi et notamment l'absence d'autre alternative possible pour obtenir le résultat ou le renseignement recherché.

La mise en place de garanties fonctionnelles découlant de l'autorisation :
Une fois cette procédure formelle d'autorisation accomplie, l'opération peut se dérouler et ouvrir droit à l'application des garanties fonctionnelles prévues par la loi de 2007.

Ces garanties fonctionnelles peuvent être évoquées, en cas de survenance d'un problème au cours d'une opération, tant par l'agent du service qui fait l'objet d'une enquête que par le

directeur de l'AISI, par l'entremise du directeur du DIS. Dans ce cas, quand le service oppose la garantie fonctionnelle, l'agent du service ne peut être retenu que pour une période de 48 heures, délai permettant au ministère public d'avoir la confirmation par le Président du Conseil de l'existence d'une opération spéciale autorisée, sans toutefois avoir le contenu exact de ladite opération (cette confirmation peut même se faire oralement).

L'opposition de la garantie fonctionnelle peut avoir lieu à n'importe quelle phase du processus judiciaire, y compris lors de la phase de jugement pour des raisons d'opportunité opérationnelle. Lors du jugement, le Président du Conseil a 10 jours pour fournir la justification de la garantie fonctionnelle, et ce jusqu'au jugement définitif, c'est à dire après appel et cassation**.**

Quand le Président du Conseil oppose la garantie fonctionnelle, il doit motiver cette opposition de façon très brève (ex : justification destinée à contrecarrer une opération terroriste). Si la Loi ne prévoit pas précisément le contenu de la motivation, celle-ci doit néanmoins tenir compte du caractère nécessairement proportionnel de la conduite délictuelle adoptée au regard du but poursuivi. La garantie fonctionnelle s'applique à l'agent infiltré (agent du service ou source) mais également à tous ceux qui ont participé directement ou indirectement à l'action (notamment aux autres fonctionnaires du service ayant planifié l'opération).

Dans la majorité des cas, ce sont des sources infiltrées et non des agents du service qui bénéficient de la garantie fonctionnelle. S'agissant de la procédure d'infiltration, la Loi autorise les services de renseignement à recourir à la provocation pour les délits spécifiés par la loi qui bénéficient de la garantie fonctionnelle (ce qui n'est pas le cas en matière de police judiciaire, où la provocation n'est pas admise sauf en matière de trafic de stupéfiants).

La garantie fonctionnelle est une cause d'exclusion de culpabilité au même titre que la légitime défense, la loi prévoyant dans son article 17 que « le personnel des services de renseignement n'est pas puni s'il accomplit un acte considéré par la loi comme un délit mais qui est autorisé légitimement au cas par cas parce qu'il est jugé indispensable à l'accomplissement des missions institutionnelles de ces services ». Cette garantie fonctionnelle n'est évidemment pas sans limite, la conduite délictueuse ne pouvant être excusée dans tous les cas. Le législateur a ainsi prévu que cette garantie ne peut valablement être invoquée en cas de crimes et délits contre l'intégrité physique et morale ainsi que de délits contre l'administration de la Justice (ex: corruption de témoin, de magistrat, falsification de preuves...). En revanche, la loi admet la fourniture de faux papiers ainsi que la possibilité de soutenir une personne en fuite. De même en est-il pour les actes délictueux commis à l'intérieur du Parlement ou des Conseils régionaux, à l'encontre des syndicats ou des journalistes.

1.3.2.2 Les organes de contrôle des services de renseignement

1.3.2.2.1 La commission parlementaire pour la sécurité de la république (COPASIR)

Des pouvoirs étendus ont été accordés par la loi de 2007 à la COPASIR en contrepartie des garanties fonctionnelles accordées aux services de renseignement. Ainsi, la COPASIR a en charge le contrôle systématique et continu du respect de la Constitution et des lois par les services *de renseignement.*

La loi a doté cet organe de pouvoir de consultation pouvant aller jusqu'à la possibilité d'imposer au Président du Conseil des obligations d'informations spécifiques à son égard. Cette commission, composée de 10 membres (5 de la majorité et 5 de l'opposition), a pour fonction de « *vérifier de manière systématique et continue que les activités des services de renseignement se conforment à la Constitution et à l'application de la loi, dans l'intérêt exclusif de la défense de la République et de ses institutions* ».

Le président du COPASIR (issu de l'opposition) a en charge le contrôle du respect de la loi par les différents services de renseignement ainsi que par les autres organismes publics. Il peut également solliciter l'autorité judiciaire pour obtenir des copies d'actes ou de documents relatifs à des procédures et enquêtes en cours. La transmission peut, par décision motivée de l'autorité judiciaire, être retardée de 6 mois renouvelables pour des raisons d'instruction du dossier.

Le pouvoir de contrôle des opérations spéciales :
La COPASIR doit être informée sous 30 jours de toute opération spéciale menée par un service de renseignement ayant conduit à la commission d'une action illégale autorisée par le chef de l'Exécutif. En tout état de cause, l'information de la COPASIR ne porte que sur des opérations passées et non des opérations en cours, même si elle est informée régulièrement. De plus, le président du Conseil doit également informer la COPASIR de sa décision d'opposer le Secret Défense à une enquête judiciaire. En outre, quand la Police Judiciaire dispose d'écoutes téléphoniques dans lesquelles est identifié un membre des services de renseignement, elle en avise l'autorité judiciaire qui doit informer le Président du Conseil pour savoir s'il souhaite appliquer le secret d'État (ou secret défense). Ce dernier doit alors aviser la COPASIR de ces faits (abstraction faite de savoir s'il applique ou non le secret d'État).

Le pouvoir de contrôle budgétaire :
La COPASIR dispose également de compétences en termes d'examen du budget, d'audition des autorités politiques (Président du conseil, ministre délégué chargé du renseignement…). Elle peut également entendre des représentants des services de renseignement et est à même de faire mener des enquêtes sur les manquements de leur personnel. Elle établit un rapport annuel au parlement.

1.3.2.2.2. L'autolimitation par la Cour constitutionnelle de l'étendue de son contrôle

En principe, la COPASIR -position critiquée par de nombreux constitutionnaliste -est en droit d'exercer un contrôle de fond sur les décisions les plus sensibles reposant sur une évaluation discrétionnaire du pouvoir exécutif et de sanctionner politiquement le gouvernement.

Toutefois, la Cour a elle-même limité son contrôle à un contrôle formel, lequel ne porte pas sur les motifs ayant conduit l'autorité politique à apposer le secret d'Etat depuis sa décision en date du 11 mars 2009. Il est à relever que la Cour a procédé elle-même à la restriction de son périmètre de contrôle alors même que le secret d'Etat ne lui est pas opposable et lui permettrait d'examiner les circonstances d'espèce.

1.3.3 Le modèle belge

1.3.3.1. Principe de dualité des services de renseignement belges

1.3.3.1.1 Le service de renseignement civil : La Sûreté de l'État (SE)

La Sûreté de l'État *(*SE) est un service de renseignement civil placé à titre principal sous l'autorité du ministre de la Justice, en charge de la sécurité intérieure et extérieure de l'Etat. Il lui arrive toutefois d'agir à la demande du ministre de l'Intérieur pour le maintien de l'ordre public et la protection des personnes.

Ses missions sont essentiellement de rechercher, analyser et gérer des informations sur des activités menaçant ou susceptibles de menacer la sûreté intérieure de l'Etat ou la pérennité de l'ordre démocratique ou constitutionnel, la sécurité extérieure de l'Etat ou les relations internationales, le potentiel scientifique ou économique ou tout autre intérêt fondamental du pays. Si la SE peut également procéder à des contrôles de sécurité, il est toutefois interdit aux fonctionnaires de la Sûreté de l'État de procéder à l'arrestation d'individus.

1.3.3.1.2 Le service de renseignement militaire : Service général du renseignement et de la sécurité (SGRS)

Le SGRS est le service de renseignement militaire placé sous l'autorité du ministre de la Défense nationale. Sa mission est de rechercher, analyser et gérer des informations sur des activités menaçant ou susceptibles de menacer l'intégrité du territoire national, les plans de défense militaires, l'exécution des tâches des forces armées, la sécurité des citoyens belges, du personnel du ministère de la défense, des installations militaires, armes, plans, systèmes informatiques ou d'autres intérêts fondamentaux du pays. Il informe les ministres compétents et conseille également le gouvernement en matière de politique extérieure et de la défense. Il a en charge la protection du secret défense. Le SGRS est en outre compétent pour l'interception de communications émises à l'étranger, et ce, sous conditions et contrôle stricts.

1.3.3.1.3. Compétence commune SE/SGRS en matière de recueil de renseignement

Les services de renseignement peuvent rechercher, collecter, obtenir et traiter des informations personnelles pour autant qu'elles soient nécessaires à l'accomplissement de leurs tâches.

Ce faisant, ils peuvent avoir recours aux services des autorités de justice et à des fonctionnaires et agents du service public ainsi qu'à toute personne ou organisation du secteur privé en vue de la recherche d'informations. Ces services peuvent recourir à l'usage de méthodes ordinaires de renseignement telles que l'usage de sources ouvertes (ex. articles de presse, rapports), l'usage de sources humaines (informateurs), l'observation et l'inspection des lieux publics et des lieux privés accessibles au public sans l'aide de moyens techniques.

Si ces méthodes habituelles engagées en vue de la recherche d'informations ne suffisent pas, les deux services de renseignement peuvent utiliser des méthodes dites spécifiques ou exceptionnelles :

- <u>Méthodes spécifiques:</u>

Observation en engageant des moyens techniques dans les espaces et locaux publics ou privés accessibles au public ou observation avec ou sans moyens techniques des espaces privés non accessibles au public ; surveillance des espaces et locaux publics ou privés accessibles au public ainsi que surveillance par des moyens techniques des objets qui y sont enfermés ;

identification de l'expéditeur ou du destinataire d'un envoi postal ou du propriétaire d'une boite postale ; identification de l'abonné(e) ou de l'utilisateur usuel d'un service de communication électronique ou du moyen de communication électronique utilisé ; localisation des données d'appel de moyens de communication électroniques et de l'origine ou la destination de communications électroniques.

L'article 18/3 de la loi organique des services de renseignement et de sécurité du 30 novembre 1998, repris par l'article 14 de la loi relative aux méthodes de recueil des données par les services de renseignement et de sécurité du 4 février 2010, dispose que : « *les méthodes spécifiques de recueil de données, peuvent être mises en œuvre compte tenu de la menace potentielle, si les méthodes ordinaires de recueil de données sont jugées insuffisantes pour permettre de récolter les informations nécessaires à l'aboutissement d'une mission de renseignement. La méthode spécifique doit être choisie en fonction du degré de gravité de la menace potentielle pour laquelle elle est mise en œuvre. La méthode spécifique ne peut être mise en œuvre qu'après décision écrite et motivée du dirigeant du service et après notification de cette décision à la commission* » (l'article 3 de la loi de 1998 entend par « commission » : la commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données des services de renseignement et de sécurité).

L'article 18/3 § 2 de la loi du 4 février 2010 précitée prévoit par ailleurs que « *Les membres de cette commission peuvent contrôler à tout moment la légalité des mesures, y compris le respect des principes de subsidiarité et de proportionnalité. Ils peuvent, à cet effet, pénétrer dans les lieux où sont réceptionnées ou conservées les données relatives aux méthodes spécifiques, se saisir de toutes les pièces utiles et entendre les membres du service. Les données recueillies dans des conditions qui ne respectent pas les dispositions légales en vigueur sont conservées sous le contrôle de la commission, selon les modalités et les délais fixés par le Roi, après avis de la commission de la protection de la vie privée. La commission interdit aux services de renseignement et de sécurité d'exploiter ces données et suspend la méthode mise en œuvre si celle-ci est toujours en cours. La commission notifie de sa propre initiative et sans délai »*

Le même article 18/3 de la loi du 4 février 2010 dispose enfin que « *L'officier de renseignement désigné pour mettre en œuvre la méthode spécifique de recueil de données informe régulièrement le dirigeant du service de l'exécution de cette méthode* ».

- Méthodes exceptionnelles : observation et surveillance d'espaces privés non accessibles au public ; création et emploi d'une personne morale en vue de soutenir des activités opérationnelles et d'avoir recours à des agents du service de renseignement ; ouverture de courrier et recueil d'informations auprès des services postaux ; recueil de données sur des comptes et transactions bancaires, pénétration dans un système informatique, mise sur écoute d'une ou plusieurs personnes sur écoute et enregistrement des communications téléphoniques.

La mise en œuvre des méthodes spécifiques est soumise au principe de subsidiarité et de proportionnalité qui est prévu à l'article Art. 18/9 § 2 de la loi du 4 février 2010.

L'article 18/10 § 1 de la loi du 4 février 2010 dispose que *« Le dirigeant du service soumet son projet d'autorisation à l'avis conforme de la commission administrative chargée de la surveillance, qui vérifie si les dispositions légales relatives à l'utilisation de la méthode exceptionnelle pour le recueil de données, ainsi que les principes de proportionnalité et de subsidiarité sont respectés (…). Sauf disposition légale contraire, la période durant laquelle*

la méthode exceptionnelle de recueil de données peut être appliquée ne peut excéder 2 mois, sans préjudice de la possibilité de prolongation (...). L'officier de renseignement désigné pour mettre en œuvre la méthode exceptionnelle de recueil de données informe régulièrement le dirigeant du service, qui, à son tour, informe la commission de l'exécution de cette méthode, selon les modalités et délais déterminés par le Roi ».

Aux termes de l'article 18/10 § 6 de la loi du 4 février 2010, *« La commission met fin à la méthode exceptionnelle de recueil de données lorsqu'elle constate que les menaces qui l'ont justifiée ont disparu ou si la méthode exceptionnelle ne s'avère plus utile à la finalité pour laquelle elle a été mise en œuvre, ou suspend la méthode exceptionnelle en cas d'illégalité. »*

1.3.4.2 Les instances gouvernementales en charge de la définition de la politique de renseignement et des organes de contrôle des services

1.3.4.2.1. Les instances politiques de coordination et d'impulsion de la politique en matière de renseignement

1.3.4.2.1.1. Un organe de coordination a été créé, l'OCAM (Organe de Coordination pour l'Analyse de la Menace), par la loi du 10 juillet 2006

La loi du 10 juillet 2006 charge l'OCAM de l'analyse de la menace en matière de terrorisme et d'extrémisme. Placé sous l'autorité conjointe des ministres de la justice et de l'intérieur, cet organisme a pour mission d'effectuer des évaluations stratégiques et ponctuelles sur les menaces terroristes et extrémistes à l'encontre de la Belgique, son travail reposant essentiellement sur l'analyse des informations transmises par les services d'appui[3] .

Banque de données OCAM :

L'arrêté royal en date du 28 novembre 2006 portant exécution de la loi du 10 juillet 2006 prévoit la création au sein de l'OCAM d'un système d'information composé d'une banque de données et de fichiers de travail créés pour des durées variables aux fins de l'analyse d'une ou de plusieurs menaces particulières. Ces données doivent présenter un lien direct avec la finalité du fichier et se limiter aux exigences qui en découlent. A la clôture de chaque analyse, une évaluation détermine les données qui sont intégrées dans la banque de données et celles qui sont détruites. A l'expiration du délai d'enregistrement, la nécessité de leur conservation ultérieure est examinée sur la base d'une évaluation du lien direct qu'elles doivent encore présenter avec les finalités pour lesquelles cette banque de données a été créée.

Procédure d'embargo :

Par dérogation à l'obligation pour les services d'appui de communiquer leurs informations à l'OCAM, les renseignements de nature judiciaire dont le Procureur fédéral estime que la communication à l'OCAM peut compromettre l'exercice de l'action publique ou la sécurité de personnes, sont exclusivement transmis au directeur de l'OCAM. Le directeur de l'OCAM et le Procureur fédéral décident conjointement si et dans quelle mesure ces renseignements sont intégrés dans l'évaluation et, le cas échéant, à quelles autres autorités cette évaluation est communiquée.

1.3.4.2.1.2. Le comité ministériel du renseignement et de la sécurité chargé de la définition de la politique de renseignement

Le Comité ministériel du renseignement et de la sécurité est l'organe politique chargé de déterminer la politique générale gouvernementale en matière de renseignement et de sécurité.

Ce comité est présidé par le Premier ministre, la plupart des ministres régaliens y siègent (intérieur, défense, justice, affaires étrangères). Il prend des initiatives politiques et législatives dans ce domaine.

Ses décisions sont exécutées par le Collège du renseignement et de la sécurité (qui doit devenir le Conseil national de Sécurité) qui est composé du délégué du Premier ministre, des chefs des services de renseignement, de la gendarmerie et de la police ainsi que d'un haut fonctionnaire du ministère des affaires étrangères.

1.3.4.3 Les organes de contrôle des services de renseignement

1.3.4.3.1. Le comité permanent « R » est l'organe de contrôle du respect des libertés individuelles et de l'efficacité des services de renseignement.

Ses membres ne sont pas des parlementaires, mais ils sont nommés par le Sénat. Les contrôles du comité « R » portent en particulier sur le respect des droits fondamentaux par les services de renseignement civils et militaires, et sur leur « coordination et (leur) efficacité ». En outre, ce comité contrôle le fonctionnement de l'OCAM. Le contrôle porte en principe aussi bien sur la légalité que sur l'efficacité et la coordination des services de renseignement. En ce qui concerne les services d'appui de l'OCAM, le contrôle porte uniquement sur leur obligation de communiquer des informations en matière de terrorisme et d'extrémisme.

Le contrôle s'effectue soit d'initiative, soit à la demande du parlement, du ministre compétent ou de l'autorité compétente. Le Comité peut aussi ouvrir une enquête sur plainte ou dénonciation d'un citoyen ou d'un fonctionnaire. En outre, il répond aux demandes d'avis de la Chambre des Représentants, du Sénat ou d'un ministre compétent sur tout projet de loi, d'arrêté royal, de circulaire ou sur tout autre document en matière de renseignement.

1.3.4.3.2. Le comité permanent « P » de contrôle des services de police

Le Comité « P » a été créé en 1991, afin de doter le Parlement fédéral d'un organe de contrôle externe sur la police. Il exerce sa mission *via* différents canaux, notamment au travers de l'examen des plaintes de citoyens. Il convient toutefois de préciser que le Comité « P » ne remplit pas de fonction de médiation et n'a pas été créé pour résoudre des problèmes individuels de plaignants en relation avec la police.

Grâce aux multiples enquêtes de contrôle et à l'examen des plaintes effectués par son Service d'enquêtes, le Comité « P » peut fournir une image fiable du fonctionnement actuel de la police. Complétée par des informations issues de nombreuses autres sources, elle lui permet d'assumer une fonction d'observatoire du fonctionnement de ce service, au bénéfice du Parlement fédéral et de l'ensemble des citoyens.

Les organes de contrôle des comités permanent « P » et « R » font eux-mêmes l'objet de contrôle par le sénat et la chambre des représentants chargés de superviser leur fonctionnement. Dans cette configuration, il convient d'observer que les parlementaires contrôlent non les services de renseignement mais l'organe chargé du contrôle de ces derniers

1.3.4.3.3 Les autres instances de contrôle des services de renseignement à la disposition des citoyens

L’Ombudsman fédéral est compétent pour les plaintes déposées par des particuliers, peut exécuter des instructions et consulter les dossiers. Mais les services de renseignement ne sont nullement tenus de lui transmettre des informations secrètes.

La commission de la protection des données examine, à la demande des citoyens, les informations personnelles établies par les services de renseignement; elle ne peut toutefois remettre que des recommandations et ne doit pas divulguer le contenu des dossiers.

Partie 2 - Analyse des dispositions envisagées

2.1. Objectifs poursuivis par la loi

La loi poursuit deux objectifs complémentaires :

- mieux encadrer l'activité des services de renseignement, d'une part, par une définition claire et accessible de leurs missions, des techniques mises en œuvre et des procédures d'autorisation et, d'autre part, par un renforcement du contrôle de ces mesures, par une autorité administrative indépendante, et par une juridiction spécialisée ;

- donner, par voie de conséquence, un cadre légal à l'activité des services de renseignement en leur permettant d'élargir le spectre légal des techniques pouvant être mises en œuvre, pour mieux répondre aux finalités énoncées par la loi.

2.1.1 Des finalités élargies

La sécurité nationale et la sauvegarde des intérêts fondamentaux de la Nation sont les objectifs de la politique de renseignement. Les finalités restent conformes aux objectifs de protection de l'ordre public et de prévention de ses atteintes et s'inscrivent dans le cadre de la police administrative. Elles sont également conformes aux finalités prévues par l'article 8 de la CEDH justifiant une ingérence dans la vie privée, parmi lesquelles la sécurité nationale, la sûreté publique, le bien-être économique du pays, la défense de l'ordre et la prévention des infractions pénales, la protection de la santé ou de la morale, ou la protection des droits et libertés d'autrui.

2.1.2. Une meilleure définition des services autorisés à mettre en œuvre les techniques de renseignement

La loi permet aux services spécialisés de renseignement de mettre en œuvre l'ensemble des techniques de renseignements entrant dans le champ de la loi.

Cela découle de l'article D. 1128 du code de la défense, créé par l'article 1er du décret n° 2014-474 du 12 mai 2014 pris pour l'application de l'article 6 *nonies* de l'ordonnance 55-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires, dans sa rédaction issue de la loi du 13 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019.

Les services spécialisés qui, avec le coordonnateur national du renseignement et l'académie du renseignement, forment la communauté française du renseignement, sont la direction générale de la sécurité extérieure (DGSE), la direction de la protection et de la sécurité de la défense (DPSD), la direction du renseignement militaire (DRM), la direction générale de la sécurité intérieure (DGSI), le service à compétence nationale dénommé « direction nationale du renseignement et des enquêtes douanières » (DNRED) et le service à compétence nationale dénommé « traitement du renseignement et action contre les circuits financiers clandestins » (TRACFIN).

Toutefois, l'autorisation peut également être donnée, seulement pour certaines de ces techniques et finalités de l'article L. 811-4 du code de la sécurité intérieure, à certains services désignés par un décret en Conseil d'Etat pris près avis de la Commission nationale de contrôle des techniques de renseignement, qui se substitue à la CNCIS, afin de tenir compte du fait qu'ils poursuivent (notamment certains services de police) des finalités entrant dans le champ de l'article L. 811-4 susmentionné.

2.1.3 Un encadrement plus lisible de l'autorisation de mise en œuvre et de ses dérogations

2.1.3.1 La loi soumet la mise en œuvre des techniques de renseignement à une **autorisation du Premier ministre, après avis préalable d'une autorité administrative indépendante**, la Commission nationale de contrôle des techniques de renseignement, avis qui, de surcroît, doit être rendu de manière expresse lorsque la technique implique une intrusion dans un lieu privé.

Lorsque le recueil de cet avis n'est pas possible, compte tenu de l'urgence absolue qui s'attache à la mise en œuvre du dispositif, l'autorité indépendante est toutefois saisie dans les plus brefs délais et recouvre ses pouvoirs de contrôle lors de l'exécution de la mesure.

La loi encadre très précisément la collecte, la durée de conservation des informations collectées et la traçabilité de l'ensemble des opérations résultant de l'autorisation de mise en œuvre de la technique de renseignement, de la demande, des modalités de sa mise en œuvre, de la nature des données collectées, de leur durée de conservation et de leur destruction, afin d'en permettre un contrôle effectif.

Enfin, lorsqu'une autorisation a été accordée après avis défavorable et recommandation au Premier ministre demeurée sans réponse ou sans réponse satisfaisante, la Commission peut saisir, à la majorité absolue de ses membres, le Conseil d'Etat.

2.1.3.2 L'ensemble des techniques de renseignement est soumis à cette procédure, qui peut toutefois être allégée pour tenir compte de certaines contraintes.

La loi ne prévoit pas elle-même que la surveillance des communications émises ou reçues à l'étranger soit soumise à un avis préalable de la CNCTR. Elle ne l'exclut pas pour autant et le décret en Conseil d'Etat auquel l'article L. 853-1 du même code renvoie pour définir notamment « la procédure de délivrance des autorisations d'exploitation des correspondances » pourra prévoir l'intervention en amont de la CNCTR, quitte à différencier suivant les autorisations concernées. Pour des raisons liées à la confidentialité et au risque que ferait courir à l'efficacité de l'action des services la divulgation de certaines capacités techniques ou modes opératoires, la loi renvoie également à un décret non publié le soin de définir les modalités de mise en œuvre de cette surveillance particulière. Ce décret non publié sera toutefois pris en Conseil d'Etat et porté à la connaissance de la délégation parlementaire au renseignement et de la CNCTR.

Cet encadrement en retrait par rapport à la procédure de droit commun alors même que peuvent être impliqués des identifiants rattachables au territoire national lorsqu'ils sont interlocuteurs d'un identifiant étranger, peut se justifier par la technique mise en œuvre (on ne cible pas l'identifiant national mais l'identifiant étranger et ce n'est que par voie de conséquence, que l'identifiant national est surveillé), et dans la mesure où la loi prévoit qu'au

cas où un identifiant français est impliqué, la conservation et la destruction des données interceptées basculent dans le régime de droit commun des interceptions de sécurité, à l'exception près du point de départ du délai de conservation des correspondances qui court à compter de la date de leur première exploitation, différence notamment justifiée par les difficultés d'accès linguistiques aux contenus de ces correspondances.

2.1.3.3 Enfin, des garanties supplémentaires sont prévues pour les mesures impliquant une intrusion dans lieux privés à usage d'habitation ou dans les systèmes de traitement automatisé de données

S'il est désormais admis que ces mesures, lorsqu'elles interviennent dans le cadre de la police administrative, n'ont pas à faire l'objet d'une autorisation préalable du juge judiciaire, pas plus qu'elles n'ont à être effectuées sous le contrôle de l'autorité judiciaire, il reste que leur mise en œuvre doit être particulièrement encadrée, compte tenu de l'atteinte qui est portée à la vie privée et familiale, conçue dans son acception la plus forte.

Pour tenir compte de cette nécessité et la concilier avec les objectifs des services opérationnels qui supposent que la mesure soit mise en œuvre à l'insu des personnes concernées, de manière rapide et confidentielle, la loi prévoit un encadrement plus important que pour les autres mesures et tenant :

- à la subsidiarité de la mise en œuvre de ces modalités, l'intrusion dans le domicile ou dans un système de traitement automatisé de données ne pouvant être autorisée que si elle est indispensable pour recueillir les renseignements recherchés. Cette nécessité doit être spécialement motivée dans l'autorisation ;
- à un avis exprès de la CNCTR, y compris en urgence, cet avis, lorsqu'il est rendu par un seul de ses membres, ne pouvant l'être que par l'un des membres conseiller d'Etat ou conseiller à la cour de cassation ;
- à l'encadrement de l'introduction limitée au temps strictement nécessaire à la mise en place, à l'utilisation ou au retrait des dispositifs techniques mentionnés aux articles L. 851-6 et L.854-2 du même code, limitée à certains agents spécialement habilités ;
- à la limitation de la durée de l'autorisation à deux mois ;
- lorsque l'autorisation a été accordée sur avis défavorable de la CNCTR ou lorsque celui-ci n'a pas donné suite aux recommandations qu'elle a émises, deux membres seulement de cette commission peuvent saisir le Conseil d'Etat de la régularité de la mise en œuvre de ces intrusions.

2.1.4. Un contrôle plus effectif

2.1.4.1 Une traçabilité des mesures facilitant le contrôle

La traçabilité de la mise en œuvre des techniques de renseignement est un élément important du nouveau dispositif dans la mesure où elle permet à la CNCTR de vérifier, à tout moment, l'exécution conforme de la mesure à l'autorisation donnée.

Cette traçabilité s'exerce sous le contrôle d'un service placé auprès du Premier ministre et grâce à :

- la tenue d'un registre recensant les demandes et autorisations de mise en œuvre des techniques de renseignement ;
- la centralisation de l'exécution des interceptions de sécurité et des demandes de données de connexion par le Premier ministre ;

- la tenue de relevés d'exécution des mesures dans les services, conformément à des règles de centralisation définies par le Premier ministre ;
- la tenue de relevé de destruction des données dans les services.

2.1.4.2 Une durée de conservation maitrisée

En application de l'article L. 822-2 du même code, les renseignements recueillis doivent être détruits au terme d'une durée maximale de douze mois à compter de leur recueil. Cette durée maximale est toutefois réduite à un mois à compter de leur enregistrement s'agissant des correspondances faisant l'objet d'interceptions de sécurité, ou portée à cinq ans à compter du recueil, s'il s'agit de données de connexion. Lorsque les correspondances sont chiffrées, le point de départ du délai de conservation est reportée à la date de leur déchiffrement.

Une durée plus longue est également possible s'agissant des données contenant des éléments de cyber-attaque ou des données chiffrées, et ce, à des seules fins d'analyse technique (identification et traitement des virus, décryptement) et à l'exclusion de toute utilisation pour la surveillance des personnes concernées par la mesure initiale.

La destruction des renseignements extraits ou transcrits est obligatoire dès qu'ils ne sont plus utiles aux finalités poursuivies.

2.1.4.3. Un contrôle effectif par deux autorités

En matière de mesures de surveillance constituant une ingérence dans la vie privée, un mécanisme de contrôle peut être institué à trois moments : lorsqu'on l'ordonne, pendant qu'on la mène ou après qu'elle a cessé.

S'agissant des deux premières phases, la nature et la logique mêmes de la surveillance secrète commandent d'exercer à l'insu de l'intéressé non seulement la surveillance comme telle, mais aussi le contrôle qui l'accompagne. Cela est admis par la CEDH.

Toutefois, puisque l'intéressé sera le plus souvent empêché d'introduire un recours effectif ou de prendre une part directe à un contrôle quelconque, il se révèle indispensable que les procédures existantes procurent en elles-mêmes des garanties appropriées et équivalentes, sauvegardant les droits de l'individu et que l'ingérence de l'exécutif dans les droits d'un individu soit soumise à un contrôle efficace.

Si elle reconnaît que le contrôle juridictionnel offre, en principe, les meilleures garanties d'indépendance, d'impartialité et de procédure régulière, la CEDH admet la possibilité qu'un tel contrôle soit exercé par une autorité administrative indépendante au regard de l'effectivité du contrôle dont elle dispose (autorisation, contrôle tout au long de l'exécution de la mesure, possibilité d'être saisi par tout individu se croyant surveillé), ce contrôle étant alors apte à limiter à ce qui était « nécessaire, dans une société démocratique » l'ingérence résultant de la législation incriminée (*Klass et autres précité, § 53 à 60*).

Toutefois, au plan interne, les dispositions de l'article 20 de la Constitution font obstacle à ce qu'une telle autorité soit dotée du pouvoir d'ordonner au Premier ministre d'interrompre une mesure de surveillance qu'elle considérerait comme illégale ou la destruction des données collectées sur le fondement d'une telle mesure. Cette autorité administrative indépendante ne

peut être dotée que d'un pouvoir de recommandation, qui, s'il n'est pas suivi d'effet, ne garantit pas suffisamment les droits des personnes visées par les mesures en cause.

C'est pourquoi il a été opté pour la création d'un système double :

- un contrôle par une autorité administrative indépendante, en cours de procédure ;
- un contrôle juridictionnel ad hoc, par une formation du Conseil d'Etat permettant de concilier les droits des administrés et les exigences de confidentialité de la procédure pour des données le plus souvent couvertes par le secret de la défense nationale.

2.1.4.3.1. Un contrôle effectif par une autorité administrative indépendante en cours d'exécution

2.1.4.3.1.1 Des pouvoirs élargis

La CNCTR dispose tout d'abord d'un droit de communication important : elle a communication de toutes les autorisations délivrées par le Premier ministre et peut également demandée à être informée, à tout moment, des modalités d'exécution des autorisations en cours et dispose d'un droit d'accès à tous documents utiles à son contrôle (autorisation, relevés, registres…)

Lorsqu'elle estime, spontanément ou sur saisine d'un tiers y ayant un intérêt direct et personnel, que la mesure est irrégulière, elle peut inviter le Premier ministre à l'interrompre, à détruire les données collectées ou à prendre les mesures correctrices qui s'imposent, le Premier ministre devant l'informer sans délai des suites données à ses recommandations-

Lorsque certaines mesures de surveillance ont été autorisées après son avis défavorable ou lorsque les recommandations qu'elle a effectuées pour interrompre ces mesures sont restées sans suite, elle peut, à la majorité absolue de ses membres ou seulement si deux d'entre eux le demandent lorsque la mesure s'accompagne d'une intrusion dans un lieu privé ou un système de traitement automatisé des données, décider de saisir le Conseil d'état, afin de le faire statuer sur la régularité d'une telle mesure.

Enfin, si comme la CNCIS actuellement, elle rédige un rapport public faisant état du nombre des irrégularités signalées au Premier ministre et des suites qui y ont été données, elle adresse également au Premier ministre, à tout moment, les observations qui lui paraissent utiles, observations qui peuvent être communiquées à la délégation parlementaire au renseignement.

2.1.4.3.1.2 Sur l'ensemble des mesures de renseignement mises en œuvre

Bien que toutes les techniques de renseignement mises en œuvre dans le cadre de la présente loi n'obéissent pas à la procédure d'autorisation sur avis préalable de la CNCTR, rares sont celles qui lui échappent purement et simplement, notamment lorsqu'il apparaît qu'un identifiant rattachable au territoire national est finalement impliqué, par voie de conséquence de la surveillance de tiers.

Si l'on peut admettre que la CNCTR ne puisse autoriser a priori, des mesures de surveillance aléatoire ou non ciblées ou ciblant des personnes se trouvant à l'étranger (surveillance internationale ..), son intervention est systématiquement rétablie, a posteriori, afin de garantir une égalité de traitement, dès lors qu'est impliqué un identifiant rattachable au territoire national.

Enfin, et même dans le cas de mesures de surveillance n'impliquant que des identifiants étrangers, la loi prévoit une possibilité de contrôle de leur exécution par la CNCTR avec une possibilité de rapport au Premier ministre sur les conditions d'exécution et de recommandation d'interrompre la mesure si elle estime que celle-ci est irrégulière

2.1.4.3.2 Un contrôle juridictionnel effectif

Le Conseil constitutionnel et la CEDH admettent la possibilité de concilier les exigences du droit au recours effectif d'une part, et le respect des objectifs des services de renseignement d'autre part, au premier chef desquels figure le secret des mesures de surveillance mises en œuvre au prix de la mise en œuvre de garanties adéquates et suffisantes contre les abus, car « *un système de surveillance secrète destiné à protéger la sécurité nationale crée un risque de saper, voire de détruire, la démocratie au motif de la défendre* (*Klass et autres*, précité, §§ 49-50, *Leander*, précité, § 60, *Camenzind c. Suisse*, 16 décembre 1997, § 45, *Recueil* 1997-VIII, et *Lambert*, précité, § 31).

2.1.4.3.2.1 *Attribution au Conseil d'Etat des contentieux relatifs à la mise en œuvre des techniques de renseignement relatifs à la sûreté de l'Etat*

Le projet de loi confie au Conseil d'Etat, en premier et dernier ressort, par voie d'action ou d'exception**,** l'ensemble du contentieux de la régularité de la mise en œuvre des techniques de renseignement.

Une telle solution présente de nombreux avantages :

- D'une part, le contrôle est exercé par la plus haute juridiction, les membres siégeant dans la formation de jugement étant habilités ès qualité, au secret de la défense nationale, et ayant, de ce fait, accès à l'ensemble des documents détenus par les services, pour exercer un contrôle effectif.

- La formation de jugement ainsi habilitée est seule compétente pour statuer sur la régularité de la mise en œuvre d'une technique de renseignement, qu'elle soit saisie très largement par voie d'action ou à titre préjudiciel, par toute juridiction saisie d'un litige dont la solution dépend de la régularité de la technique mise en œuvre et qui souhaiterait user de cette procédure sans nécessairement demander la déclassification des données.

- Sa nature juridictionnelle lui confère des pouvoirs d'annulation, d'indemnisation ou d'injonction et lui permet également de lier l'appréciation des juges de droit commun qui la saisissent sur la question de la régularité des techniques de renseignement mises en œuvre.

2.1.4.3.2.2 Une procédure aménagée

Afin de concilier les exigences de la doctrine du renseignement et celles du procès équitable, la procédure suivie devant le Conseil d'Etat déroge au code de justice administrative sur plusieurs points essentiels :

- un jugement en premier et dernier ressort par le Conseil d'Etat, dont la formation de jugement, composée de trois membres, peut être élargie lorsque l'importance de l'affaire le justifie ;
- une instruction non contradictoire et couverte par le secret de la défense nationale ;
- une audience séparée pour le requérant et pour les services, cette dernière se tenant à huis clos ;
- une communication systématique de la requête à la commission nationale de contrôle des techniques de renseignement qui peut présenter des observations ;
- une décision limitée à son dispositif ;
- une possibilité de se borner à confirmer ou infirmer l'existence de la mise en œuvre d'une technique alléguée.

Ces dérogations, importantes aux principes des droits de la défense et du droit au procès équitable, sont toutefois contrebalancées par des pouvoirs accrus du juge spécialisé :

- le juge peut être saisi très largement, sans obstacle probatoire, par toute personne y ayant un intérêt direct et personnel qui soupçonnerait seulement la mise en œuvre à son endroit, d'une mesure de surveillance et dans certains cas, par la CNCTR ;

- cette saisine n'est enfermée dans aucun délai ni formalisme si ce n'est la saisine préalable par le requérant seulement, de la CNCTR, qui, compte tenu de la particularité de ce contentieux, a pour effet de mettre en état le dossier en ses lieu et place ;

- le juge dispose d'un accès à l'ensemble des documents et informations détenus par les services, aucun secret ne lui étant opposable. Son contrôle est donc plein et entier, contrairement à ce qui existe aujourd'hui (cf. CE Assemblée, 6 novembre 2002, Moon) ;

- afin de pallier l'impossibilité pour le justiciable, de soulever des moyens alors qu'il ne connaît pas la mesure en cause, la loi permet au juge de se saisir de tout moyen, même d'office. De même, les requêtes sont systématiquement communiquées à la CNCTR qui peut présenter des observations ;

- en outre, la juridiction est dotée de pouvoirs importants, puisqu'elle peut annuler l'autorisation, ordonner la destruction des données collectées ou, s'il le demande, indemniser le requérant du préjudice qu'il estime avoir subi ;

- enfin, lorsqu'elle constate qu'une irrégularité est susceptible de constituer une infraction pénale, la juridiction en donne avis au procureur de la République et transmet l'ensemble des éléments du dossier au vu desquels elle a statué à la

Commission consultative du secret de la défense nationale, afin que celle-ci donne son avis au Premier ministre sur la possibilité de déclassifier tout ou partie des éléments en vue de leur transmission au procureur de la République.

Ainsi, les principes mis en œuvre par la loi apparaissent très protecteurs dans la mesure où ils garantissent :

- une prévisibilité de la loi, accessible aux citoyens tant par sa précision et sa lisibilité que par son champ d'application qui englobe l'ensemble des techniques de renseignement pouvant être mises en œuvre et l'ensemble des services habilités à le faire ;

- une procédure très encadrée, permettant un contrôle effectif par une autorité indépendante, en cours d'exécution ;

- un contrôle juridictionnel dérogatoire mais de nature à garantir un droit au recours effectif.

2.2. L'examen des dispositions

2.2.1. Dispositions générales (Livre VIII, titre 1er)

2.2.1.1. Etat du droit

En l'état actuel du droit, seul l'emploi des interceptions de sécurité fait l'objet d'un cadre légal, qui est prévu aux articles L.241-1 à L.241-4 du code de la sécurité intérieure. Ce cadre précise le principe du secret des correspondances auquel il ne peut être porté atteinte que par la loi, dans les seuls cas de nécessité d'intérêt public. Ces nécessités sont énumérées à l'article L.241-2 de ce code.

2.2.1.2. Difficultés rencontrées

Le cadre légal actuel ne concerne que les interceptions de sécurité, les autres techniques de renseignement ne disposant pas de cadre légal. Au-delà de la définition de ce cadre légal étendu pour les différentes techniques de renseignement, l'actualisation des finalités du renseignement est nécessaire, aux fins de les préciser et de les adapter au contexte actuel, dans la mesure où elles n'ont pas été modifiées depuis la loi de juillet 1991. .

2.2.1.3. Objectif recherché

Les techniques de renseignement disponibles étant plus larges que les seules interceptions de sécurité, il convient de permettre leur emploi dans des conditions légales pour les services de renseignement qui souhaitent y recourir, tout en cadrant leur utilisation à des finalités limitativement énumérées. Il apparaît également souhaitable de préciser davantage les finalités en les étendant pour couvrir tous les besoins de recueil du renseignement.

2.2.1.4. Options

La définition de finalités spécifiques selon les techniques de renseignement utilisées ou selon les services n'avait guère de sens. Dès lors que l'ensemble des techniques de renseignement faisaient l'objet d'un cadre légal, les finalités avaient vocation à leur être communes. Le maintien des finalités actuelles aurait également pu être préféré, considérant que l'intervention de nouvelles techniques était sans effet sur les finalités pour lesquelles le renseignement est mis en œuvre. Toutefois, depuis la loi de 1991, à l'origine de ces dispositions du code de sécurité intérieure, des manques sont apparus dans les finalités. De plus, des services entrant dorénavant dans le champ de la loi nécessitent une actualisation de ces finalités. Enfin, la notion de « sécurité nationale » n'est pas précisée dans la loi, concept s'avérant particulièrement large tout en ne couvrant pas nécessairement tous les besoins.

Le choix a donc été fait de définir des finalités pour l'ensemble des techniques du renseignement, en les définissant plus précisément.

Sept grandes catégories de finalités sont désormais envisagées.

Cinq sont communes avec les finalités figurant à l'article L. 241-2 du code de la sécurité intérieure :

- la sécurité nationale ;
- les intérêts économiques et scientifiques essentiels de la France ;
- la prévention du terrorisme
- la prévention de la criminalité et de la délinquance organisées ;
- la prévention de la reconstitution ou du maintien de groupements dissous en application de l'article L. 212-1 ;

Ont été ajoutés :

- les intérêts essentiels de la politique étrangère et l'exécution des engagements européens et internationaux de la France ;
- la prévention des violences collectives de nature à porter gravement atteinte à la paix publique.

La référence à la notion de sécurité nationale, mentionnée par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et précisée, en droit interne, par l'article L. 1111-1 du code de la défense, inclut l'indépendance nationale, l'intégrité du territoire et la défense nationale, ainsi que la prévention de toute forme d'ingérence étrangère et des atteintes à la forme républicaine et à la stabilité des institutions. La référence à l'exécution des engagements internationaux de la France, exigence constitutionnelle, permet d'inclure notamment la prévention de la prolifération des armes de destruction massive.

2.2.1.5. Impacts attendus

Les finalités ainsi définies couvrent l'intégralité de l'activité de renseignement des services utilisant les techniques entrant dans le champ de la loi.

2.2.2 Dispositions relatives à la procédure applicable (Livre VIII, titre II)

2.2.2.1 Etat du droit

En l'état actuel du droit, ne sont réglementées que la procédure des interceptions de sécurité (article L. 241-2 et suivants du code de la sécurité intérieure) et celle de l'accès aux données de connexions (article L. 246-1 du code de la sécurité intérieure).

2.2.2.1.1 Procédure d'autorisation

Les interceptions de sécurité sont autorisées par le Premier ministre, sur demande écrite et motivée des ministres de la défense, de l'intérieur ou du ou des ministres chargés des douanes, et sont transmises sous 48h, à une autorité administrative indépendante : la commission nationale de contrôle des interceptions de sécurité (CNCIS). Si le président de la CNCIS considère que la légalité de l'autorisation n'est pas certaine, il peut réunir la CNCIS, qui, lorsqu'elle estime qu'une interception de sécurité a été autorisée en méconnaissance de la loi, peut adresser au Premier ministre et au ministre dont émane la demande, une recommandation tenant à ce qu'elle soit interrompue. Le Premier ministre informe sans délai la CNCIS des suites données à cette recommandation.

L'accès aux données de connexion est autorisé par une personnalité qualifiée placée auprès du Premier ministre, sur demande des agents, individuellement désignés et dûment habilités, des services relevant des ministres de l'intérieur, de la défense ou de celui chargé des douanes.

L'accès à ces données en temps réel, sur sollicitation des opérateurs du réseau peut, en outre, être autorisé par le Premier ministre pour une durée maximale de 30 jours, sur demande des mêmes ministres. Cette autorisation est ensuite communiquée au président de la CNCIS sous 48h qui peut, s'il estime la décision illégale, réunir la commission qui statue dans un délai de 7 jours et peut, le cas échéant, émettre des recommandations tendant à ce qu'il soit mis fin à la mesure.

2.2.2.1.2. Difficultés rencontrées

Ces difficultés sont de plusieurs ordres :

En premier lieu, la CNCIS ne connaît que d'un nombre limité de techniques de renseignement, en l'occurrence régies par la loi de 1991.

En second lieu, la CNCIS intervient *a posteriori*, l'autorisation ayant déjà été délivrée par le Premier ministre, même si, dans la pratique, la CNCIS émet un avis *a priori* s'agissant des demandes d'interceptions de sécurité et d'accès aux données de connexion en temps réel. Ses pouvoirs sont limités dès lors que, lorsqu'elle constate la mise en œuvre irrégulière d'une technique, elle ne dispose que du pouvoir d'émettre une recommandation au Premier ministre qui doit lui faire connaître (sans délai pour les interceptions de sécurité et sous 15 jours pour les données de connexion) les suites qui ont été données. Elle peut également remettre un rapport rendu public sur les recommandations émises et leur suivi mais ne peut saisir la délégation parlementaire au renseignement ni les juridictions de droit commun.

2.2.2.1.3. Objectifs recherchés

- Soumettre l'ensemble des techniques de renseignement à une même procédure d'autorisation claire, précise et prévisible pour le citoyen ;
- Prévoir l'avis préalable d'une autorité administrative indépendante : la commission nationale de contrôle des techniques de renseignement, avec des pouvoirs renforcés pour certaines mesures plus attentatoires aux libertés, comportant l'intrusion dans un lieu privé
- Elargir le contrôle de l'autorité administrative indépendante sur le déroulement des mesures mises en œuvre, en dotant la CNCTR de pouvoirs effectifs
- Créer un contrôle juridictionnel ad hoc, conciliant les exigences de confidentialité inhérentes aux mesures de surveillance mises en œuvre avec celles du droit au procès équitable.

2.2.2.1.4 Liste des dispositions législatives et réglementaires à modifier

2.2.2.1.4.1 Autorisation de mise en œuvre (Chapitre 1er Titre II- article L. 821-1 et suivants)

L'article L. 821-1 crée une procédure unique pour l'ensemble des techniques de recueil du renseignement mentionnées au titre V du Livre VIII (L. 821-1), à savoir :

- l'accès aux données de connexion ;
- les interceptions de sécurité ;
- les captation, fixation, transmission et enregistrement de parole prononcées à titre privé ou confidentiel ou d'image de personne se trouvant dans un lieu privé ;
- les captation, transmission et enregistrement de données informatiques.

Seules en sont exclues les mesures de surveillance internationale prévues à l'article L. 854-1 qui sont soumises à une procédure spécifique (cf. infra).

La procédure de droit commun applicable à l'ensemble des autres techniques peut varier en fonction de l'urgence, ou des modalités particulières des mesures de surveillance qui peuvent rendre impossible un avis préalable de la CNCTR ou au contraire, en faire un élément quasi-conforme de la procédure, la CNCTR pouvant alors saisir la Conseil d'Etat en cas d'autorisation donnée nonobstant son avis défavorable.

Cette procédure est organisée selon les principes de prévisibilité et de traçabilité correspondant aux normes constitutionnelles et conventionnelles :

L'article L. 821-2 encadre la demande des services, qui doit être précise et circonstanciée, s'agissant des finalités recherchées, des techniques envisagées, des personnes, lieux ou véhicules ciblés. Ainsi, en vertu du principe de proportionnalité, une autorisation ne pourra être délivrée que si la finalité invoquée par le service à l'origine de la demande est en adéquation avec les missions qui lui sont confiées.

L'article L. 821-3 prévoit la procédure d'avis de la CNCTR : cet avis est rendu sous 24 h par son président ou l'un de ses membres. La commission peut être réunie à la demande du président, s'il estime que la conformité à la loi d'une demande n'est pas certaine. Dans ce cas l'avis est rendu sous 3 jours ouvrables. En l'absence d'avis rendu dans ce délai, l'avis est réputé rendu.

Cette procédure allie les exigences opérationnelles, par sa rapidité, l'avis pouvant être rendu, lorsqu'aucun problème n'est décelé, « sous 24h » et par la possibilité de désigner un seul membre pour statuer, et celles de la sécurité juridique puisque le membre statuant seul peut toujours recourir à un avis collégial.

L'article L. 821-4 encadre l'autorisation donnée par le Premier ministre: doivent y être précisés expressément, la ou les techniques dont la mise en œuvre est autorisée, la ou les finalités poursuivies, sa durée de validité dans la limite d'une durée maximale de 4 mois , les personnes, lieux ou véhicules sur lesquelles elle porte.

Enfin, l'autorisation doit également préciser le ou les services autorisés à mettre en œuvre la ou les mesures autorisées, parmi les services de renseignement mentionnés à l'article 6 *nonies* de l'ordonnance n° 58-100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires ou ceux, autres que les services de renseignement, figurant dans un décret en Conseil d'Etat précisant, pour chaque service, celles des finalités et techniques pouvant donnant lieu à autorisation.

Cette autorisation doit pouvoir se démarquer de la demande, dès lors que les services peuvent être amenés à demander l'autorisation de mettre en œuvre plusieurs techniques différentes, avec un degré d'ingérence variable. La décision finale appartient au Premier ministre, celui-ci pouvant être conduit à limiter cette autorisation dans la durée, dans l'étendue des mesures sollicitées ou des personnes visées ou à la limiter à certaines finalités seulement.

La demande et la décision d'autorisation sont enregistrées par les services du Premier ministre sur des registres tenus à la disposition de la CNCTR et qui constituent les premiers éléments d'un dispositif de traçabilité assuré par un service placé auprès du Premier ministre et auxquels s'ajouteront ensuite, les procès-verbaux d'exécution des mesures et de destruction des données.

Afin de répondre aux contraintes opérationnelles, l'article L. 821-5 prévoit enfin une procédure d'urgence absolue, sans avis préalable de la CNCTR mais information immédiate de celle-ci. : cette procédure, qui n'a vocation à être utilisée qu'à titre exceptionnel, compte tenu des facilités opérationnelles prévues par l'article L. 821-3 (avis sous 24h, par un seul membre), devra être expressément motivée et réservée aux cas qui ne peuvent être anticipés et ne souffrent aucune attente (pose de balise par exemple), à l'instar de ce qui existe en procédure judiciaire (cf. article 230-35 CPP).

L'article L. 821-6 prévoit dans tous les cas, que lorsqu'elle estime qu'une autorisation a été accordée en méconnaissance des dispositions précitées, la CNCTR peut émettre une recommandation motivée visant à l'interrompre et à détruire les données collectées sur son fondement. Le Premier ministre doit alors l'informer sans délai des suites qu'il réserve à cette recommandation

Lorsque le Premier ministre ne donne pas suite à cette recommandation ou lorsqu'elle estime que les suites sont insuffisantes, la Commission peut, à la majorité absolue de ses membres, décider de saisir le Conseil d'Etat

Au total, cette procédure très détaillée dans la loi, placée sous le regard direct de la CNCTR - y compris en urgence - qui peut formuler des avis préalables, des recommandations, en cas de passer outre ou de mise en œuvre non conforme visant à interrompre ou détruire les données collectées, et, le cas échéant, saisir le Conseil d'Etat, est très protectrice et constitue une garantie efficace pour le citoyen.

2.2.2.1.4.2 Renseignements collectés (Chapitre II-Titre II- article L. 822-1 et suivants)

Le régime actuel des interceptions de sécurité prévoit une durée de conservation de 10 jours à compte de la date des enregistrements, la transcription des interceptions devant ensuite être détruite, sans condition de délai, *dès que leur conservation n'est plus indispensable à la réalisation des fins mentionnée* (cf. L. 242-7 du code de la sécurité intérieure)

Les articles L 822-1 et suivants créent un régime de conservation des informations plus maîtrisé :

Pour garantir l'effectivité du contrôle, l'article L. 822-1 prévoit une traçabilité de la mise en œuvre des mesures (date de début et fin de la mise en œuvre, nature des données recueillies) organisée par un service placé auprès du Premier ministre qui définit les modalités de leur centralisation.

Le relevé des opérations est conservé par le service qui a mis en œuvre la mesure et tenu à la disposition de la CNCTR L'article L. 822-3 prévoit d'ailleurs que les renseignements ne peuvent être collectés, transcrits, extraits ou exploités à d'autres fins que celles prévues par la loi.

L'article L. 822-2 module la durée de conservation des correspondances enregistrées en fonction de leur nature, afin de concilier protection de la vie privée et usage opérationnel par les services.

Les données recueillies doivent être détruites au terme d'une durée maximale de douze mois à compter de leur recueil. Cette durée maximale est toutefois réduite à un mois à compter de leur enregistrement, s'il s'agit d'interceptions de sécurité, ou portée à cinq ans, s'il s'agit de données de connexion. Lorsque les renseignements recueillis sont chiffrés, la durée peut être prolongée pour les seuls besoins de l'analyse technique du chiffrement.

Une durée plus longue est également possible s'agissant des données contenant des éléments de cyber-attaque, et ce, à des seules fins d'analyse technique (identification et traitement des virus) et à l'exclusion de toute utilisation pour la surveillance des personnes concernées par la mesure initiale.

Les données recueillies ne peuvent être extraites ou exploitées pour d'autres fins que celles mentionnées à l'article L. 811-3. Les extraits ou exploitations doivent être détruits lorsqu'ils ne sont plus indispensables à la réalisation de ces fins (article L. 822-3), et font l'objet de relevés accessibles à la CNCTR (article L. 822-4 du même code).

Pour les données de connexion, la durée de cinq ans proposée dans le texte apparaît comme un allongement raisonnable.

Issu du décret d'un décret du 24 décembre 2014 pour l'application de l'article 20 de la loi de programmation militaire du 18 décembre 2013, l'article R 246-6 du code de la sécurité intérieure dispose : « Le Premier ministre enregistre et conserve pendant une durée maximale de trois ans, dans un traitement automatisé qu'il met en œuvre, les informations ou les documents transmis par les opérateurs et les personnes mentionnés à l'article L 246-1. »

Or des exemples récents montrent que cette durée de trois ans peut poser problème : il est parfois nécessaire de pouvoir remonter l'historique des données collectées sur une étendue de temps plus longue. En matière de contre-espionnage, où les enquêtes s'étalent souvent sur de très longues durées, le besoin d'un historique de données est encore plus prégnant (par exemple dans le cas d'une « cellule dormante »).

S'agissant des « contenus » (images de personnes dans un lieu privé, données informatiques), la durée proposée, fixée à un an, concilie strictement l'atteinte à la vie privée et les contraintes liées aux enquêtes. Toutefois, dans un souci de renforcement des garanties et s'agissant des paroles prononcées à titre privé ou confientiel, elles sont détruites au plus tard à l'expiration d'un délai d'un mois à compter de leur enregistrement, selon le même régime que celui des interceptions de sécurité.

Contrairement aux données collectées dans le cadre de réquisitions judiciaires qui sont conservées, quelle que soit leur nature, pour le temps nécessaire à l'enquête – et bien souvent des années, les données recueillies en matière de renseignement ne sont conservées que pour une durée limitée alors que comme en matière judiciaire, certaines enquêtes peuvent avoir une durée importante.

2.2.2.2. Création de la Commission nationale de contrôle des techniques de renseignement (Livre VIII, titre IV, chapitre I à IV)

2.2.2.2.1 Etat du droit

En l'état actuel du droit, seules deux techniques de renseignement sont soumises, à des degrés variables, à une autorité administrative indépendante, la Commission nationale de contrôle des interceptions de sécurité (CNCIS) prévue aux articles L. 243-1 à L. 243-11 du code de la sécurité intérieure.

Interceptions de sécurité

De sa propre initiative ou sur saisine de toute personne y ayant un intérêt direct et personnel, la CNCIS peut procéder au contrôle des interceptions de sécurité en cours, et en cas de constat d'irrégularité, recommander au Premier ministre son interruption. Elle informe ensuite le requérant qu'elle a procédé aux vérifications nécessaires.

La CNCIS remet chaque année un rapport au Premier ministre, qui le rend public, précisant notamment le nombre de recommandations formulées et les suites qui y sont apportées. Elle lui adresse en outre, toute recommandation qu'elle juge utile.

Accès aux données de connexion

La CNCIS dispose d'un accès permanent au dispositif de recueil des informations ou documents mis en œuvre, afin de procéder aux contrôles visant à s'assurer du respect des conditions fixées par la loi. En cas de manquement, elle adresse une recommandation au Premier ministre qui doit lui faire connaître, dans un délai de 15 jours, les mesures prises pour remédier au manquement constaté.

2.2.2.2.2. Difficultés rencontrées

Outre son champ d'intervention réduit, les pouvoirs de la CNCIS sont également insuffisants puisqu'elle n'émet pas d'avis préalable sur les demandes d'accès aux données de connexion et, en l'état actuel du droit, sur les demandes d'interceptions de sécurité, même si tous les Premiers ministres successifs depuis 1991 ont validé la pratique de l'avis préalable par la CNCIS avant de rendre leur décision.

Composée de 9 membres : 2 membres du Conseil d'Etat, 2 de la cour de cassation 4 parlementaires et une personnalité qualifiée en matière de communication électronique nommés pour une durée de 6 ans, elle ne saurait faire face à l'afflux d'avis résultant de la création d'une procédure d'avis préalable et de contrôle des mesures de surveillance régies par le présent projet de loi. Les membres issus du Conseil d'Etat et de la Cour de Cassation sont renouvelés par moitié tous les 3 ans.

2.2.2.2.3. Objectif recherché

Les pouvoirs doivent être élargis pour permettre à cette autorité administrative indépendante de constituer un contrepoids efficace au Gouvernement, dans l'utilisation des techniques de renseignement.

Les articles L. 831-1 et L. 832-2 définissent cette autorité administrative indépendante, composée de 9 membres : 2 conseillers d'Etat, 2 conseillers à la Cour de cassation, une personnalité qualifiée pour sa connaissance en matière de communications électroniques, 2 députés et 2 sénateurs, les parlementaires étant désignés par le président de chaque assemblée aux fins d'assurer une représentation pluraliste du Parlement.

<u>Son indépendance est garantie :</u>

- par un mandat de 6 ans (à l'exception des parlementaires désignés pour la durée de la législature) non renouvelable, une nomination de ses membres par décret et leur inamovibilité (article L. 831-2 du même code) ;
- par la règle selon laquelle, dans l'exercice de leur mission, les membres de la commission ne reçoivent d'instruction d'aucune autorité (article L. 832-1 du même code) ;
- par l'incompatibilité avec tout intérêt direct ou indirect dans l'activité des personnes mentionnées à l'article L. 34-1 du code des postes et des communications électroniques et 1 et 2 de la loi pour la confiance dans l'économie numérique.

L'article L. 832-3 du code de la sécurité intérieure définit les règles de quorum, fixé à 4 membres, l'inscription de cette règle participant à l'objectif de prévisibilité.

Au titre de son pouvoir de contrôle élargi, la CNCTR bénéficie d'un accès large aux informations relatives aux mesures de surveillance mises en œuvre :

L'article L. 832-5 du même code prévoit en premier lieu que les membres de la commission sont autorisés, es qualité, à avoir accès à tout élément d'information couvert par le secret de la défense nationale et utile à l'exercice de leur mission.

L'article L. 833-2 du même code organise un véritable droit d'information de la CNCTR, à divers moments de la procédure. Elle reçoit ainsi, de plein droit, les demandes et autorisations délivrées et peut avoir accès à tous les registres, relevés, enregistrements et transcriptions mentionnées au titre II, de même qu'elle peut demander à être informée à tout instant des modalités d'exécution des autorisations en cours. Le Premier ministre peut également lui communiquer tout ou partie des rapports de l'inspection des services du renseignement ainsi que des rapports des inspections des ministères, en lien avec les missions de la Commission.

Cette information élargie permet un contrôle plus effectif :

L'article L. 833-3 du même code lui permet, comme l'ancienne CNCIS, de procéder au contrôle de toute technique mise en œuvre, de sa propre initiative ou sur saisine de toute personne y ayant un intérêt direct et personnel.

- Lorsqu'elle est saisie d'un simple soupçon de mise en œuvre d'une mesure de surveillance, elle procède au contrôle de la ou des techniques invoquées en vue de vérifier qu'elles ont été ou sont mises en œuvre dans le respect des dispositions légales et peut se borner à notifier à l'auteur de la réclamation qu'il a été procédé aux vérifications nécessaires, sans confirmer ni infirmer leur mise en œuvre (article L. 833-3 du même code)

- Elle peut, le cas échéant, inviter le Premier ministre à ordonner l'interruption de la mesure concernée et la destruction des données collectées ou prendre les mesures correctrices nécessaires pour éviter la réitération de l'irrégularité constatée (article L. 833-4 du même code)

- Elle peut enfin, à la majorité absolue de ses membres, saisir le Conseil d'Etat lorsque ses avis ou recommandations au Premier ministre ne sont pas suivies d'effet (article L. 821-6 du même code). Cette saisine intervient à la demande de seulement deux membres lorsque la mise en œuvre d'une technique de renseignement s'accompagne d'une intrusion dans un lieu privé à usage d'habitation ou dans un système de traitement automatisé de données.

- Enfin, la CNCTR participe, par ses rapport et recommandations, à l'information du public et des assemblées parlementaires :
    - l'article L. 833-4 du code de la sécurité intérieure prévoit ainsi, à l'instar de ce que faisait la CNCIS, qu'elle remet un rapport au Premier ministre sur les modalités d'exercice de sa mission, le nombre des recommandations émises, notamment le nombre de demandes d'interruption de mesures et le nombre de fois où le Premier ministre n'y a pas donné suite ;
    - l'article L 833-5 du code de la sécurité intérieure prévoit en outre que la CNCTR adresse à tout moment au Premier ministre les observations qu'elle juge utiles ;

- l'article L. 833-6 du code de la sécurité intérieure l'autorise à répondre aux demandes d'avis du Premier ministre, des présidents des assemblées et de la délégation parlementaire au renseignement, étant observé en outre, que son président peut, comme aujourd'hui le président de la CNCIS, être auditionné.

Ces observations et rapport sont également communiqués à la délégation parlementaire au renseignement.

2.2.2.2.4 Impact attendu

- Création de la CNCTR

Comme elle le rappelle dans son 22ème rapport d'activité pour les années 2013-2014, la CNCIS « fonctionne à effectifs constants depuis sa création il y a près d'un quart de siècle alors que ses missions se sont considérablement accrues au fil des années ». Composée de 3 membres, parmi lesquels figurent deux parlementaires qui n'assistent qu'aux réunions organisées à intervalles réguliers, la CNCIS ne dispose aujourd'hui, outre son président, que de 4 agents exerçant à temps plein.

Héritière de la CNCIS, la CNCTR verra ses missions considérablement élargies :

- à l'ensemble des techniques de recueil de renseignement prévues par la loi, et non plus aux seules interceptions de sécurité et demandes d'accès administratif aux données de connexion ;
- elle agira par ailleurs *a priori*, en formulant un avis préalable à l'octroi de l'autorisation d'agir (ce qui n'était pas prévu par la loi du 10 juillet 1991), sauf dans un nombre limité de cas, mais aussi pendant la mise en œuvre de la technique et *a posteriori*, une fois le recours à la technique terminé.

Par conséquent, afin qu'elle puisse exercer un contrôle efficace, garant de la protection des libertés individuelles, la CNCTR se verra doter des moyens nécessaires à l'accomplissement de ses missions, en particulier du fait de leur nature de plus en plus technique, et d'exercer en complète indépendance.

La CNCTR sera ainsi composée de 9 membres (contre 3 pour l'actuelle CNCIS), indépendants du pouvoir exécutif : 4 magistrats (2 du Conseil d'Etat et 2 de la Cour de cassation), 1 personnalité qualifiée pour sa connaissance en matière de communications électroniques (nommée par le président de l'ARCEP) et 4 parlementaires (2 députés et 2 sénateurs, assurant une représentation pluraliste du Parlement).

Outre les agents exerçant actuellement au sein de la CNCIS, la CNCTR verra ses moyens en personnels renforcés. Un secrétaire général assistera le président de la commission et de nouveaux agents seront recrutés en raison de leurs compétences juridiques mais aussi de leurs compétences techniques en matière de communications électroniques et de protection des données personnelles.

D'ores et déjà, un ingénieur sera recruté à la CNCIS dans le courant de l'année 2015.

Les moyens dévolus à l'actuelle personnalité qualifiée prévue à l'actuel article L.246-2 du code de la sécurité intérieure, compétente pour statuer sur les demandes d'accès administratif

aux données de connexion, placée auprès du Premier ministre mais qui travaille d'ores et déjà en étroite coopération avec la CNCIS, ont vocation à intégrer la CNCTR.

Enfin, comme c'est le cas depuis 1991, la CNCTR pourra s'appuyer, dans le cadre de ses missions, sur les moyens du Groupement interministériel de contrôle (GIC), structure dépendant du Premier ministre. Les moyens du GIC seront eux-mêmes renforcés et adaptés au regard de l'activité supplémentaire induite par la mise en œuvre de la loi. Un audit sera très prochainement réalisé afin d'évaluer précisément ces besoins nouveaux.

- La procédure d'autorisation et de contrôle

Ainsi décrite, la procédure d'autorisation et de contrôle est extrêmement lisible, traçable et accessible et permet de déterminer l'ensemble des conditions d'autorisation d'une mesure de surveillance sollicitée et des points de contrôle effectués tant par la CNCTR que par le Premier ministre.

Cette clarté de la procédure participe d'une part, à l'exigence de prévisibilité de la loi et d'autre part, contribue à l'effectivité du contrôle des mesures autorisées, tant sur le bien-fondé de l'autorisation que sur le respect de ses conditions.

Elle rend également accessible la procédure aux fonctionnaires qui la mettent en œuvre et permet de tracer une ligne de partage entre l'ordre manifestement illégal, parce que n'entrant pas dans les finalités ou ne résultant pas de la procédure ainsi décrite et le commandement légitime, permettant à l'agent d'être exonéré de sa responsabilité pénale, en cas de mise en œuvre simplement illégale.

Toutefois, si cette procédure encadrée est une condition importante de l'effectivité du contrôle, elle n'est pas suffisante, compte tenu des exigences constitutionnelles et conventionnelles, qui imposent que l'autorité de contrôle dispose de pouvoirs effectifs vis-à-vis de l'autorité administrative.

C'est la raison pour laquelle le projet de loi prévoit de doubler le contrôle a priori et en cours d'exécution par un contrôle juridictionnel, au moyen d'une juridiction ad hoc propre à concilier les exigences de confidentialité des mesures de surveillance avec le droit au recours effectif dont doivent bénéficier tous les citoyens.

2.2.2.3 Attribution du contentieux de la régularité de la mise en œuvre des techniques de renseignement au Conseil d'Etat (Titre IV)

2.2.2.3.1. Etat du droit

En l'état actuel du droit, il n'existe pas de juridiction ad hoc : les citoyens peuvent soit contester la décision administrative autorisant la mise en œuvre d'une technique de renseignement, soit saisir le juge pénal, lorsque la mesure a été mise en œuvre en dehors de toute autorisation ou en méconnaissance de l'autorisation donnée.

Concrètement, le plus souvent, le contrôle de la mesure est exercé par le juge pénal lorsqu'il est saisi d'écoutes téléphoniques manifestement illégales et donc susceptibles d'être qualifiées d'atteintes au secret des correspondances par une personne dépositaire de l'autorité publique.

En effet, dans ce cas, l'exonération de responsabilité prévue au deuxième alinéa de l'article 122-4 du code pénal et relative au commandement de l'autorité légitime n'est plus opérante ainsi que cela a été rappelé dans l'arrêt de la chambre criminelle de la Cour de cassation relative à l'affaire des "écoutes de l'Elysée" (Crim, 30 septembre 2008) : les juges retiennent que, nonobstant l'absence de cadre légal et la violation de la procédure administrative mise en place par les directives des Premiers ministres successifs, "*le commandement de l'autorité légitime ne peut être retenu en faveur d'un officier supérieur de gendarmerie et de hauts fonctionnaires dès lors que ne leur était imposée aucune obéissance inconditionnelle à des ordres manifestement illégaux*".

2.2.2.3.2. Difficultés rencontrées

L'effectivité du contrôle est limitée par plusieurs contraintes :

- d'une part, en application de l'article R. 421-1 du code de justice administrative, le juge administratif ne peut être saisi que d'une décision : or le citoyen n'en a pas nécessairement connaissance, ce qui concrètement limite le contrôle du juge administratif ; par ailleurs, il ne peut être saisi d'un simple soupçon ;

- d'autre part, tant le contrôle du juge administratif que celui du juge pénal sont limités par le secret de la défense nationale : seules les opérations déclassifiées peuvent être portées à sa connaissance et lui permettre d'apprécier le caractère manifestement illégal d'une décision ou d'un agissement ;

- même lorsque les informations ne sont pas couvertes par le secret de la défense nationale, la doctrine du renseignement impose que la personne faisant l'objet d'une mesure de surveillance régulière ou à l'inverse, ne faisant l'objet d'aucune mesure de surveillance, soit tenue dans l'ignorance de cette stratégie afin d'éviter qu'elle adapte son comportement en conséquence ;

- C'est également le cas en matière d'accès aux informations contenues dans les fichiers dits de souveraineté (intéressant la sureté nationale) pour lesquels toute communication d'information compromet la finalité du traitement (présence ou absence de l'intéressé dans le fichier, nature des éléments y figurant ou n'y figurant pas…).

Par suite :

- soit le juge ne peut exercer aucun contrôle avant déclassification par le Premier ministre ou le ministre compétent, après avis de la CCSDN : pas de contrôle effectif et risque de condamnation pénale de l'agent ayant mis en œuvre une technique de renseignement, faute pour le juge de vérifier qu'il l'a fait sur ordre légitime ;

- soit, pour les informations non classifiées dont la communication ne compromet pas la finalité du traitement, l'administration produit des notes blanches (rares) ;

- soit, lorsque la production de notes blanches met en évidence qu'une personne fait l'objet d'une surveillance et compromet de ce fait la finalité assignée au traitement, le juge fait application de la jurisprudence *Moon* (CE Ass., 6 novembre 2002, *Moon Sun Myung*, n° 194295, au recueil) qui postule la divisibilité des informations

contenues dans un fichier. Or cette jurisprudence, rendue à propos d'un fichier SIS et non d'un fichier relatif à la sureté de l'Etat, heurte de plein fouet la doctrine du renseignement qui impose, par essence, qu'aucune donnée ne soit communiquée (politique de non confirmation, non dénégation, admise par la CEDH-Affaire Kennedy 2010) ;

Il est donc indispensable, tant pour les informations classifiées résultant par nature, des mesures, que celles contenues dans les fichiers de souveraineté (concrètement, parmi ceux de l'article 26 de la loi de 1978, ceux qui ont pour finalité la sureté de l'Etat) de permettre au juge de se fonder sur tous les éléments versés à la procédure, sans les verser au contradictoire :

- Afin de lui permettre d'exercer un contrôle plein et entier
- Sans déroger au secret de la défense nationale ni aux exigences de la doctrine du renseignement.

2.2.2.3.3. Objectif recherché

L'idée est de confier, par voie d'action ou d'exception, à une juridiction administrative spécialisée, l'ensemble du contentieux de la régularité de la mise en œuvre des techniques de renseignement. Cela vise à concilier les exigences de confidentialité, inhérentes au fonctionnement des services de renseignement avec le droit des citoyens, notamment au recours effectif, la juridiction spécialisée, dotée de pouvoirs d'instruction accrus, exerçant un contrôle pour son compte.

Le projet de loi du gouvernement aménage également la procédure applicable au contentieux de la mise en œuvre des traitements ou partie de traitements relatifs à la sûreté de l'Etat, d'ailleurs le plus souvent renseigné par des données issues de mesures de surveillance.

En effet, même si le fondement est différent (secret de la défense nationale ou doctrine du renseignement), dans les deux cas :

- Le juge doit pouvoir tout contrôler, sans limite, avec des pouvoirs de juge de plein contentieux

- Mais les personnes visées par les mesures ou les fichiers ne doivent rien savoir, pas même connaître l'existence de ces mesures ou ces données.

2.2.2.3.4. Modalités de mise en œuvre.

Afin de leur permettre un contrôle effectif, les membres Conseil d'Etat sont autorisés es qualité, à connaître des informations protégées par le secret de la défense nationale et utiles à leur mission, ce qui leur permet un contrôle effectif (article L. 841-2 du code de la sécurité intérieure), et ont accès à l'ensemble des pièces en possession de la CNCTR et des services, sans que ces documents soient versés dans le cadre de l'instruction contradictoire (article L. 842-4 du même code).

Le Conseil d'Etat est seul compétent pour statuer sur la légalité de la mise en œuvre d'une technique de renseignement, par voie d'action : à ce titre, il peut être saisi par toute personne y ayant un intérêt direct et personnel, ce qui constitue un mode de saisine très large, sans obstacle probatoire, le simple soupçon étayé de la mise en œuvre d'une mesure de surveillance suffisant. Afin d'offrir une garantie supplémentaire au citoyen, la saisine du Conseil d'Etat est précédée d'une saisine de la CNCTR, qui de fait, constitue une instance de mettre en état sa réclamation.

Il peut également être saisi par la CNCTR à la majorité absolue de ses membres (ou de seulement d'eux d'entre eux lorsque la technique de renseignement s'accompagne d'une intrusion dans un domicile ou dans un système de traitement automatisé d'informations), lorsque celle-ci estime qu'une mesure a été autorisée ou une technique a été mise en œuvre en méconnaissance des dispositions de la présente loi ou que ses recommandations n'ont pas été suivies d'effet.

Il peut enfin être également saisi à titre préjudiciel, par toute juridiction administrative ou autorité judiciaire saisie d'un litige dont la solution dépend de la légalité d'une technique de renseignement couverte par le secret de la défense nationale, dont la mise en œuvre est alléguée : la juridiction de droit commun, pénale ou administrative ou le procureur de la République, peuvent ainsi le saisir à titre préjudiciel et se trouvent liés par sa décision quant à la légalité de la technique mise en œuvre.

A ce titre, seule la juridiction pénale regarde comme opérant le moyen tiré de l'irrégularité de la mise en œuvre des techniques de renseignement, soit pour condamner pénalement son auteur, soit pour annuler la procédure fondée sur les données collectées irrégulièrement. L'article L. 842-6 du code de la sécurité intérieure prévoit à ce titre que lorsque l'irrégularité constatée par le Conseil d'Etat est susceptible de constituer une infraction, elle en avise le procureur de la République et transmet l'ensemble des éléments du dossier au vu duquel elle a statué à la Commission consultative du secret de la défense nationale afin que celle-ci donne au Premier ministre son avis sur la possibilité de déclassifier tout ou partie de ces éléments en vue de leur transmission au Procureur de la République.

L'article 4 aménage la procédure applicable à ce contentieux, en dérogeant sur certains points au code de justice administrative, pour concilier droit au recours effectif et exigences du secret de la défense nationale. Est ainsi inséré un chapitre spécial au titre VII du Livre VII du code de justice administrative, relatif au contentieux de la mise en œuvre des techniques de renseignement.

Ces aménagements, exigés par le secret de la défense nationale, portent essentiellement :

- sur une procédure contradictoire asymétrique, adaptée aux exigences du secret de la défense nationale : la formation de jugement peut se fonder sur tous éléments relatifs à la mise en œuvre des techniques alléguées sans les verser au contradictoire (article L. 773-3 du même code).
- à la publicité des audiences à laquelle le président de la formation de jugement peut déroger en ordonnant le huis-clos (article L. 773-4 du même code).

- à la motivation de la décision, qui lorsqu'aucune technique de renseignement n'a été mise en œuvre ou lorsqu'elle l'a été de manière légale, se borne à indiquer qu'aucune illégalité n'a été commise, sans confirmer ni infirmer la mise en œuvre d'une telle technique (article L. 773-6 du même code). Cette motivation est donc compatible avec

la doctrine du renseignement qui suppose que les mesures de renseignement soient mises en œuvre à l'insu des personnes qu'elles visent, afin de ne pas compromettre les finalités poursuivies ou la sécurité des services ou des sources.

Ces possibilités sont autant d'aménagements rendus indispensables par la doctrine du renseignement, qui impose que la personne faisant l'objet d'une mesure de surveillance régulière ou à l'inverse, ne fait l'objet d'aucune mesure de surveillance, soit tenue dans l'ignorance de cette stratégie afin d'éviter qu'elle adapte son comportement en conséquence.

Pour pallier ces aménagements notables en termes de droit au procès équitable, le Conseil d'Etat est doté de pouvoir d'instruction accrus :

- les membres de la formation de jugement et le rapporteur public sont habilités es-qualité au secret de la défense nationale et peuvent avoir accès à l'ensemble des pièces détenues par la CNCTR et les services (article L. 773-2 du même code) ;
- pour pallier le caractère particulier de ce contentieux qui se développe sans décision et sans instruction écrite et contradictoire et ne permet pas au requérant de soulever les moyens pertinents, les membres de la formation de jugement peuvent relever tout moyen d'office (article L. 773-3 du même code) ;
- en outre, ils peuvent entendre, à tout moment de la procédure et lors d'audience séparées, le plaignant d'une part et les représentants du premier ministre ou des services ayant mis en œuvre la technique incriminée (article L. 773-5 du même code) ;
- enfin, lorsqu'elle n'est pas la requérante, la CNCTR reçoit systématiquement communication de la procédure et peut présenter des observations de nature à éclairer l'avis qu'elle a rendu (article L. 773-4 du même code).

Enfin, les pouvoirs de la formation de jugement sont ceux d'une juridiction de plein contentieux de droit commun : lorsqu'elle constate qu'une technique de renseignement est ou a été mise en œuvre ou exploitée en méconnaissance des dispositions du livre VIII du code de la sécurité intérieure, elle peut annuler l'autorisation et ordonner la destruction des renseignements irrégulièrement collectés, en informe la juridiction qui l'a éventuellement saisie ou le requérant sans faire état d'éléments protégés par le secret de la défense nationale. Elle peut également, lorsqu'elle est saisie de conclusions en ce sens, condamner s'il y a lieu, l'Etat, à l'indemniser le plaignant du préjudice qu'il a subi.

Pour pallier l'étanchéité de la procédure relative à la régularité de la mise en œuvre des techniques de renseignements à l'égard des autorités judiciaires, notamment pénales, le projet de loi institue un mécanisme novateur qui permet à la formation de jugement, lorsqu'elle estime que l'irrégularité constatée est susceptible de constituer une infraction, d'en aviser le procureur de la République et de transmettre l'ensemble des éléments du dossier au vu duquel elle a statué à la Commission consultative du secret de la défense nationale afin que celle-ci donne au Premier ministre son avis sur la possibilité de déclassifier tout ou partie de ces éléments en vue de leur transmission au procureur de la République.

Enfin, autre innovation procédurale, le projet de loi prévoit également, en son article 11, que les exigences de la procédure contradictoire sont adaptées au contentieux portant sur l'accès ou la mise en œuvre de traitements ou partie de traitements intéressant la sûreté de l'Etat (dont la liste est fixée par décret en Conseil d'État).

Ce contradictoire est plus ou moins adapté selon que les informations sont couvertes par le secret de la défense nationale (absence totale de contradictoire) ou que la communication des

informations, même non couvertes par le secret de la défense nationale, est susceptible de compromettre les finalités du traitement.

Dans ce dernier cas, la juridiction de jugement se fonde sur les éléments contenus le cas échéant dans le traitement sans les révéler ni préciser si le requérant figure ou non dans le traitement. Toutefois, lorsqu'elle constate que le traitement ou la partie de traitement faisant l'objet du litige comporte des données personnelles le concernant qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite, elle en informe [peut en informer] le requérant. »

2.2.2.3.5. Impacts attendus

Cette procédure contentieuse est une véritable innovation, créant un véritable contrôle effectif et pertinent du juge, compatible avec le fonctionnement des services du renseignement.

L'existence d'une telle procédure, confiée au Conseil d'Etat en premier et dernier ressort, est une garantie forte, permettant de concilier le secret de la défense nationale avec le droit au recours, la juridiction étant à même d'effectuer un contrôle plein et entier sans se voir opposer un quelconque secret, puis de tirer les conséquences de ce contrôle, par voie d'action ou d'exception, en allant jusqu'à aviser le procureur de la République et à saisir la CCSDN pour donner un caractère totalement effectif à ce contrôle.

Le contrôle opéré est donc plein et entier, sans que le secret de la défense nationale y fasse obstacle, la juridiction étant ensuite à même de tirer les conséquences concrètes de ce contrôle, avec des pouvoirs qui, contrairement à ceux d'une autorité administrative indépendante, s'imposent au Premier ministre et aux juridictions de renvoi.

Les décisions du Conseil d'Etat sont rendues en premier et dernier ressort, selon une procédure asymétrique dérogeant, sur certains points, au code de justice administrative.

2.2.2.4. Disposition visant à encadrer les interceptions de sécurité (Livre VIII, titre III, Chapitre II)

2.2.2.4.1 Etat du droit

Les interceptions de sécurité sont régies par les articles L. 241-1 à L. 245-3 du code de la sécurité intérieure.

Ces interceptions s'inscrivent dans le cadre de finalités limitativement énumérées par l'article L. 241-2 : la recherche « *des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de l'article L. 212-1* ».

L'autorisation prévue à l'article L. 241-2 est accordée par décision écrite et motivée du Premier ministre ou de l'une des deux personnes spécialement déléguées par lui. Elle est donnée sur proposition écrite et motivée du ministre de la défense, du ministre de l'intérieur ou du ministre chargé des douanes, ou de l'une des deux personnes que chacun d'eux aura spécialement déléguées. Le Premier ministre, en l'occurrence le groupement interministériel de contrôle (GIC), organise la centralisation de l'exécution des interceptions autorisées.
L'autorisation mentionnée à l'article L. 241-2 est donnée pour une durée maximum de quatre mois, selon des quotas arrêtés par ministère. Elle cesse de plein droit de produire effet à l'expiration de ce délai. Elle ne peut être renouvelée que dans les mêmes conditions de forme et de durée.

La mise en œuvre de ces interceptions s'effectue sous le contrôle d'une autorité administrative indépendante : la commission nationale de contrôle des interceptions de sécurité (CNCIS). Si le président de la CNCIS considère que la légalité de l'autorisation n'est pas certaine, il peut réunir la CNCIS, qui, lorsqu'elle estime qu'une interception de sécurité a été autorisée en méconnaissance de la loi, peut adresser au Premier ministre et au ministre dont émane la demande, une recommandation tenant à ce qu'elle soit interrompue. Le Premier ministre informe sans délai la CNCIS de suites données à cette recommandation.

Les opérations font l'objet, sous l'autorité du Premier ministre, de relevés faisant état du début et fin de l'opération, et d'un relevé de destruction des enregistrements et des transcriptions

Les enregistrements sont détruits à l'expiration d'un délai de 10 jours. Les transcriptions doivent être détruites dès que leur conservation n'est plus nécessaire à la réalisation des finalités.

2.2.2.4.2. Difficultés rencontrées

Il y a une divergence entre les règles fixées par le législateur et la pratique des services et de la Commission Nationale des Interceptions de Sécurité (CNCIS) : en effet, dès les premiers mois de son fonctionnement, la CNCIS a instauré, avec l'accord du Premier ministre, un contrôle préalable à la décision d'autorisation, allant ainsi au-delà des exigences légales qui ne prévoyaient qu'un contrôle ex post de la commission.

Par ailleurs, le régime actuel circonscrit l'écoute à la personne faisant l'objet de l'interception. Or la réalité de la menace et l'efficacité des écoutes obligent les services à aller au-delà de la seule personne directement écoutée, un membre de son entourage immédiat étant susceptible de révéler des informations ayant un lien direct avec la poursuite des finalités assignées aux missions des services de renseignement.

2.2.2.4.3. Objectif recherché

L'objectif est d'inscrire ces interceptions de sécurité dans le cadre du régime général applicable à l'ensemble des techniques de renseignement mises en œuvre par les services de renseignement sans en modifier fondamentalement le régime.

Deux garanties supplémentaires ont été ajoutées par rapport au régime prévalant jusqu'alors :

- ces interceptions seront désormais soumises à l'avis préalable de la Commission nationale de contrôle des techniques de renseignement. Cette pratique, source de protection des droits des citoyens, sera désormais expressément prévue par la loi ;
- la durée de conservation des données recueillies est écourtée par rapport à la durée de droit d'un an, et est portée à 1 mois à compter de l'enregistrement des correspondances.

Par ailleurs, la rédaction du nouvel article L 852-1 du même code permettra que les écoutes puissent porter sur les correspondances échangées par des personnes appartenant à l'entourage de la personne visée, lorsqu'elles sont susceptibles de jouer un rôle d'intermédiaire, volontaire ou non pour son compte, ou de fournir des informations au titre de la finalité faisant l'objet de l'autorisation.

Les interceptions de sécurité sont évaluées à 6000 par an. Cette rénovation du cadre juridique pourrait favoriser leur mise en œuvre. Toutefois, l'impact est très difficile à évaluer.

2.2.2.4.4 Liste des dispositions législatives et réglementaires à modifier

Articles L 241-1 et suivants du code de la sécurité intérieure.

2.2.3. Dispositions relatives aux autres dispositifs techniques de captations des données (Livre VIII, titre III, chapitre III)

2.2.3.1. Etat du droit

Les dispositifs techniques de captation de données ne sont actuellement prévus et encadrés par aucun texte.

2.2.3.2. Difficultés rencontrées

Le caractère protéiforme de la menace nécessite un recueil d'information le plus large possible et ce quel que soit le support utilisé par les personnes ciblées par les services. Des données importantes à la réalisation des missions des services spécialisés du renseignement, peuvent ainsi être échangées via les nouveaux moyens électroniques d'échanges et/ou en certains lieux.

Or les services ne disposent aujourd'hui d'aucun cadre légal permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé ou la captation, la transmission et l'enregistrement de données informatiques transitant par un système automatisé de données ou contenues dans un tel système.

En l'absence d'un tel cadre légal, les agents qui mettraient en œuvre certaines de ces techniques de renseignement ainsi que leur hiérarchie, pourraient en outre, se voir reprocher des infractions en matière d'atteinte à la vie privée.

2.2.3.3. Objectif recherché

L'objectif principal est de donner aux services les moyens d'assurer de façon efficace les missions qui leur sont assignées, tout en entourant la mise en œuvre de ces techniques de garanties importantes, eu égard à la particulière atteinte à la vie privée qu'elles entrainent.

Par ailleurs, il s'agit de protéger les agents de ces services contre toute condamnation pénale : la responsabilité pénale des agents agissant désormais dans le cadre de la loi ne pourrait en effet plus être recherchée puisque, aux termes du premier alinéa de l'article 122-4 du code pénal, « *N'est pas pénalement responsable la personne qui accomplit un acte prescrit ou autorisé par des dispositions législatives ou réglementaires* ».

C'est le cas en matière d'enquête judiciaire : l'officier de police judiciaire et le juge d'instruction, lorsqu'ils mettent en œuvre des interceptions téléphoniques ou des sonorisation, ne commettent pas le délit d'atteinte à l'intimité de la vie privée prévu à l'article 226-1 du code pénal parce qu'ils agissent en application des articles 100 ou 706-96 du code de procédure pénale. Aucune immunité pénale n'est pourtant explicitement prévue, elle résulte directement et de manière suffisante de l'application de l'article 122-4 du code pénal.

2.2.3.4 Impacts attendus

L'instauration dans la loi d'un régime relatif à l'ensemble des techniques de captation des données assurera aux missions des services spécialisés la sécurisation matérielle et juridique indispensable à l'efficacité de leur mission.

Seront ainsi autorisés l'utilisation de dispositifs techniques permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou de l'image d'une personne se trouvant dans un lieu privé ainsi que la captation, la transmission et l'enregistrement de données informatiques.

Les demandes de communications de données de connexion sont évaluées à 350 000 par an. Il est attendu une augmentation des demandes à destination des opérateurs télécoms et des hébergeurs qu'il est difficile d'évaluer.

La plupart des grandes démocraties permettent à leurs services de renseignement de mettre en œuvre ces techniques. Ainsi, le *Regulation of Investagory Powers Act* de 2000, au Royaume-Uni, permet au ministre de l'intérieur de délivrer un *warrant* autorisant l'introduction dans un lieu aux fins d'installer des micros ou des caméras. De même, la loi italienne sur le renseignement de 2007 donne ce pouvoir au président du conseil. Peuvent être autorisées, dans ce cadre, des opérations visant à la captation de données informatiques ou l'intrusion dans les lieux privés d'habitation.

Par ailleurs, le droit pénal français prévoit, depuis 2011, de capter des flux de données informatiques.

La captation de données devient essentielle pour faire face au contournement, de plus en plus fréquent, des dispositifs d'interception (qu'il s'agisse de conversations téléphoniques ou d'échanges de correspondances électroniques). En effet, les services spécialisés sont confrontés à plusieurs phénomènes :

- le contournement des dispositifs d'interception, qu'il s'agisse de conversations téléphoniques ou d'échanges de correspondances électroniques ;

- les cibles, notamment terroristes, sont de plus en plus méfiantes à l'égard des moyens de communication et recourent de manière croissante à des moyens permettant de déjouer les interceptions (cryptage des communications orales ou des transmissions de données, utilisation de forums de discussion, enregistrement de données sur des serveurs accessibles au moyen d'un mot de passe, enregistrement de données dans une clef USB puis envoi de ces données depuis un ordinateur non surveillé dans un cybercafé, etc.) ;

- l'extraordinaire diversification des moyens de communication (téléphone, messageries Internet, Skype, etc.), d'ailleurs de plus en plus souvent cryptées, ne permet plus, au moyen de dispositif classique des interceptions, d'assurer une surveillance continue de la « cible » dès lors que celle-ci, comme c'est de plus en plus souvent le cas, change sans cesse de vecteur de communication ou d'identifiant (numéro de téléphone, adresse électronique, pseudonyme, etc.).

La captation des données informatiques présente un intérêt majeur en matière de contreterrorisme. En effet, l'utilisation massive par la mouvance jihadiste des nouvelles technologies de communication a considérablement accru l'échange de données de toutes natures (notamment photo et vidéo) échappant à l'interception. La récupération des données informatiques relatives notamment aux pages consultées, aux messages échangés ou encore à des commandes de matériels (des équipements de type paramilitaire sont fréquemment acquis par les candidats au départ en Syrie ou en Irak, ou commandés à leurs proches) est indispensable pour matérialiser leur engagement jihadiste, identifier leurs interlocuteurs et alimenter de futures procédures judiciaires.

Les dispositions sur la captation informatique trouveront également une application intéressante en matière de lutte contre la prolifération des armes de destruction massive : il s'agit alors de surveiller les organes, souvent des sociétés-écrans, qui cherchent à acquérir des biens auprès d'entreprises de haute technologie situés dans les grands pays industriels comme la France.

De même, les services spécialisés sont confrontés à une méfiance croissante des cibles, qui sont très informées des différentes techniques de surveillance des communications. Ainsi, certaines d'entre elles limitent au maximum les échanges d'informations par téléphone ou voie électronique.

En matière de terrorisme, et comme l'ont confirmé des cas récents, les projets criminels ont cette particularité qu'ils prennent forme de plus en plus souvent dans des cercles très restreints, familiaux ou amicaux, afin de limiter au maximum le risque de « fuite » ou d'exposition aux enquêtes. Par ailleurs, la méfiance est constante en matière de contre-espionnage ou de contre-ingérence, les services spécialisés ayant alors affaire à des professionnels du renseignement qui sont au fait de toutes les techniques de clandestinité et savent déjouer les filatures.

L'efficacité des investigations suppose donc de pouvoir disposer de techniques variées, y compris la pose et l'utilisation de dispositifs de captation d'images ou de sons. Ainsi, lorsque

la cible utilise avec prudence ses moyens de communication ou déjoue les surveillances physiques, seule la pose de micros ou de caméras permet de capter ses conversations ou de la voir manipuler par exemple des armes à feu ou des explosifs.

Dans certains cas, d'ailleurs, la mise en place des dispositifs techniques permet de lever le doute sur l'activité terroriste d'une personne et, le cas échéant, de mettre fin à des investigations inutiles pour réorienter l'activité des services vers des menaces avérées.

Dans le domaine de la haute criminalité organisée, les mêmes dispositifs permettront d'acquérir des informations précieuses à l'occasion de réunions de représentants de groupes criminels transnationaux qui peuvent se tenir en France, compte tenu de son attrait. De telles réunions, qui ne constituent pas en soi une infraction susceptible de mobiliser des moyens judiciaires, nécessitent une forte réactivité dès lors que les déplacements de ces personnes sont signalés dans le cadre de coopération avec les services partenaires.

2.2.3.5. Modalités de mise en œuvre

Compte tenu de l'ingérence plus importante portée à la vie privée par ces mesures, la durée de l'autorisation d'utilisation de dispositifs techniques permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou de l'image d'une personne se trouvant dans un lieu privé, ainsi que la captation, la transmission et l'enregistrement de données informatiques transitant par un système automatisé de données ou contenues dans un tel système.est réduite à deux mois, renouvelable dans les mêmes conditions de forme)

Lorsque la mise en œuvre de ces techniques doit s'accompagner de l''introduction dans un véhicule ou un lieu privé, ou de l'introduction dans un système de traitement automatisé de données, celle-ci sera possible mais entourée de garanties supplémentaires :

- la demande devra expressément justifier cette nécessité et préciser tous éléments permettant d'encadrer strictement cette pénétration ;
- les opérations matérielles nécessaires à la mise en place, l'utilisation ou au retrait de ces dispositifs techniques ne pourront être effectuées que par des agents spécialement habilités aux seules fins de la mise en place, l'utilisation ou le retrait du dispositif technique.
- L'avis de la CNCTR ne peut être rendu que de manière expresse, soit de manière collégiale, soit, par l'un de ses membres, membre du Conseil d'Etat ou de la Cour de cassation ;
- L'autorisation ne vaut que pour une durée maximale de 30 jours, renouvelable dans les mêmes formes
- Même en urgence, l'autorisation ne peut être donnée qu'après avis de la CNCTR, sauf lorsque cette autorisation ne concerne pas un lieu privé à usage d'habitation.
- Enfin, lorsque l'autorisation est donnée nonobstant l'avis défavorable de la CNCTR, deux de ses membres seulement peuvent saisir le Conseil d'Etat.

Au total, les garanties apportées aux personnes faisant l'objet de ces modalités particulières de mise en œuvre des techniques de renseignement apparaissent suffisantes au regard de l'ingérence portée à leur vie privée.

2.2.4. Dispositions visant à encadrer les mesures de surveillance internationale (Livre VIII, titre III, chapitre IV)

2.2.4.1 Objectif recherché

Cet article a pour objet d'offrir un cadre spécifique aux interceptions de communications électroniques émises ou reçues à l'étranger.

Les mesures de surveillance et de contrôle mises en œuvre dans le cadre des dispositions du présent article ne peuvent être diligentées que pour les finalités de droit commun qui président aux interceptions de sécurité réalisées sur le territoire national visées à l'article L.811-4.

Bien que l'objet de la surveillance prévue par le présent article porte sur les communications échangées par les personnes ne résidant pas habituellement sur le territoire national, des communications rattachées au territoire national peuvent être incidemment concernées par les mesures mises en œuvre au titre du présent article, si les personnes surveillées entrent en communication avec des personnes utilisant des identifiants français.

C'est pourquoi le troisième alinéa de l'article L. 853-1 prévoit explicitement que les communications interceptées dont l'une des terminaisons s'avèrerait rattachable au sol français seront soumises aux règles de conservation et de destruction de droit commun prévues par l'article L. 822-2 pour les correspondances recueillies dans le cadre des interceptions de sécurité, à l'exception près du point de départ du délai de conservation des correspondances qui court à compter de la date de leur première exploitation et non de leur recueil, différence notamment justifiée par les difficultés d'accès linguistiques aux contenus de ces correspondances.

Les conditions d'application de l'article L. 853-1 seront définies par un décret en Conseil d'Etat qui définira notamment les règles de conservation et de destruction des données collectées – hors données mettant en jeu des identifiants rattachables au territoire national, renvoyées au droit commun comme il a été dit - mais également les modalités de délivrance des autorisations d'exploitation des correspondances interceptées.

Les modalités de mise en œuvre des mesures de surveillance considérées seront en revanche décrites dans un décret qui ne sera, pour sa part, pas publié – sur le modèle des décrets régissant les certains fichiers de souveraineté. Leur divulgation dévoilerait en effet des informations de nature à porter gravement préjudice au secret de la défense nationale et à entraver les missions des services spécialisés de renseignement.

Ce décret non publié sera toutefois pris en Conseil d'Etat et après avis de la Commission nationale de contrôle des techniques de renseignement et porté à la connaissance de la Délégation parlementaire au renseignement aux fins que ces institutions puissent être à même d'assurer pleinement les missions et responsabilités de suivi et de contrôle qui leur sont dévolues.

La Commission nationale de contrôle des techniques de renseignement sera, pour sa part, plus particulièrement chargée de veiller à ce que lesdites mesures soient mises en œuvre par les services spécialisés intéressés conformément aux décisions du Premier Ministre. Elle fera, au

moins chaque semestre, rapport de son contrôle au Premier ministre qui sera alors tenu de répondre aux recommandations et observations qu'elle aura formulées.

2.2.5. La modification du régime de l'accès aux données de connexion (Livre VIII, titre III, chapitre Ier)

2.2.5.1. Etat du droit

Les articles L.246-1 à L. 246-5 du code de la sécurité intérieure régissent l'accès administratif aux données de connexion.

L'article L. 246-1 définit le champ d'application de la mesure : finalité, définition des données, source des données.

L'article L.246-2 précise la procédure d'autorisation : demande écrites et motivées des agents des services compétents auprès d'une personnalité qualifiée placée auprès du premier ministre, ou de ces adjoints, communication de la décision de la personnalité qualifiée à la commission nationale de contrôle des interceptions de sécurité.

L'article L. 246-3 instaure un régime particulier pour la géolocalisation en temps réel par sollicitation du réseau qui s'écarte de la procédure d'accès aux données de connexion et s'aligne sur celui plus exigeant des interceptions de sécurité : décision du Premier ministre sur sollicitation des ministres compétents, après consultation la CNCIS, cette dernière exerçant le même type de contrôle qu'en matière d'interceptions de sécurité.

2.2.5.2. Difficultés rencontrées

La législation mise en place n'a procédé qu'à une uniformisation imparfaite des régimes dont il est souhaité un renforcement.

Par ailleurs, bien que l'encadrement de la géolocalisation en temps réel constitue une avancée majeure, il présente un caractère incomplet et ne permet pas de prendre en compte la variété technique des méthodes utilisées pour répondre aux besoins des services en termes de localisation de personnes et des biens.

Enfin, le droit positif ne permet pas de recourir aux nouvelles technologies pour exploiter au mieux, en vue de la détection précoce de la menace terroriste et son identification, l'utilisation des réseaux de communication.

2.2.6. Objectif recherché

Les nouvelles dispositions visent à supprimer la procédure d'autorisation de demande d'accès à des données de connexion par les services auprès d'une personnalité qualifiée, pour harmoniser le régime d'autorisation.

Toutefois, pour tenir compte de la spécificité de ces demandes, tout à la fois moins attentatoires aux libertés individuelles et très ancrées dans l'urgence opérationnelle, la procédure proposée est assouplie : comme actuellement, une dérogation au régime de droit

commun permet que la demande soit faite non pas par le ministre compétent mais par les agents des services.

La localisation en temps réel d'une personne, d'un véhicule ou d'un objet est désormais encadrée à l'article L. 851-6 :

Les services spécialisés de renseignement auront ainsi la possibilité, pour les seuls besoins des missions autorisées par la loi, de recourir à la technique du « balisage », déjà prévue en matière judiciaire.

Ces dispositions visent à élargir les possibilités de géolocalisation simultanée, ou géolocalisation en temps réel. La géolocalisation consiste dans les faits, soit à surveiller en simultané les déplacements d'une personne ou d'un objet sur l'ensemble du territoire, soit de reconstituer *a posteriori* son itinéraire grâce aux données de connexion liées, notamment, à l'usage d'un téléphone connecté à un réseau GSM.

Dans ce second cas, les services de renseignement disposent déjà de moyens juridiques : il s'agit des dispositions du code de la sécurité intérieure (articles L 246-1 et suivants) qui régissent l'accès administratif aux données de connexion.

Les données de géolocalisation sont aujourd'hui une « matière première » essentielle aux enquêtes, dans un cadre administratif comme dans un cadre judiciaire. Ce sont elles, en effet, qui permettent d'établir la présence d'une personne (ou en tout cas d'un terminal de communication ou d'un objet « balisé ») dans un lieu donné ou, croisées avec les données relatives à d'autres personnes, d'établir des réseaux de relation ou des filières.

S'agissant plus particulièrement de la géolocalisation simultanée, elle apparaît comme un complément indispensable aux surveillances physiques. Celles-ci, en premier lieu, sont particulièrement consommatrices en effectifs : pour surveiller un seul individu de manière continue, une vingtaine d'agents sont nécessaires. Une telle mobilisation d'agents aguerris est difficilement tenable dans la durée, surtout dans le contexte actuel résultant de l'accroissement très rapide de la menace jihadiste.

Par ailleurs, la capacité de pénétration discrète de certains milieux ou zones géographiques qui se caractérisent par l'enclavement ou une forte identité peut être singulièrement limitée faute de pouvoir agir sans éveiller des interrogations ou des soupçons.

Enfin, et de plus en plus souvent, les cibles terroristes font preuve d'une grande vigilance et s'efforcent de déjouer toute surveillance physique directe. De même, un agent de renseignement étranger agissant sur le territoire français en recourant à une couverture, et qui bénéficie d'une grande liberté de déplacement, ne peut pas nécessairement faire l'objet d'une surveillance physique au regard des mesures de contre-filature mises en œuvre par la cible et du risque de révéler la connaissance de son activité par les services français.

A l'inverse, le balisage des véhicules (ou de tout autre objet, comme une valise par exemple) présente l'avantage de la discrétion. Il est en outre irremplaçable lorsque les personnes surveillées sont mobiles sur l'ensemble du territoire, à plus forte raison lorsqu'elles se rendent dans des lieux isolés en milieu rural où leur surveillance physique est difficile.

D'une manière générale, la géolocalisation simultanée rend possible un suivi dynamique de la

« cible » et permet de s'adapter en permanence, y compris en situation d'urgence : les services ont connaissance à tout moment de l'itinéraire suivi et, le cas échéant, des points d'arrêt qui peuvent permettre de déterminer les centres d'intérêts voire les objectifs de la cible.

En ce qui concerne la géolocalisation simultanée, deux modalités sont possibles :

- le suivi dynamique d'un terminal de télécommunication, déjà autorisé par le code de la sécurité intérieure ;
- l'utilisation d'une balise GSM ou GPS placée sur un objet ou un véhicule, ou à l'intérieur de celui-ci.

C'est cette dernière technique que l'article L 851-6 a pour objet d'autoriser aux services de renseignement et, dans certaines conditions, aux services de police et de gendarmerie.

Elle est soumise au régime de droit commun d'autorisation sur demande du ministre compétent auprès du Premier ministre après avis de la CNCTR, elle comporte des dispositions spéciales organisant une procédure d'urgence restreinte à l'existence d'une menace imminente ou d'un risque très élevé de ne pouvoir effectuer l'opération ultérieurement.

Dans ce cas, l'installation et l'exploitation du dispositif sont effectuées sans autorisation préalable, le Premier ministre et la Commission nationale de contrôle des techniques de renseignement en étant informés sans délai. Le Premier ministre peut ordonner la cessation immédiate de l'installation du dispositif, la cessation immédiate de l'exploitation des données ainsi que la destruction des données collectées. Il informe de sa décision la Commission nationale de contrôle des techniques de renseignement immédiatement et par tout moyen.

Par ailleurs, le projet de loi encadre de nouveaux modes d'exploitation des données de connexion et de réseau pour les besoins de prévention du terrorisme.

Les actes de terrorisme perpétrés en France au cours du mois de janvier 2015 témoignent de l'importance cruciale qui s'attache désormais au suivi le plus exhaustif possible des échanges que peuvent nouer sur le territoire national les activistes terroristes par la voie des communications électroniques. Seul un tel suivi est de nature à permettre la détection précoce des projets et menées à caractère terroriste et de renforcer ainsi l'efficacité de leur prévention.

La simple sollicitation *a posteriori*, auprès des opérateurs, de certaines données techniques de communication relatives à des personnes surveillées – ce que permet l'actuel L. 246-1 du code de la sécurité intérieure – n'est pas suffisante pour disposer d'une appréhension globale en temps réel.

C'est pourquoi, l'article L 851-3 autorise, pour les besoins de la détection précoce d'actes de terrorisme, la collecte, en temps réel, sur les réseaux des opérateurs, de la totalité des données, informations et documents relatifs aux communications de personnes préalablement identifiées comme des menaces. Contrairement à ce qu'il en est des personnes surveillées au titre des interceptions de sécurité, le contenu de leurs communications ne sera en aucun cas intercepté. Seules les données de connexions seront recueillies sur le fondement de ce nouvel article.

Par ailleurs, si elle nécessite un suivi exhaustif des activistes déjà identifiés et répertoriés, l'anticipation de la menace attachée aux activités terroristes, qui constitue un impératif majeur pour la sécurité nationale, rend également nécessaire la détection de personnes qui ne

l'avaient pas été précédemment et qui se trouvent engagés dans des entreprises radicales aux fins d'anticiper leur éventuel passage à l'acte sur le sol français ou européen et tout projet terroriste que ceux-ci nourriraient contre les ressortissants et intérêts français.

Afin d'identifier le plus en amont possible l'existence de ces menaces, les services de renseignement, confrontés à une multitude sans cesse croissante de réseaux, modes et supports de communications générant au plan planétaire des flux massifs de données, doivent pouvoir recueillir, traiter, analyser et recouper un grand nombre d'éléments techniques anonymes pour détecter les signaux de faible intensité qui témoignent d'une menace pesant sur les intérêts de notre pays.

Il convient de dépasser l'approche exclusivement fondée sur le suivi de cibles déjà connues ou repérées pour privilégier la recherche d'objectifs enfouis sous le maquis des réseaux de communications transnationaux, Internet offrant à cet égard des opportunités de furtivité immenses pour les acteurs et vecteurs de la menace.

Opérée grâce à la détection anonymisée de certains comportements de communication, cette détection sera prévue par le nouvel article L. 851-4 du code de la sécurité intérieure. La levée de l'anonymat pesant sur les données collectées, qui serait justifiée par la révélation de la réalité d'une menace, ferait l'objet de la procédure de droit commun d'autorisation par le Premier ministre après avis de la commission de contrôle.

Enfin, l'article L. 851-7 prévoit la possibilité de mettre en œuvre un dispositif technique de proximité

Pour faire face à une menace particulièrement importante au regard des intérêts publics mentionnés à l'article L. 811-3 du code de la sécurité intérieure, il est nécessaire de pouvoir accéder à certaines données, voire dans le cadre de la prévention du terrorisme, de procéder à des interceptions de sécurité, au moyen d'un dispositif technique exceptionnel et dans le cadre d'une procédure dérogatoire au régime général d'autorisation prévu à l'article L. 821-1 du code de la sécurité intérieure.

L'objectif est de permettre à certains services de renseignement de mettre en œuvre efficacement ce dispositif technique de proximité, pour des finalités limitées et dans un cadre permettant l'exercice d'un contrôle effectif.

Ce dispositif est une technique essentielle qui intervient en complément des surveillances physiques ou pour préparer des investigations techniques. Le capteur permet de recueillir les données techniques de connexion strictement nécessaires à l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur ou des données de géolocalisation d'un équipement terminal.

L'intérêt de cette technique est qu'elle permet d'identifier les moyens de communication de la cible. Une fois cette identification opérée, la personne pourra faire l'objet d'une réquisition administrative, dans les conditions prévues par la loi, afin que les services puissent obtenir son numéro de téléphone, l'historique des données de connexion ou, éventuellement, ces mêmes données « en temps réel » ; elle pourra également faire l'objet d'une interception de sécurité si nécessaire, selon la procédure de droit commun.

Dans un contexte où les cibles changent souvent de vecteur de télécommunication ou d'identifiant téléphonique pour brouiller les pistes, il est devenu nécessaire de recourir à cette technique pour connaître le numéro de téléphone à surveiller.

Ainsi, les personnes voulant échapper à la vigilance des services de renseignement (qu'il s'agisse de terrorisme, d'espionnage, de criminalité organisée ou encore d'ingérence économique) utilisent généralement plusieurs téléphones non identifiés, qui ont pu être acquis sous une fausse identité. Il peut aussi arriver, comme l'ont montré les récentes affaires de terrorisme, qu'elles utilisent les téléphones de leur entourage.

Par ailleurs, un dispositif mobile de proximité permet, dans des situations d'urgence extrême en matière de prévention du terrorisme, d'intercepter les contenus émis ou reçus par le téléphone de la cible. Cette possibilité technique est précieuse pour les services chargés de l'intervention.

L'utilisation d'un tel dispositif est encadrée par plusieurs garanties :

- Inscription du dispositif dans un registre spécial, tenu à la disposition de la Commission nationale de contrôle des techniques de renseignement.
- Mise en œuvre par un agent individuellement désigné et dûment habilité.
- Autorisation du Premier ministre, prise après avis de la Commission nationale de contrôle des techniques de renseignement, sans préjudice de l'article L. 821-5.
- Autorisation qui peut également porter sur un lieu ou une période déterminés, dans la limite de 6 mois. Dans ce cas, elle intervient après avis exprès de la Commission et doit être spécialement motivée.

Enfin, pour la prévention d'un acte de terrorisme, le dispositif technique mentionné au premier alinéa peut être utilisé, pour la durée strictement nécessaire, aux fins d'intercepter directement des correspondances émises ou reçues par un équipement terminal. Dans ce cas, l'autorisation ne peut être accordée que pour une durée de 72 h et selon la même procédure très encadrée que pour les lieux et périodes déterminés.

Enfin, pour tenir compte des contraintes opérationnelles, ce dispositif peut être utilisé sans autorisation préalable, en cas d'urgence liée à une menace imminente ou à un risque très élevé de ne pouvoir effectuer l'opération ultérieurement. Le Premier ministre et la CNCTR en sont informés sans délai et autorisent sa mise en œuvre sous 48h. Dans le cas contraire, il est mis fin au dispositif et les données collectées sont détruites.

Cette solution, très dérogatoire, permet de concilier souci d'opérationnalité et protection de la vie privée des personnes, dès lors que l'atteinte portée sans autorisation aucune, a vocation à s'étendre sur une durée très brève.

L'impact sur l'activité des opérateurs, notamment sur les infrastructures de réseaux, est difficile à évaluer, et dépendra assez largement des modalités de mise en œuvre technique par les services de l'Etat. Toutefois, il convient de souligner que de tels accès doivent être proportionnés aux finalités de la mise en œuvre du dispositif, et ne sauraient dès lors avoir un caractère massif.

2.2.7. L'obligation faite aux opérateurs de communications électroniques d'autoriser l'accès à leurs locaux (article L. 871-4)

2.2.7.1. Etat du droit

La conservation de données par les opérateurs de communications électroniques constitue des traitements de données à caractère personnel et fait, à ce titre, l'objet d'un contrôle possible par la commission nationale de l'informatique et des libertés au titre des ses pouvoirs généraux de contrôle a posteriori (article 44 de la loi du 6 janvier 1978) quel que soit la finalité du traitement (commerciale, conservation pour mise à disposition des autorités publiques).

Le contrôle de la CNCIS se limite aux procédures et traitements mis en œuvre par l'administration. L'article R. 246-8 du code de la sécurité intérieure prévoit ainsi que « la commission nationale de contrôle des interceptions de sécurité dispose d'un accès permanent aux traitements automatisés mentionnés aux articles R. 246-5, R. 246-6 et R. 246-7. L'autorité ayant approuvé une demande de recueil d'information ou de documents fournit à la commission tous éclaircissements que celle-ci sollicite sur cette demande ».

2.2.7.2. Difficultés rencontrées

La Commission nationale de contrôle des interceptions de sécurité dispose actuellement d'un accès direct au traitement mis en œuvre par les services de renseignement dans le cadre du recueil et de l'exploitation des données prévus au code de la sécurité intérieure, au même titre que la CNIL. Toutefois, la combinaison de ces deux procédures de contrôle reste insatisfaisante.

En effet, seule la CNIL dispose aujourd'hui d'un pouvoir de contrôle lors de la phase amont de la procédure chez les opérateurs, privant ainsi la CNCIS d'une partie de l'effectivité de son contrôle, lequel se limite également à l'accès aux traitements et non à l'environnement dans lequel ceux-ci sont mis en œuvre.

Par ailleurs, les contrôles de la CNIL visent à s'assurer de la conformité avec la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et non au respect des procédures telles que définies au code de la sécurité intérieure.

2.2.7.3. Objectif recherché

Cette disposition nouvelle vise à renforcer les pouvoirs d'investigation de la CNCTR, à l'instar d'autres autorités administratives indépendantes et, par conséquent, l'effectivité de ses contrôles.

Elle vise également à rationaliser les contrôles pour garantir le respect de la protection des libertés fondamentales des personnes dont les données sont recueillies, conservées et exploitées au profit des services de renseignement au regard de l'ensemble des règles régissant cette dérogation au secret des correspondances et ce tout au long de l'exécution de la mesure et quels qu'en soient les moyens.

2.2.7.4. Impacts attendus

- Renforcer l'étendue et l'effectivité du contrôle et la protection des libertés individuelles.

- Améliorer la visibilité de l'autorité de contrôle sur le dispositif d'accès aux données de connexion et de géolocalisation par les services de renseignement pour permettre la détection précoce d'éventuelles entorses aux procédures et y remédier le plus en amont possible.

2.2.8. Dispositions diverses (Livre VIII, titre VIII)

2.2.8.1. La protection de l'identité des agents (identité, dispense de publication d'actes administratifs, anonymisation de signature d'un acte administratif, restriction de la consultation d'un acte administratif par une juridiction nationale) (L. 891-1)

2.2.8.1.1. Etat du droit

A ce jour :

- tous les décrets sont soumis à une obligation de publication au JO en application de l'ordonnance n° 2004-164 du 20 février 2004. Ainsi, actuellement, les décrets d'organisation de la DGSE, DGSI, DRM etc. sont publiés au JO ;

- toutes les décisions individuelles de nomination, promotion de grade et mise à la retraite des fonctionnaires de l'Etat de catégorie A doivent être publiées au JO, en application du décret n° 63-280 du 19 mars 1963 pris en application de l'article 28 de la loi n° 84-16 du 11 janvier 1984 ;

- toutes les décisions individuelles de nomination, promotion de grade et mise à la retraite des fonctionnaires de l'Etat autres que de catégorie A doivent être publiées : au JO ou, à défaut, par d'autres moyens (BO, affichage, …), en application de l'article 28 de la loi n° 84-16 et du décret n° 63-280 ;

- les actes réglementaires autres que les décrets (dont les arrêtés délégation de signature) doivent être publiés, l'administration pouvant déterminer elle-même le mode de publicité approprié. A l'heure actuelle, des délégations de signature de la DGSI sont publiées au JO.

2.2.8.1.2. Difficultés rencontrées

La publication des mesures d'organisation d'une part, et des mesures nominatives d'autre part, constitue une source de vulnérabilité pour les services et leurs agents. Cette obligation, issue pour partie de principes jurisprudentiels, est en contradiction avec les dispositions issues du Livre blanc de 2008 et reprises par la LOPPSI du 14 mars 2011 à l'article 413-13 du code pénal et à l'article L. 2371-1 du code de la défense.

2.2.8.1.3. Objectif recherché

L'objectif est de supprimer ou de limiter l'obligation de publication des actes réglementaires et individuels relatifs aux services spécialisés de renseignement afin d'assurer l'effectivité de la protection qui doit s'attacher, au regard de leur mission, tant à l'identité des agents qu'à l'organisation de ces services.

2.2.8.1.4 Dispositions prévues

- L'alinéa 1 prévoit une dérogation aux dispositions de l'ordonnance 2004-164 précitée, s'agissant des décrets relatifs à l'organisation et au fonctionnement des services au JO (article 1)

- L'alinéa 2 prévoit une publication aménagée de ces actes et des actes individuels devant faire l'objet d'une publication, à un recueil spécial tenu par le SGDSN

- L'alinéa 3 prévoit une signature par numéro d'identification de leur auteur attribué avec la délégation de signature, se substituant aux mentions des prénoms, nom et qualité, exigées par l'article 4 de la loi DCRA du 12 avril 2000

- L'alinéa 4 prévoit une dérogation au CJA, de nature à permettre à l'administration de communiquer aux TA/CAA/CE des actes publiés dans son « *recueil spécial* » sans que cela soit communiqué à la partie adverse. Le détail d'une telle procédure relève du domaine réglementaire, et nécessite un décret (très probablement, en Conseil d'Etat. Cf. partie « *R* » du CJA). C'est l'objet de l'alinéa 5.

Ces dispositions permettent de déroger implicitement à la loi n° 84-16 et à son décret n° 63-280, en prévoyant que le mode normal de publication des décisions nominatives (y compris de catégorie A) est la publication au « *recueil spécial* » tout en garantissant leur opposabilité.

Un décret précise les conditions d'accès au recueil, les modalités de dérogation à la règle du contradictoire devant les juridictions.

2.2.8.1.5. Impacts attendus

L'aménagement des règles de publication des décisions nominatives devrait permettre de garantir la préservation de la confidentialité de l'organisation des services et l'anonymat des agents des services du renseignement, anonymat consubstantiel au fonctionnement de ces services et à la protection des fonctionnaires qui y travaillent.

Par ailleurs, l'instauration de règles spéciales (recueil spécial, numéro d'identification des agents…) permet de garantir un contrôle du juge quant à la régularité et à l'opposabilité des décisions.

2.2.9. L'exercice d'un droit de communication au profit de TRACFIN (article 8 modifiant l'article L. 561-26 du code monétaire et financier)

2.2.9.1. Etat du droit

TRACFIN est un service de renseignement rattaché aux ministères financiers. Il concourt au développement d'une économie saine en luttant contre les circuits financiers clandestins, le blanchiment d'argent et le financement du terrorisme. Ce service est chargé de recueillir, analyser et enrichir les déclarations de soupçons que les professionnels assujettis sont tenus, par la loi, de lui déclarer.

Afin de remplir sa mission de lutte contre le blanchiment et le financement du terrorisme, TRACFIN dispose de pouvoirs strictement encadrés par la loi et bénéficie notamment d'un droit de communication. En application de l'article L. 561-26 du code monétaire et financier et dans le but de reconstituer l'ensemble des transactions faites par une personne ou une société ayant fait l'objet d'un signalement, TRACFIN peut demander que les professionnels concernés par le dispositif anti blanchiment lui communiquent les pièces (relevés de comptes, factures, etc.) utiles à son enquête. Ces pièces sont transmises à TRACFIN quel que soit le support utilisé pour leur conservation. TRACFIN peut également fixer au professionnel un délai pour la transmission de ces éléments.

En ce qui concerne les organismes financiers, TRACFIN peut exercer cette prérogative en se rendant sur place selon les dispositions de l'article L.561-26 II du code monétaire et financier. TRACFIN ne peut exercer directement son droit de communication auprès des avocats ; la demande devant obligatoirement être transmise au bâtonnier de l'ordre auprès duquel l'avocat est inscrit.

Par ailleurs, en application de l'article L561-27 du code monétaire et financier, TRACFIN dispose également d'un droit de communication auprès des administrations d'État, des collectivités territoriales et des établissements publics ainsi que de toute personne chargée d'une mission de service public.

2.2.9.2. Difficultés rencontrées

Le droit de communication, tel qu'il est prévu à l'article L. 521-26 ne permet pas à TRACFIN de remplir pleinement sa mission de lutte contre le blanchiment.

2.2.9.3. Objectif recherché

Le III de l'article L. 521-26 devient le IV, et il est proposé d'ajouter un III à l'article L. 521-26 afin d'élargir l'étendue du droit de communication de TRACFIN en lui permettant d'exercer ce droit auprès des entreprises de transport terrestres, ferroviaires, maritimes et aériens ainsi qu'auprès des agents et opérateurs de voyage et de séjour, entités non soumises au dispositif de lutte contre le blanchiment d'argent et le financement du terrorisme.

Ce droit de communication porte sur tous éléments d'information relatifs à la nature de la prestation de voyage et s'il y a lieu aux bagages et marchandises transportés.

2.2.9.4. Impacts attendus

TRACFIN pourra ainsi obtenir des éléments d'information relatifs à la nature de la prestation de transport rendue (date, heure, lieu de départ et d'arrivée), des éléments d'identification des

personnes ayant payé ou bénéficié de celle-ci, de même que des éléments d'information relatifs aux bagages et marchandises éventuellement transportés.

L'exercice de ce droit permettra à TRACFIN d'enrichir ses analyses et ses enquêtes en établissant une corrélation précise et étayée entre des flux financiers et des déplacements de personnes ou de marchandises. En matière de lutte contre le terrorisme, les éléments recueillis pourront ainsi permettre l'approfondissement de la connaissance du fonctionnement des filières, la reconstitution précise des déplacements, voire leur anticipation.

Au-delà de la connaissance du déplacement lui-même, il peut s'avérer très utile de faire le lien entre le payeur et le (ou les) bénéficiaire(s) de la prestation de transport, d'apprécier le caractère préparé ou non du déplacement (en rapprochant la date du paiement d'une prestation à celle du voyage effectivement réalisé) ou d'avoir connaissance des bagages ou marchandises transportés au regard des problématiques liées au transport d'équipements spécifiques ou d'acheminement de marchandises prohibées.

En conséquence, les renseignements obtenus permettront à TRACFIN de consolider ses analyses et de transmettre le cas échéant, une note d'information à l'autorité judiciaire.

2.2.10. Excuse pénale pour les actions menées sur les systèmes d'information localisés hors du territoire national (article 9)

Dans le prolongement de l'excuse pénale créée par la loi de programmation militaire du 18 décembre 2013 pour les actions des agents de l'Etat répondant à une attaque informatique, il est nécessaire de protéger les agents qui mènent, notamment depuis le territoire national et donc directement passibles de la loi pénale française, des actions plus intrusives sur les systèmes d'information d'entités menaçant nos intérêts et localisés à l'étranger.

Tel est l'objet de l'article 9 du projet de loi.
Cette excuse pénale n'est évidemment pas absolue. Elle ne protège les agents des services que des poursuites qui pourraient être engagées sur le fondement des dispositions du code pénal créant des infractions spécifiques pour les cas d'intrusion ou atteinte à un système d'information. A contrario elle ne les protège pas d'autres qualifications pénales criminelles (cas d'une action informatique qui aurait des conséquences très importantes sur la population civile d'un pays) ou délictuelles (violences involontaires). Elle est donc parfaitement proportionnée aux missions assignées aux services pour la protection des intérêts de notre pays à l'étranger.

On notera que ce type d'excuse pénale existe déjà dans d'autres champs assez proches (voir ainsi l'article L. 4123-12 du code de la défense pour l'usage de la force et des mesures coercitives en opération par les militaires).

2.2.11. Dispositions relatives au renseignement en milieu pénitentiaire (article 12)

2.2.11.1. Diagnostic

2.2.11.1.1. Etat des lieux

Au 1er janvier 2015, 77 291 personnes étaient placées sous écrou (77 883 au 1er janvier 2014) dont 66 270 détenus (67 075 au 1er janvier 2014). Parmi ces détenus, 25% étaient des

prévenus (soit 16 549 personnes). En flux, sur l'ensemble de l'année 2013, on dénombre 89 290 placements sous écrou et 88 203 libérations.

Parmi ces personnes détenues, on compte 291 détenus particulièrement signalés, 314 personnes détenues pour des faits de terrorisme dont 179 au titre de l'islamisme radical.

Le service public pénitentiaire se doit d'assurer la sécurité, au sein de ses établissements, tant de ses personnels que de l'ensemble des personnes détenues. Pour ce faire, il doit veiller à ce que la réglementation et les procédures de sécurité soient correctement appliquées par tous.

Il doit aussi disposer des moyens suffisants pour remplir cette mission de service public en préservant le juste équilibre entre le caractère contraignant, voire intrusif des mesure de contrôle et la nécessité d'éviter toute réalisation des risques, nombreux dans l'environnent carcéral : évasion, racket, maintien de lien interdit avec l'extérieur, abus des personnes les plus vulnérables etc. Parmi les défis auxquels l'administration pénitentiaire est aujourd'hui confrontée, figurent l'utilisation de téléphones portables frauduleusement introduits au sein d'un établissement pénitentiaire et l'utilisation détournée des matériels informatiques mis à disposition ou détenus par la population pénale.

La téléphonie

La hausse des découvertes de téléphones portables (ou accessoires, puces, chargeurs etc..) est aujourd'hui incontestable. Ils représentent environ 50 % des objets illicites trouvés en détention : pas moins de 27 524 de ces objets ont pu être découverts en 2014, contre 20 532 en 2012 et seulement 10 990 en 2010.

Or l'administration pénitentiaire ne dispose pas de moyens juridiques pour intercepter les communications électroniques ou radioélectriques faites de manière illégale.

En effet, aux termes de l'article 39 de la loi n° 2009-1436 pénitentiaire du 24 novembre 2009, *« les personnes détenues ont le droit de téléphoner aux membres de leur famille. Elles peuvent être autorisées à téléphoner à d'autres personnes pour préparer leur réinsertion. Dans tous les cas, les prévenus doivent obtenir l'autorisation de l'autorité judiciaire.*

L'accès au téléphone peut être refusé, suspendu ou retiré, pour des motifs liés au maintien du bon ordre et de la sécurité ou à la prévention des infractions et, en ce qui concerne les prévenus, aux nécessités de l'information.

Le contrôle des communications téléphoniques est effectué conformément à l'article 727-1 du code de procédure pénale ».

L'article 727-1 du code de procédure pénale, introduit par la loi n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance, prévoit qu' *« aux fins de prévenir les évasions et d'assurer la sécurité et le bon ordre des établissements pénitentiaires ou des établissements de santé habilités à recevoir des détenus, les communications téléphoniques des personnes détenues peuvent, à l'exception de celles avec leur avocat, être écoutées, enregistrées et interrompues par l'administration pénitentiaire sous le contrôle du procureur de la République territorialement compétent, dans des conditions et selon des modalités qui sont précisées par décret.*

Les détenus ainsi que leurs correspondants sont informés du fait que les conversations téléphoniques peuvent être écoutées, enregistrées et interrompues.

Les enregistrements qui ne sont suivis d'aucune transmission à l'autorité judiciaire en application de l'article 40 ne peuvent être conservés au-delà d'un délai de trois mois ».

Le champ de l'article 727-1 est limité aux communications téléphoniques effectuées sur les postes téléphoniques mis à disposition par l'établissement.

L'article 27 du règlement intérieur type annexé à l'article R. 57-6-18 du code de procédure pénale précise ainsi que *« les communications téléphoniques sont réalisées au moyen des différents postes téléphoniques mis à disposition par l'établissement. L'utilisation ou la détention de téléphones portables ou de tout autre appareil communiquant est interdite ».*

Aucune disposition n'autorise donc l'identification des téléphones portables utilisés illégalement en détention.

Le Conseil d'Etat considère à cet égard que la possession d'un téléphone portable par un détenu, compte tenu de l'usage qui peut en être fait, notamment pour s'affranchir des règles particulières applicables, en vertu de l'article 727-1 du code de procédure pénale, aux communications téléphoniques des détenus et pour faire échec aux mesures de sécurité prises dans l'établissement pénitentiaire, doit être regardée comme la détention d'un objet dangereux (CE, 4 février 2013, n° 344266).

L'informatique

Plus de 2 500 ordinateurs sont par ailleurs actuellement présents légalement en détention. Si leur utilité est indiscutable et ne doit pas être remise en cause, les risques d'usage détourné sont également avérés de la part de certaines personnes détenues.

L'administration pénitentiaire doit en outre pouvoir disposer des informations utiles sur les profils de personnes qui lui sont confiées, dans leur propre intérêt et dans l'intérêt de l'ensemble de la population pénale qu'elle sera amenée à côtoyer.

Le présent projet de loi comporte ainsi plusieurs dispositions qui participent d'un meilleur contrôle et qui donnent à l'administration pénitentiaire la faculté d'interrompre l'utilisation de moyens de communication illicites par les personnes détenues.

L'article 12 du projet de loi permet à l'administration pénitentiaire de disposer des prérogatives nécessaires à la neutralisation des correspondances illicites émises ou reçues par la voie des communications électroniques ou radioélectriques par une personne détenue.

Cet article prévoit également que l'administration pénitentiaire peut s'assurer que l'usage des matériels informatiques autorisés en détention est conforme aux dispositions légales et réglementaires en vigueur, en vérifiant le contenu des disques durs des ordinateurs et en détectant les connections sur des réseaux non autorisés que les détenus peuvent être amenés à réaliser clandestinement.

Les vérifications des matériels informatiques des personnes détenues seront placées sous le contrôle du procureur de la République.

2.2.11.1.2. Cadre constitutionnel

Il appartient au législateur, en vertu de l'article 34 de la Constitution, de fixer les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques.

- Le droit au respect de la vie privée :

Le droit au respect de la vie privée est rattaché à l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789, aux termes duquel *« le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'Homme. Ces droits sont la liberté, la propriété, la sûreté, et la résistance à l'oppression »* (n° 99-416 DC, 23 juillet 1999, cons. 45).

Le Conseil constitutionnel considère qu' *« il appartient au législateur, en vertu de l'article 34 de la Constitution, de fixer les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ; qu'il doit, en particulier, assurer la conciliation entre le respect de la vie privée et d'autres exigences constitutionnelles, telles que la recherche des auteurs d'infractions et la prévention d'atteintes à l'ordre public, nécessaires, l'une et l'autre, à la sauvegarde de droits et principes de valeur constitutionnelle »* (n° 2010-604 DC, 25 février 2010, cons. 22).

Les restrictions qui peuvent être apportées à ce droit doivent être justifiées par un motif d'intérêt général et mises en œuvre de manière adéquate et proportionnée à cet objectif (n° 2012-652 DC, 22 mars 2012, cons. 8).

- Le droit au secret des correspondances :

Le Conseil constitutionnel rattache le droit au secret des correspondances aux articles 2 et 4 de la Déclaration des droits de l'homme et du citoyen de 1789 (n° 2004-492 DC, 2 mars 2004, cons. 4).

Il considère qu' *« il incombe au législateur d'assurer la conciliation entre, d'une part, la prévention des atteintes à l'ordre public et la recherche des auteurs d'infractions, toutes deux nécessaires à la sauvegarde de droits et de principes de valeur constitutionnelle, et, d'autre part, l'exercice des libertés constitutionnellement garanties. Au nombre de celles-ci figurent la liberté d'aller et venir, l'inviolabilité du domicile privé, le secret des correspondances et le respect de la vie privée »* (même décision).

- Les droits des personnes détenues :

S'agissant spécifiquement des personnes détenues, le Conseil constitutionnel considère qu' *« il appartient au législateur de fixer les règles concernant les garanties fondamentales accordées aux personnes détenues. Celles-ci bénéficient des droits et libertés constitutionnellement garantis dans les limites inhérentes à la détention. Il en résulte que le législateur doit assurer la conciliation entre, d'une part, l'exercice de ces droits et libertés que la Constitution garantit et, d'autre part, l'objectif de valeur constitutionnelle de sauvegarde de l'ordre public ainsi que les finalités qui sont assignées à l'exécution des peines privatives de liberté »* (n° 2014-393 QPC, 25 avril 2014, cons. 5)

Pour le Conseil constitutionnel, l'exécution des peines privatives de liberté en matière correctionnelle et criminelle a été conçue non seulement pour protéger la société et assurer la punition du condamné, mais aussi pour favoriser l'amendement de celui-ci et préparer son éventuelle réinsertion (même décision, cons. 4).

2.2.12.1.3. Cadre conventionnel

L'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales consacre le droit pour chacun au respect de la correspondance au titre de la protection, plus large, de la vie privée et familiale. Ce même article précise que l'autorité publique ne peut s'ingérer dans l'exercice de ce droit *« que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui »*.

Les conversations téléphoniques font partie de la « vie privée » et de la « correspondance » (CEDH, 2 août 1984, Malone c/ Royaume-Uni, § 64 ; 24 avril 1990, Kruslin et Huvig c/ France, 2 arrêts, §§ 25 et 26 ; 25 juin 1997, Halford c/ Royaume-Uni, § 48 ; 25 mars 1998, Kopp c/ Suisse, § 53 ; 24 août 1998, Lambert c/ France, § 21).

La CEDH applique sa jurisprudence à la surveillance de personnes détenues. Ainsi l'enregistrement des conversations téléphoniques d'une personne détenue constitue une ingérence dans l'exercice par celui-ci de ses droits garantis par l'article 8 (CEDH, 27 avril 2004, Doerga c/ Pays-Bas). Il en va de même pour l'enregistrement des conversations tenues dans les parloirs des prisons (CEDH, 20 décembre 2005, Wisse c/ France).

Dès lors, tant l'interception des conversations téléphoniques, que le contrôle des ordinateurs des personnes détenues, doivent être prévus par un texte.

2.2.11.1.4. Cadre législatif

La loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par voie de télécommunication, dont les dispositions figurent désormais aux articles L. 241-1 et suivants du code de la sécurité intérieure, impose que les atteintes portées au secret des correspondances soient prévues par la loi. Aux termes de l'article L. 241-1 du code de la sécurité intérieure en effet, *« le secret des correspondances émises par la voie des communications électroniques est garanti par la loi.*

Il ne peut être porté atteinte à ce secret que par l'autorité publique, dans les seuls cas de nécessité d'intérêt public prévus par la loi et dans les limites fixées par celle-ci ».

Eléments de droit comparé

Dans l'ensemble des pays étudiés, la possession d'un téléphone portable est prohibée en détention. Il est même question, en ce moment, dans certains pays tels l'Espagne, de renforcer les dispositifs de brouillage des télécommunications illicites, réalisées par les détenus, dans le cadre de leur incarcération.

Le plus souvent, l'utilisation des téléphones portables en détention constitue une infraction pénale ou bien une faute disciplinaire. En outre, le fait de transmettre à un détenu, dans le

cadre d'une visite en établissement carcéral, un téléphone portable, peut aussi constituer une infraction de nature pénale (**par exemple au Royaume-Uni**) ou bien administrative (**par exemple en Allemagne**).

Dans certains pays (**Italie, Portugal**), la réglementation permet aux détenus de communiquer assez régulièrement avec leur famille, **depuis un téléphone fixe** de l'établissement carcéral. La réglementation italienne établit même des différences de traitement selon les détenus, certains d'entre eux bénéficiant de droits plus restreints que d'autres, en raison de la nature de leur condamnation.

Seront examinés plus en détail, ci-dessous, les différentes réglementations de pays européens.

En Allemagne, la réglementation applicable dans les prisons est contenue, au niveau fédéral, dans un Code fédéral des prisons, et depuis 2006 au niveau des Länder, dans les différents codes des prisons. Un certain nombre de Länder ont **expressément interdit** dans leur code des prisons l'usage des téléphones portables, tandis que d'autres ne traitent pas de la question. Le fait de transmettre à un détenu un téléphone portable constitue une infraction administrative.

En Espagne, les téléphones portables sont interdits en détention. Il n'y a pas de débat à ce jour pour les autoriser. Il est même plutôt question d'installer **des inhibiteurs de téléphones** portables plus efficaces. A l'instar de la France, les téléphones portables sont, dans les faits, amplement présents en détention, malgré l'interdiction. Il y a eu d'ailleurs récemment un cas médiatisé d'un détenu qui twittait.

En Italie, la détention de téléphones portables en milieu carcéral n'est pas autorisée. La législation est très stricte en ce domaine. Les téléphones découverts dans les cellules sont saisis.
Toutefois, il existe une procédure pour les **appels téléphoniques**, qui est strictement encadrée par les textes (Art. 39 du règlement d'exécution DPR 30/06/2000 n°220). **Une fois par semaine**, les détenus peuvent téléphoner à leur famille, à l'exception des condamnés au titre de l'art. 4bis de l'Ordonnance pénitentiaire, qui n'ont droit qu'à deux appels par mois (association mafieuse, association aux fins de trafic de stupéfiants, séquestration,...) Des conversations supplémentaires sont possibles également avec des tiers, **en cas d'urgence** ou en cas de transfèrement. Les conversations sont à la charge du détenu avec des cartes de téléphones prépayées.
Pour pouvoir téléphoner, le détenu doit faire une demande afin d'obtenir l'autorisation du Directeur d'établissement (pour les condamnés), de l'autorité judiciaire (pour les détenus provisoires), du JAP (pour les personnes ayant fait un recours). Cette autorisation vaut jusqu'à révocation. C'est l'établissement qui met à disposition les moyens techniques pour permettre ces appels. Les appels sont de dix minutes maximum et doivent être faits sur un **numéro fixe** attribué nominativement à une personne autorisée à communiquer avec le détenu. Une facture devra être jointe à la demande, avec les justificatifs familiaux nécessaires. La circulaire du 26 avril 2010 de la Direction générale des détenus a introduit la **possibilité d'appeler des téléphones portables** pour les **détenus ordinaires** qui n'ont pas eu de parloirs ou d'appels pendant au moins 15 jours et qui ont déclaré que les contacts par mobile étaient le seul moyen de conserver des contacts avec leur famille.

Au Portugal, l'utilisation de portables à l'intérieur des prisons est interdite par le règlement général des établissements pénitentiaires (décret-loi 51/2011). En effet, l'article 211 du règlement exclut l'utilisation de tout autre moyen de communication avec l'extérieur, autre que la correspondance écrite et le **téléphone fixe**, et celui-ci dans les conditions strictes établies par l'article 209 (en règle générale, deux appels par semaine préalablement autorisés par le directeur de l'établissement, d'une durée non supérieure à dix minutes ; payés par le détenu).
Par ailleurs, l'établissement de toute communication avec l'extérieur non permise ou établie avec recours à des moyens frauduleux est une **faute disciplinaire grave** (article 104 du Code d'Exécution des Peines et Mesures Privatives de Liberté, loi 115/2009). La sanction disciplinaire applicable, est décidée en fonction de la nature et de la gravité de l'infraction, et choisie au sein d'une liste de mesures disciplinaires prévue à l'article 105 du CEP (réprimande écrite; privation d'usage et possession de biens personnels jusqu'à un délai maximum de 60 jours; interdiction de l'utilisation de rémunérations et recettes du travail jusqu'à un délai maximum de 60 jours; restriction d'activités socio-culturelles et d'occupation des temps libres; réduction du temps journalier passé en plein air; confinement en cellule jusqu'à un délai maximum de 30 jours; mise en cellule disciplinaire jusqu'à un délai maximum de 21 jours).

Au Royaume-Uni, le fait, pour un prisonnier, de posséder en détention un téléphone portable constitue une **faute disciplinaire** contraire aux règles pénitentiaires, en vertu du *Prison rule 51* (12). Il ne s'agit cependant pas d'une infraction pénale. Une procédure disciplinaire peut en conséquence être engagée à son encontre.
En vertu de la section 40C du prison Act de 1952, constitue une **infraction pénale**, le fait d'apporter, de transmettre, de lancer, ou de donner en connaissance de cause à un prisonnier, un article figurant à la liste B (« a mobile phone » est dans la liste B). Cette infraction est passible de 2 ans d'emprisonnement et/ou d'une amende.

En Roumanie, la possession et l'utilisation du téléphone portable sont prohibées et constituent **une infraction pénale**. Les détenus disposent du droit de téléphoner à des proches depuis un téléphone fixe de l'établissement carcéral, dans des conditions strictes établies par la loi carcérale n° 254 de 2013. Depuis 2008, 10.000 téléphones environ sont découverts chaque années par l'administration pénitentiaire, dont 1/5 avant qu'ils ne parviennent aux détenus. Au regard des risques de la poursuite de l'activité criminelle depuis les lieux de détention, des risques de pressions sur les témoins et victimes et des risques de concertation entre détenus pour la préparation d'actions dirigées contre l'administration pénitentiaire (arguments repris de l'exposé des motifs), le parlement a adopté le 10 décembre 2013 un **projet de loi** du Ministère de la Justice, qui prévoit l'installation de dispositifs de brouillage dans les établissements de détention. Ces dispositifs seront installés par l'Administration Pénitentiaire en relation avec l'Autorité administrative équivalent à l'ART française. Le directeur de l'Administration Pénitentiaire a annoncé leur entrée en service pour le début de l'année 2015.

PAYS	USAGE DU TELEPHONE	MODALITES D'UTILISATION	UTILISATION D'UN TELEPHONE PORTABLE	DIVERS
ALLEMAGNE	La réglementation est contenue dans le Code fédéral des prisons et dans les différents codes des Länder		Interdite en détention	
BELGIQUE	Tous les détenus peuvent téléphoner			
ESPAGNE	Tous les détenus peuvent téléphoner sauf s'il existe une interdiction de communiquer du juge		Interdite en détention	Pas de débat à ce jour sur la possibilité d'autorisation d'utilisation de téléphone portable en détention
ITALIE	Tous les détenus peuvent téléphoner	Utilisation d'un téléphone fixe dans des conditions strictes définies par le règlement : 1 appel hebdomadaire de 10 mn maximum sur un poste fixe, réglé par le détenu. Depuis 2010, il existe une possibilité d'appeler un téléphone portable pour les détenus	Interdite en détention	

		ordinaires qui n'ont pas eu de parloir ou d'appel pendant 15 jours (le téléphone mobile étant le seul moyen d'entrer en contact avec la famille)		
PAYS-BAS	Tous les détenus peuvent téléphoner sauf s'il existe une interdiction de communiquer du juge	Utilisation d'un téléphone fixe pour 10mn par semaine dans un lieu prévu à cet effet, réglée par le détenu sauf si le directeur en décide autrement	Utilisation Interdite en détention et susceptible d'une punition de 2 semaines	
PORTUGAL	Tous les détenus peuvent téléphoner	Utilisation d'un téléphone fixe dans des conditions strictes définies par le règlement : 2 appels hebdomadaires de 10mn maximum, réglés par le détenu	L'établissement de toute communication avec l'extérieur (autre que le courrier ou le téléphone fixe) est une faute disciplinaire grave : réprimande écrite, privation d'usage et de possession de biens personnels jusqu'à 60 jours, interdiction d'utilisation de rémunérations du travail, confinement, restriction du temps journalier en plein air, mise en cellule disciplinaire jusqu'à 21 jours ou en cellule de	

			confinement jusqu'à 30 jours…	
ROYAUME UNI	Tous les détenus peuvent téléphoner	Utilisation d'un téléphone fixe dans des conditions strictes définies par le règlement :	Utilisation Interdite en détention et susceptible d'une punition de 2 ans d'emprisonnement et .ou d'une amende	
ROUMANIE	Tous les détenus peuvent téléphoner	Utilisation d'un téléphone fixe dans des conditions strictes définies par le règlement	Utilisation Interdite en détention et susceptible d'une sanction pénale	Installation de dispositifs de brouillage qui devaient être mis en service début 2015 (depuis 2010, environ 10 000 téléphones portables sont découverts dans les prisons roumaines).

S'agissant de la possession ou de l'utilisation d'ordinateurs par les personnes détenues, la France ne se démarque pas de ses voisins européens :

Utilisation du matériel informatique en détention (2013)

	Modalités d'accès	**Propriétaire du matériel**	**Types de matériel**	**Réglementation**	**Divers**

Belgique	les ordinateurs sont localisés soit en cellule soit dans les salles de formation (e-Learning)	administration pénitentiaire qui les loue aux détenus ou les met à disposition (formation). La possibilité d'achat a été supprimée (trafic)	ordinateurs et /ou consoles de jeux (les 2 sont possibles en cellule) mais pas d'accès aux cyber bases de l'AP. Accès possible à internet dans le cadre d'e Learning + accès spécifique (ex : catalogue des bibliothèques publiques)	Pas de mention de l'utilisation des ordinateurs dans la loi de principe. L'accès est réglé par une circulaire ministérielle. Pas d'accès aux dernières consoles (qui permettent l'accès à internet)	Projet en cours : Cloud computing qui crée un accès spécifique pour le détenu pour accéder aux infos suivantes : cantine, accès aux dossiers judiciaires, commandes de films, etc. (système installé dans les prisons en construction et progressivement dans les autres)
Espagne	les ordinateurs sont à 2 endroits : localisés soit en cellule, soit dans les salles de formation	administration pénitentiaire ou détenus mais : les appareils doivent être achetés via les services de l'administration si le détenu est considéré comme dangereux, l'autorisation d'achat sera donnée par l'EMS espagnol	pour des raisons de sécurité, tous les matériels sont bloqués (pour accès internet). Pas d'accès au cyber base de l'AP	l'ensemble des règles est contenus dans un même document : instructions générales du secrétaire des institutions pénitentiaires (3/2010)	
Royaume-Uni	les ordinateurs sont localisés dans des espaces communs mais chaque directeur doit élaborer ses propres fonctionnements en fonction du profil des détenus : basic,		voire la description dans la circulaire jointe	l'ensemble des règles est contenu dans un document en cours de réactualisation PSI 49/2011. les « privilèges » (possibilités d'accéder à un ordinateur) sont déclinés selon l'évolution du	

	standard et renforcé (les nouvelles constructions prévoient l'accès au réseau informatique directement dans les cellules)			détenu	
Suède	sans accès à Internet, ils sont placés dans les espaces communs, avec accès ils sont dans les salles de formation en détention	administration pénitentiaire	les consoles de jeux peuvent être empruntées par les détenus et sont bloquées (pour accès internet). Pas d'accès au cyber base de l'AP	L'utilisation des ordinateurs est précisée dans la loi pénitentiaire dans la partie objet qu'un détenu peut posséder. Pas de site d'expérimentation internet. Les ordinateurs à disposition ne permettent pas l'accès à internet. Les consoles de jeux sont désactivées par l'AP. ils peuvent selon conditions avoir accès aux dernières générations de console	

2.2.11.2. Objectif

2.2.11.2.1. Nécessité de l'action

La téléphonie

La hausse des découvertes de téléphones portables (cf.supra) démontre d'une part que les deux modes principaux d'introduction frauduleuse que sont les parloirs et les projections sont insuffisamment endigués, d'autre part que les détecteurs (289 instruments mobiles déployés) et les brouilleurs (628 appareils installés) ne sont pas suffisamment efficaces ou dissuasifs pour éviter de la part de la population pénale la prise de risque de commission d'une

infraction (recel de l'infraction d'introduction d'objet prohibé en l'espèce un de téléphone portable).

Concernant l'introduction de téléphones portables, des mesures ont été déployées dans le cadre du plan sécurité au cours des années 2013 et 2014, qui a notamment permis l'achat de 282 portiques de détection de masses métalliques, de 393 magnétomètres et l'installation de filets anti-projections sur les 35 établissements pénitentiaires les plus impactés par ce phénomène. La découverte de téléphones portables a continué de croître pendant cette période, une hausse qui s'explique en partie par l'augmentation du nombre de portiques en sortie de parloirs et l'augmentation de la population pénale.

D'autres moyens doivent être développés pour lutter contre l'usage de moyens de communication illicites.

Depuis les programmes immobiliers 4000 et 13200, le cahier des charges prévoit que les établissements doivent être équipés de brouilleurs au minimum dans tous les quartiers d'isolement (QI) et quartiers de détention (QD) et dans chaque maison centrale (MC) et quartier de maison centrale (QMC). 628 dispositifs équipent aujourd'hui les établissements et ont vocation à être développés avec le plan de lutte anti-terroriste.

Il existe 7 types de brouilleurs aujourd'hui, dont aucun ne peut apporter totale satisfaction en milieu pénitentiaire pour des raisons techniques (la 4G, voire la 3G dans certains cas n'est pas brouillée), sanitaires (puissance d'émission limitée) ou environnementales (risque de brouiller le voisinage). En outre, ils ne doivent en aucun cas perturber le fonctionnement des équipements électroniques de l'établissement.

Une technologie plus perfectionnée est en cours de test sur deux établissements.

Au-delà de la question du brouillage, il parait nécessaire aujourd'hui de doter l'administration pénitentiaire de moyens modernes de recueil de données techniques de connexion et de données relatives à la localisation dans un objectif premier de sécurité de l'établissement puisque ces moyens permettront de mieux identifier les détenteurs de téléphone portable et d'interrompre leurs communications.

L'informatique

L'usage d'un outil informatique est régi par les dispositions de l'article 19 VII du règlement intérieur type annexé à l'article R. 57-6-18 du code de procédure pénale. Cet usage est strictement limité à des activités socioculturelles, d'enseignement, de formation ou professionnelles, sur un support informatique. Les données de l'ordinateur sont soumises au contrôle de l'administration et il n'est pas prévu d'accès à internet.

Une instruction générale détermine les caractéristiques auxquelles doivent répondre ces équipements, ainsi que les conditions de leur utilisation : c'est la circulaire relative à l'accès à l'informatique des personnes détenues du 17 juillet 2009. Elle interdit tous les éléments communicants (wifi, 3G) tout ce qui est graveur, clé USB, périphérique extérieur, logiciel de chiffrement, de numérisation etc…. Les entrées USB sont scellées.

La circulaire précitée précise ainsi que ces contrôles doivent être réalisés par les correspondants locaux des systèmes d'information (CLSI) et qu'il convient d'analyser la machine, recueillir, conserver et transmettre le cas échéant les informations à l'autorité judiciaire, mais sans altérer son système d'exploitation.

C'est dans ce but qu'a été créé un outil de fouille des ordinateurs, dénommé SCALPEL qui, depuis une clé USB ou un CD-ROM, permet d'analyser un système complet en n'effectuant aucune écriture sur le disque dur ; SCALPEL a été progressivement déployé dans les établissements pénitentiaires depuis fin 2007 : la dernière version mise à disposition des établissements est récente puisqu'elle date de mai 2014.

Certains parviennent cependant à dissimuler des traces d'utilisation de fichiers ou de connexion.

En outre, si les « fouilles informatiques » sont systématiques à chaque changement d'établissement, au départ ou à l'arrivée, la réglementation pénitentiaire n'impose qu'un contrôle annuel de l'ensemble des ordinateurs des personnes placées sous-main de justice. Cette disposition est pragmatique : elle correspond aux capacités et disponibilités actuelles des CLI déployés dans les établissements ou au sein des directions interrégionales.

Le scan effectué par SCALPEL est par ailleurs long (jusqu'à plusieurs heures) ; il aboutit à l'émission automatique d'un rapport, qui relève le cas échéant toutes les anomalies détectées (connexions illicites, fichiers et logiciels interdits…). Lorsqu'un poste fait l'objet d'une suspicion, son disque dur est retiré par l'administration, le temps d'une analyse approfondie.

Cette analyse débute tout d'abord par le recensement des fichiers puis vient leur analyse. S'il s'agit d'images par exemple, il faut les regarder les unes après les autres, de même pour les vidéos. Il est ainsi fréquent que cette investigation dure près d'une semaine pour un disque (mise en place du poste de fouille, analyse des fichiers présents, recherche de fichiers supprimés, etc...).

Cet outil ne pouvait donc être utilisé, au regard des moyens humains mis à disposition de l'administration pénitentiaire, de façon systématique et régulière, sur tous les ordinateurs octroyés aux personnes détenues, notamment en établissement pour peine (centre de détention et maisons centrales) où se trouve la plus grande partie de ces matériels. Cela implique donc de sélectionner les matériels qui seront contrôlés au regard des profils des personnes détenues qui les possèdent et au risque de ne pas contrôler l'ordinateur duquel il est fait un usage illicite.

Cependant, les recrutements d'informaticiens dans les directions interrégionales dans le cadre du plan de lutte anti-terroriste va permettre d'y procéder de manière plus régulière. Parallèlement, d'autres méthodes et solutions techniques doivent être mises en œuvre. Ainsi, il paraît souhaitable de permettre à l'administration pénitentiaire de procéder à une surveillance en temps réel sur les matériels informatiques laissés à disposition des personnes détenues pour empêcher une connexion illicite.

2.2.11.2.2. Objectifs poursuivis

Il n'est pas inutile de rappeler les chiffres des découvertes d'objets illicites et des actes de violences commis en détention.

On observe ainsi une augmentation sur les 5 dernières années de 56,96% du nombre de découvertes pour une augmentation non corrélative de 8,64% de la population pénale écrouée et hébergée durant la même période.

TOTAL	NOMBRE DE DECOUVERTES								*Evolution des découvertes %*	Population écrouée et hébergée au 01-01-N+1	Evolution de la population écrouée et hébergée %
	TELEPHONES ET ACCESSOIRES	STUPEFIANTS	ARMES	EXPLOSIFS	ARGENT	ALCOOL	AUTRES	PROJECTION EXTERIEURE			
56 149	27 524	9 895	1 017	1	1 479	847	8 545	6 841	*12,23%*	66 270	-1,21%
49 280	23 495	8 998	766	2	1 293	760	7 809	6 157	*17,42%*	67 075	0,75%
40 693	20 532	8 755	705	0	1 234	930	7 296	1 241	*20,21%*	66 572	2,68%
32 468	16 487	7 795	705	0	872	850	5 759		*25,56%*	64 787	6,55%
24 168	10 990	6 661	512	0	706	523	4 776			60 544	

S'agissant des violences, on observe une évolution sur les 5 dernières années de 21,64% du nombre de violences physiques sur le personnel et de 2,92% des violences entre personnes détenues.

	Violences sur le personnel		Violences entre personnes détenues	Population écrouée et hébergée au 01-01-N+1	Evolution de la population écrouée et hébergée %
	Physiques	verbales			
2014	4 122	15 559	8 060	66 270	-1,21%
2013	4 192	15 880	8 560	67 075	0,75%
2012	4 403	16 878	8 861	66 572	2,68%
2011	4 083	15 829	8 365	64 787	6,55%
2010	3 230	14 349	7 825	60 544	

L'usage non contrôlé de téléphones interdits contribue à fragiliser la sécurité des établissements en permettant la préparation de tentatives d'évasion, d'intrusion, d'entrées de produits interdits contre lesquels il faut lutter et génère un trafic source de tensions.

La nécessité d'une loi

Il résulte du cadre normatif ci-dessus exposé qu'une base légale est nécessaire pour permettre une interception des communications électroniques ou radioélectriques et un contrôle des ordinateurs.

Il résulte en outre très clairement du cadre constitutionnel et législatif que seule la loi peut autoriser l'interception des communications électroniques ou radioélectriques passées illégalement.

S'agissant du matériel informatique, une loi apparaît également nécessaire eu égard à l'ingérence dans la vie privée des personnes détenues que constitue le dispositif prévu par le projet de loi. Leur matériel informatique pourra en effet être contrôlé à tout moment et leurs données pourront être enregistrées. . Conformément à l'article 24 de la loi n° 2000-321 du 12 avril 2000, seule une loi peut écarter par principe l'intervention d'une procédure contradictoire préalablement à l'intervention d'une mesure de police.

L'intervention du législateur renforce en outre la protection des droits des personnes détenues en prévoyant l'information du Procureur de la République. Elle sécurise enfin l'ensemble du dispositif au regard d'éventuelles contestations contentieuses.

2.2.12.3. Options

2.2.12.3.1. Mesure 1 : Téléphonie

Option 1 (écartée)

Si certains l'appellent de leurs vœux, la libéralisation de l'usage de la téléphonie en détention n'est pas envisageable compte tenu des motifs même qui président à son contrôle actuel et déjà développés plus haut.

Il doit en effet être rappelé que l'absence de contrôle des communications peut mettre non seulement en péril la sécurité des établissements pénitentiaires (préparatifs de projets d'évasion) mais, et les hypothèses sont plus fréquentes, permettre la poursuite d'activités délictueuses ou criminelles (organisation ou gestion de trafics de stupéfiants, de réseaux de proxénétisme,…) ou d'interférer dans l'instruction des affaires judiciaires (par des pressions sur les victimes, les témoins,…).

Cette évolution pourrait permettre de réduire le nombre de téléphones illicites en détention. Leur présence illicite ne serait cependant pas éradiquée dès lors qu'une intention criminelle ou délictuelle animera certaines personnes détenues qui ne voudront pas que leur communication soit entendue.

Cette option est donc écartée.

Option 2 (retenue)

Confirmation législative du droit de brouillage, d'interruption et consécration de la possibilité pour l'administration pénitentiaire de capter les données de connexion d'un appareil téléphonique frauduleusement utilisé par une personne détenue.

Cet accroissement des moyens de neutraliser ces matériels participe de la lutte aussi bien contre les trafics internes (sollicitations d'introduction d'objet par parloirs ou projection) que contre les violences (vol, rackets, notamment vis à vis des plus vulnérables et de leur famille à l'extérieure).

Il doit en outre être rappelé que les évolutions technologiques rendent parfois inopérants les moyens de contrôle classiques que sont les portiques de détection – quels qu'ils soient – et les fouilles intégrales. Ainsi, les téléphones portables miniatures, au format de clés de voiture, ne comportant aucun composant métallique sont introduits facilement en détention.

Un des moyens techniques disponible est appelé « dispositifs techniques de proximité » dont la commercialisation est strictement encadrée par l'article 226-3 du code pénal.

Le mode opératoire idéal d'une action de dispositif technique de proximité pourrait se dérouler en début de service de nuit, lorsque les personnes sont en cellule, entre 20H00 et 23H00, période propice aux appels illicites des personnes détenues et créneau le plus souvent utilisé par eux.

La sensibilité de l'appareil permet une interception entre 250 mètres et 1 mètre. Il doit être réglé à chaque utilisation en fonction de l'antenne-relais à proximité de manière à ne pas capter hors de la zone sélectionnée des téléphones qui n'ont pas vocation à être détectés (passants à côté de la prison, magistrat autorisé à se déplacer en détention avec un téléphone, surveillant, avocat ou intervenant, récupérant son téléphone dans un casier). Ce réglage est d'autant plus précis qu'il est réalisé sur une courte distance. Ce dispositif n'est, à ce stade, pas d'une utilisation aisée et doit être utilisé avec beaucoup de précaution et de parcimonie

Pour l'établissement, le recensement du nombre de téléphones portables sur une zone peut permettre d'accentuer ou non des fouilles de cellule en fonction des résultats obtenus.

Ces mesures continueront à être complétées par les opérations de police judiciaire régulièrement organisées à l'entrée des établissements par la gendarmerie ou la police nationale, sur réquisitions du ministère public et dont l'efficacité et le caractère dissuasif sont également unanimement reconnus.

Les données techniques de connexion ainsi collectées pourront être communiquées au Procureur de la République ainsi que, dans le cadre d'un partenariat protocolisé, aux services de renseignement ou de police.

2.2.12.3.1. Mesure 2 : Informatique

Option 1 (écartée) :

Interdire la détention de tout ordinateur ou à l'inverse, libéraliser leur usage et autoriser l'accès à l'informatique

Il serait simpliste de prétendre éradiquer toute possibilité d'usage détourné d'un ordinateur par l'interdiction globale de toute détention d'un tel appareil par une personne détenue.

De même est-il déraisonnable de penser que les ordinateurs, propriété privée des personnes détenues pour certains, puissent être considérées comme inviolables et exclus de tout contrôle portant atteinte à l'intimité.

Une libéralisation de l'accès à internet comporte également des risques excessifs, dont la responsabilité pèserait sur l'administration pénitentiaire en cas de commission d'une infraction notamment.

Pour autant, l'administration pénitentiaire entend accompagner l'évolution des comportements et des attentes sociales et expérimente actuellement des cyber-base dans certains établissements, mais sur la base d'un accès très contrôlé à internet. Elle permet aux personnes détenues de consulter certains sites internet dans un espace dédié et dans le respect des règles de sécurité pénitentiaires et informatiques. Tout échange d'information entre une personne détenue et l'extérieur doit être, a priori, contrôlé par l'administration pénitentiaire.

Option 2 (écartée) :

Limiter le contrôle approfondi des ordinateurs à un cadre judiciaire ou par des services spécialisés de renseignement.

La nature du contrôle que l'administration se doit d'opérer sur les ordinateurs n'est pas liée à l'existence d'une raison plausible de soupçonner qu'une infraction a été commise, ni à l'existence d'une information laissant penser que la sûreté de l'Etat est notamment enjeu : il s'agit plus prosaïquement d'assurer la sécurité des établissements pénitentiaires et de s'assurer que l'usage des appareils contribue à la réinsertion de la personne détenue, préventivement à toute suspicion.

Les cadres judiciaires ou de renseignement spécialisé administratif ne concourent pas aux mêmes objectifs.

En outre, l'administration pénitentiaire ne fait pas partie des services spécialisés de renseignement. En toute logique, elle ne bénéficie pas des mêmes prérogatives ou cadre d'action.

Pour autant, les services spécialisés de renseignement disposeront, en vertu de la présente loi, des mêmes prérogatives au sein des établissements pénitentiaires qu'à l'extérieur.

Option 3 (retenue) :

Permettre un contrôle par l'administration pénitentiaire, préventif, par tout moyen utile, des ordinateurs.

Comme il a été dit, les moyens pénitentiaires actuels de contrôle informatique permettent de détecter les utilisations qui ont été faites de l'ordinateur. Cependant, certaines techniques avancées de cryptage peuvent permettre d'échapper à cette détection. Seuls des logiciels intégrés aux ordinateurs des publics cible permettraient de les tracer. Ces logiciels de détection pourront être utilisés pour détecter les connexions frauduleuses à Internet à partir d'ordinateurs autorisés.

Les mesures préventives qui seront mises œuvre le seront en toute transparence : la population pénale est avisée individuellement de la possibilité de mise en œuvre de ces techniques par un document signé et classé au dossier.

2.2.12.4. Impacts

2.2.12.4.1. Impacts juridiques

L'article 12 du projet de loi ajoute deux articles au code de procédure pénale.

Il créé un article 727-2 qui , en prévoie la possibilité de brouillage ou d'interruption des correspondances émises ou reçues par la voie des communications électroniques ou radioélectriques de manière illégale. Il permet également de recueillir, au moyen d'un dispositif technique de proximité, les données techniques de connexion des équipements terminaux. Cette possibilité s'ajoute aux interceptions des communications téléphoniques réalisées à partir des postes téléphoniques, prévues à l'article 727-1 du code de procédure pénale.

Il crée un article 727-3permettant à l'administration pénitentiaire d'accéder aux données contenues dans les équipements informatiques ou matériels assimilés utilisés par les personnes détenues sont régulièrement détenus et utilisés utilisés et de s'assurer qu'aucune connexion interdite n'est réalisée.

2.2.12.4.2. Impacts sur les services judiciaires

L'impact sur les magistrats du parquet dépendra des modalités de contrôle par le procureur qui seront fixées par décret.

2.2.12.4.3. Impacts sur les finances publiques

Le renforcement du contrôle de l'administration pénitentiaire sur les communications téléphoniques et les équipements informatiques et plus généralement le développement du renseignement pénitentiaire nécessitent des moyens techniques nouveaux mais également un renforcement des moyens humains destinés à traiter ces informations.

Le plan du gouvernement de lutte contre le terrorisme prévoit la création de 483 emplois et 80 M€ de crédits hors dépenses de personnel sur la période 2015-2017 pour l'administration pénitentiaire.

154 emplois supplémentaires et 10,5 M€ de crédits hors personnel sont plus particulièrement destinés au renforcement du renseignement pénitentiaire.

S'agissant du contrôle des communications téléphoniques :

- Le recours aux dispositifs technique de proximité permet une détection efficace des téléphones portables. Le coût d'un équipement est d'environ 375.000 €. 4,5 M€ sont prévus sur 2015-2017 pour le financement de 12 dispositifs.

- Les dispositifs de brouillage des communications de nouvelle génération ont un coût unitaire d'environ 180 K€. 10 établissements sont équipés ou en cours d'équipement. 3 M€ sont prévus sur le triennal 2015-2017 pour équiper la totalité des 26 établissements susceptibles d'accueillir des détenus radicalisés de dispositifs de brouillage de nouvelle génération.

S'agissant du contrôle des équipements informatiques

- Le renforcement du contrôle des équipements informatiques nécessite de disposer d'informaticiens pour développer des outils de contrôle et procéder aux fouilles. Dans le cadre du plan de lutte contre le terrorisme, 22 informaticiens supplémentaires seront recrutés sur 2015-2016 pour les services déconcentrés (fouilles des matériels) et centraux (conception et développement des outils de contrôle et de requêtes).

S'agissant plus généralement du développement du renseignement pénitentiaire

- Des moyens sont nécessaires afin d'accroître les capacités de renseignement dans les établissements sensibles et au niveau interrégional:

    - Au-delà des 22 emplois d'informaticiens mentionnés précédemment, 42 emplois seront créés dans les délégations interrégionales du renseignement pénitentiaire (DIRP) avec un effort particulier sur Paris, Lyon, Marseille et Lille (14 officiers de renseignement, 14 analystes-veilleurs pour la surveillance des réseaux sociaux, 14 conseillers d'insertion et de probation pour les personnes suivies en milieu ouvert)

    - 44 officiers de renseignement à plein temps seront recrutés en 2015-2016, au profit des maisons centrales, de certains établissements de plus de 600 places et certains établissements parisiens

    - Des moyens immobiliers doivent accompagner ces créations de poste. 3 M€ sont prévus à ce titre par le plan de lutte contre le terrorisme sur 2015-2017.

- Le renforcement du renseignement pénitentiaire implique également des moyens de pilotage par l'administration centrale. Le plan de lutte contre le terrorisme prévoit donc 6 créations d'emplois à ce titre, notamment pour la coordination de la mise en œuvre de ce plan, la veille sur les réseaux sociaux et les questions informatiques et l'appui technique pour les outils informatiques de renseignement et de sécurité (CAR, SCALPEL).

2.2.12.4.3. Impacts sur l'aide juridictionnelle

Néant

2.2.12.4.4. Impacts sur les collectivités territoriales

Il n'y a pas d'impact sur les collectivités territoriales.

2.2.12.4.5. Impacts sur les entreprises

Aucun

2.2.12.4.6. Impacts sur l'égalité entre les femmes et les hommes

Néant

2.2.12.4.7. Impacts sur les personnes handicapées

Néant

2.2.11.5. Consultations et modalités d'application

2.2.12.5.1. Consultations

Consultations obligatoires

Néant

Consultations facultatives

Aucune consultation facultative n'a été réalisée.

Une information aux organisations syndicales est toutefois prévue ultérieurement, compte tenu des attentes fortes en matière de renforcement des moyens de sécurité des organisations syndicales et des réponses que ces mesures permettent d'apporter.

2.2.12.5.2. Application de la loi dans le temps et dans l'espace

La loi est d'application immédiate.

La population pénale déjà incarcérée à la date de son entrée en vigueur sera également avisée, par tout moyen, de l'existence de ces nouvelles dispositions.

Les textes réglementaires suivants devront être pris sur le fondement de la loi :

La mise en œuvre du principe de surveillance des communications radioélectriques ou électroniques de certains détenus devrait en toute logique impliquer la mise en œuvre d'un traitement automatisé après publication de la loi. Ce traitement automatisé devrait en toute logique faire l'objet d'une déclaration CNIL et, s'agissant d'un traitement qui pourrait comporter des données personnelles sensibles (religion pratiquée…) sur les détenus et sur les personnes avec lesquelles ils entrent en relation, un décret en Conseil d'Etat après avis CNIL pourrait apparaître nécessaire.

La loi s'applique sur l'ensemble du territoire national.

Partie 3– Liste des consultations et des textes d'application

Les autorités suivantes ont été consultées :

- L'Autorité de régulation des communications électroniques et des postes (ARCEP)
- La Commission nationale informatique et libertés (CNIL)
- La Commission consultative du secret de la défense nationale (CCSDN)
- La Commission nationale de contrôle des interceptions de sécurité (CNCIS)

Tableau des textes d'application

Article du projet de loi	Type de texte	Objet du texte réglementaire
Article 1er	Décret en Conseil d'Etat	Il détermine les conditions dans lesquelles l'autorisation de mise en œuvre des techniques de recueil de renseignement peut être délivrée au bénéfice des services qu'il désigne autres que les services spécialisés de renseignement.

Article 1er	Décret en Conseil d'Etat	Ce décret détermine, dans la limite de douze mois, ou pour les données de connexion, de cinq ans à compter de leur recueil, la durée avant que ces renseignements collectés dans le cadre d'une technique de renseignement autorisée en application du livre VIII de la partie législative du code de la sécurité intérieure, ne soient détruits.
Article 1er	Décret en Conseil d'Etat	Il définit les conditions d'exploitation, de conservation et de destruction des renseignements collectés et précise la procédure de délivrance des autorisations d'exploitation des correspondances.
Article 3	Décret en Conseil d'Etat	Fixe la liste des agents individuellement désignés et dûment habilités appartenant à un service mentionné aux articles L. 811-2 et L. 811-4 pouvant effectuer les opérations mentionnées au 1° et 2° de l'article L. 853-1 du code de la sécurité intérieure.
Article 3r	Décret en Conseil d'Etat (non publié)	Il précise en tant que de besoin les modalités de mise en œuvre de la surveillance prévue à l'article L. 853-1 du code de la sécurité intérieure.
Article 11	Décret en Conseil d'Etat	Il fixe la liste des traitements ou parties de traitements intéressant la sûreté de l'Etat prévue à l'article 41 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
Article 12	Décret	Il fixe les conditions et modalités dans lesquelles l'administration pénitentiaire peut, sous le contrôle du procureur de la République, accéder aux données informatiques contenues dans les systèmes de traitement

		automatisé de données que possèdent les personnes détenues et détecter toute connexion à un réseau non autorisé