Note numéro 13
septembre 2015

Note du CREOGN

Centre de Recherche de l'Ecole des Officiers de la Gendarmerie Nationale

Comprendre la loi sur le renseignement

Pourquoi une loi sur le renseignement ?

La France demeurait une des rares démocraties à ne pas disposer d'une loi encadrant l'action des services de renseignement. Cette « clandestinité », protégée par la théorie des « actes de gouvernement » créait une grande insécurité juridique, dans la mesure où le risque de condamnation de notre pays par la Cour Européenne des Droits de l'Homme (CEDH) était élevé. Par ailleurs, à titre individuel, les agents des services agissaient parfois, sur le territoire national comme à l'étranger, sans autorisation de la loi et risquaient ainsi de voir leur responsabilité pénale engagée.
La légitimité du renseignement exige une loi précise, pour ne pas encourir le grief d'incompétence négative, prévisible dans ses conséquences, accessible à tous, et qui, par ses finalités et les moyens mis en œuvre, réponde à un besoin social impérieux, à une nécessité d'intérêt public, et respecte le principe de proportionnalité. C'est ce que rappelle la loi, dès son premier article (Art. 801-1 du Code de sécurité intérieure).

Sans doute entaché par quelques scandales passés, le renseignement a été longtemps un sujet tabou. Par touches successives, le législateur a élaboré un corpus juridique portant sur les interceptions de sécurité (loi n°91-646 du 10 juillet 1991, relative au secret des correspondances émises par la voie des communications électroniques) puis l'accès aux données de connexion dans un cadre administratif (article 6 de la loi « anti-terroriste » du 23 janvier 2006 puis article 20 de la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire). La loi du 9 octobre 2007 a créé la Délégation parlementaire au renseignement en vue de légitimer la fonction « renseignement » par un contrôle parlementaire *a posteriori*. Il manquait un texte définissant les missions de services, encadrant leur activité, notamment lors de la mise en œuvre de techniques pouvant être très intrusives au regard de la vie privée et organisant un contrôle de ces mesures, par une autorité administrative indépendante et par une juridiction garante des libertés.
Tout au long du débat parlementaire, en particulier au Sénat, le législateur et le gouvernement ont apporté des précisions, dans l'oralité des débats, comme dans les amendements, afin d'éviter l'inconstitutionnalité du texte.

Les lignes de force de la loi

1/ Un seul texte, inséré dans le nouveau livre VIIII du Code de la sécurité intérieure, fixe des principes et une procédure communs à toutes les techniques de recueil du renseignement (accès aux données de connexion, interceptions de sécurité, sonorisation, captation d'images et de données, etc.) utilisées sur le territoire national (les dispositions relatives à l'étranger ont été déclarées contraires à la Constitution). L'emploi de certains appareils ou dispositifs techniques (IMSI catchers, balises, algorithmes) est très strictement encadré ;

2/ La loi réaffirme le principe de respect de la vie privée (Art. 801-CSI) qui porte notamment sur le secret des correspondances, la protection des données personnelles et l'inviolabilité du domicile ;
3/ Le renseignement est une politique publique dont l'objet est de concourir à la stratégie de sécurité nationale et à la défense et à la promotion des intérêts fondamentaux de la Nation. Elle ne peut être mise en œuvre que par l'État ;
4/ Les agents relevant des services de renseignement bénéficient de la protection de la loi. Un statut de « lanceur d'alerte » est créé à leur profit ;
5/ Les données recueillies font l'objet d'un encadrement strict ;
6/ Une autorité administrative indépendante, la Commission Nationale de Contrôle des Techniques de Renseignement (CNCTR) intervient a priori, sauf cas d'urgence, et dispose de pouvoirs de contrôle très étendus ;
7/ Le Conseil d'État veille au respect du principe de légalité. Il peut être saisi par toute personne qui souhaite vérifier qu'aucune technique de renseignement n'est illégalement prise à son égard et par la CNCTR.

Les services concernés par la loi

La loi concerne tout d'abord le « premier cercle » des services spécialisés dans le renseignement(Art. L.811-2 du CSI). Mais la loi s'applique aussi à un « deuxième cercle » (Art. L811-4 du CSI), constitué des services autres que les services de renseignement et reconnus comme tels par un décret en Conseil d'État. Les services de renseignement du premier et du deuxième cercle peuvent échanger entre eux toutes les informations utiles à l'accomplissement de leurs missions (Art. L.863-2).

Les services de renseignement ont pour missions, en France et à l'étranger**,** la recherche, la collecte, l'exploitation et la mise à disposition du gouvernement des renseignements relatifs aux enjeux géopolitiques et stratégiques ainsi qu'aux menaces et aux risques susceptibles d'affecter la vie de la Nation. Ils contribuent à la connaissance et à l'anticipation de ces enjeux ainsi qu'à la prévention et à l'entrave de ces risques et menaces. Les services ne sont pas mentionnés par la loi, car leur organisation relève du pouvoir réglementaire. Ils sont énumérés à l'article D. 1128 du code de la défense : 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). Avec le Coordonnateur national du renseignement et l'Académie du renseignement, ces services forment ce que l'on appelle la « communauté du renseignement ».

D'autres services relèvent d'un « deuxième cercle ». Sans être consacré par la loi, ce vocable a été fréquemment employé lors des débats au Parlement. Parmi les services relevant de l'article L.811-4, le ministre de l'Intérieur a mentionné notamment certains services de la DGPN, de la Préfecture de police et de la Direction Générale de la Gendarmerie Nationale. Ces services (cf. ancien article R264-2 du CSI) étaient déjà autorisés à demander des interceptions de sécurité ou à accéder aux données de connexion (pour la gendarmerie : SDPJ, SDAO, Pôle PJ, sections de recherches). On peut imaginer que le décret en Conseil d'Etat, appliquant l'article L.811-4 CSI, ne réduira pas les compétences actuellement reconnues. Mais le texte de loi indique que les techniques et les finalités seront précisées pour chaque service en fonction de leur nature et de leurs missions.
L'administration pénitentiaire ne figure pas dans le « deuxième cercle », malgré la volonté des députés. Le Gouvernement et le Sénat n'ont pas voulu créer un mélange des genres, sans pour

autant contester la nécessité d'organiser la collecte du renseignement au sein des établissements pénitentiaires (un service « central » de renseignement pénitentiaire, bureau rattaché à la sous-direction de l'état-major de sécurité, s'appuie sur un réseau d'officiers de renseignement structuré au niveau des neuf Directions Interrégionales Pénitentiaires (DIRP),de la mission des services pénitentiaires de l'outre-mer et des établissements pénitentiaires). Il appartient à l'administration pénitentiaire de renforcer ses moyens et ses liens avec les services, seuls habilités à mettre en œuvre des techniques d'enquête.

L'article L.863-2 autorise les services de renseignement à échanger toutes informations utiles à l'accomplissement de leurs missions, qu'ils appartiennent au premier ou au deuxième cercle. Cet article n'est pas anodin, car il fait écho au rapport de Jean-Pierre Sueur sur les mouvements jihadistes[1], dans lequel celui-ci constatait à propos de certain service spécialisé, « *une certaine tendance à « aspirer » l'ensemble des renseignements produits par les autres services sans que ceux-ci ne soient informés de la suite donnée aux signalements ou aux informations ainsi transmis. […]Les services émetteurs ne peuvent pas évaluer la qualité ou l'utilité des éléments qu'ils transmettent, ce qui leur permettrait pourtant d'améliorer leurs pratiques de manière permanente. Cette absence de retour a aussi parfois un effet démobilisateur pour leurs personnels*[2] ».

Les techniques de renseignement mises en œuvre par les services

Les services de renseignement et les services du « deuxième cercle » peuvent, selon leurs missions et les finalités poursuivies, mettre en œuvre des techniques de renseignement :

- *les interceptions de sécurité (Art. L. 852-1 CSI) ;*
- *l'accès administratif aux données de connexion (Art. L. 851-1 et s. CSI) ;*
- *la géolocalisation en temps réel des terminaux mobiles (Art. L. 851-4 CSI) ;*
- *la géolocalisation en temps réel par « balise » d'une personne, d'un véhicule ou d'un objet (Art. L.851-5 CSI) ;*
- *le suivi en temps réel sur les réseaux de personnes préalablement identifiées comme présentant un risque particulier en matière de terrorisme (Art L. 851-2 CSI) ;*
- *la détection d'une menace terroriste grâce à l'analyse, par un « algorithme », des communications échangées au sein des réseaux des opérateurs (Art. L. 851-3 CSI) ;*
- *les captation, fixation, transmission et enregistrement de paroles prononcées à titre privé ou confidentiel ou d'image de personne se trouvant dans un lieu privé (Art. L.853-1 I CSI);*
- *l'accès, l'enregistrement, la conservation et la transmission de données informatiques stockées dans un système de traitement automatisé de données (Art. L.853-2 I 1° CSI) ;*
- *la captation de données, telles qu'elles s'affichent sur un écran, telles qu'elles y sont introduites par saisie, ou telles qu'elles sont reçues ou émises par des périphériques audiovisuels (Art. L853-2 I 2°CSI) ;*
- *le déploiement d'antennes relais mobiles, ou IMSI catchers, se substituant aux antennes relais fixes des opérateurs (Art. L.851-6 CSI ; Art. L.852-1 II CSI) ;*
- *les recherches sous pseudonyme (« cyberpatrouilles » administratives) (Art. L.863-1* **CSI).**

1Rapport n°388 (2014-2015), Jean-Pierre Sueur, *Filières jihadistes, pour une réponse globale sans faiblesse*, P.88

2
Cité dans le Rapport de Pierre Bas au nom de la Commission des lois du Sénat, n°460 2014-2015, p. 102.

Le droit de faire usage d'une identité d'emprunt ou fausse qualité est prévu par l'article L.861-2 du CSI pour les agents des services spécialisés (Art. L.811-2 CSI) et ceux des autres services (Art. L811-4 CSI). Il s'agit plus d'une modalité d'action que d'une technique de renseignement.

Sauf cas particulier (urgence absolue, cyberpatrouilles) ces techniques font toutes l'objet d'une autorisation préalable de mise en œuvre par le Premier ministre, après avis de la CNCTR.

Certaines techniques existaient déjà avant la loi :
- les interceptions de sécurité étaient régies par la loi du 10 juillet 1991 relative au secret des correspondances émises par les voies de télécommunications. Elles se sont progressivement adaptées au développement des nouvelles technologies de communication, encore embryonnaires au début des années quatre-vingt-dix.
Elles sont reprises par la loi sur le renseignement (Art. L. 852-1 nouveau du CSI) et peuvent être étendues aux personnes appartenant à l'entourage s'il existe « des raisons sérieuses de croire que l'une ou plusieurs d'entre elles sont susceptibles de fournir des informations au titre de la finalité qui motive l'autorisation ». Une autorisation est nécessaire pour chacune de ces personnes ;
- l'accès administratif aux données de connexion (Art. L. 851-1 à L.857 nouveaux du CSI) était l'acte préparatoire aux interceptions de sécurité avant que loi du 23 janvier 2006, relative à la lutte contre le terrorisme, lui donne son « autonomie ». Introduite aux fins de prévenir le terrorisme, initialement réservée aux services spécialement habilités de la police et de la gendarmerie, cette technique à été étendue à tous les services de renseignement par l'article 20 de la loi de programmation militaire du 18 décembre 2013 ;
- la géolocalisation en temps réel des terminaux mobiles sur sollicitation des réseaux (Art. L.851-4 nouveau du CSI) a également été légalisée par la loi de programmation militaire.

D'autres techniques sont désormais autorisées par la loi sur le renseignement.

Une première technique de renseignement vient compléter le dispositif de géolocalisation en temps réel prévu par la loi de programmation militaire et qui ne portait que sur des appareils mobiles. L'article L. 851-5 nouveau du CSI autorise la pose de « balises » GSM ou GPS pour géolocaliser en temps réel une personne, un véhicule, un objet.

Deux techniques ne peuvent être mises en œuvre qu'aux seules fins de la prévention du terrorisme :
- le suivi en temps réel sur les réseaux des opérateurs de téléphonie et fournisseurs d'accès à internet de personnes préalablement identifiées comme présentant un risque particulier en matière de terrorisme (Art L. 851-2 du CSI). Chaque personne doit faire l'objet d'un examen individuel. Seules les données de connexion peuvent être recueillies, les contenus relevant de la procédure d'interception de sécurité ;
- la détection d'une menace terroriste, grâce à l'analyse par un « algorithme », des communications échangées au sein du réseau d'un opérateur téléphonique ou d'un fournisseur d'accès (Art. L. 851-3 du CSI). Il s'agit de déceler des comportements à partir des métadonnées sans procéder à l'identification de leur auteur. Les données recueillies sont celles, et seulement celles, qui correspondent aux paramètres de conception de l'algorithme. En cas de menace avérée, une deuxième phase s'ouvre alors. Après avis de la CNCTR, le Premier ministre peut autoriser la levée de l'anonymat. Cette technique est sans doute celle qui est la plus contestée par les opposants à la loi. Elle est « expérimentale », la loi l'autorisant jusqu'au 31 décembre 2018. Un rapport sur son application devra être remis au Parlement avant le 30 juin 2018.
Trois techniques ne peuvent être mises en œuvre qu'à titre de subsidiarité, lorsque les

renseignements ne peuvent être recueillis par un autre moyen légalement autorisé :
- les captation, fixation, transmission et enregistrement de paroles prononcées à titre privé ou confidentiel ou d'image de personne se trouvant dans un lieu privé (Art. L.853-1 I du CSI);
- l'accès, l'enregistrement, la conservation et la transmission de données informatiques stockées dans un système de traitement automatisé de données (Art. L.853-2 I 1° du CSI). Cet accès est considéré comme particulièrement intrusif et assimilé à une introduction domiciliaire quant à la durée d'autorisation ;
- la captation de données, telles qu'elles s'affichent sur un écran, telles qu'elles y sont introduites par saisie, ou telles qu'elles sont reçues ou émises par des périphériques audiovisuels (Art. L853-2 I 2° du CSI). Cette mesure a notamment pour intérêt d'accéder aux contenus avant leur cryptage.

La loi autorise dans des conditions très strictes le déploiement de dispositifs techniques de proximité, tels que les *IMSI*[3] *catchers*. Ces appareils sont des antennes-relais de téléphone qui sont déployés afin de leurrer les téléphones mobiles qui émettent autour dans un rayon de quelques centaines de mètres. Ils ne peuvent être utilisés que pour le seul recueil des données de connexion (Art. L. 851-6 CSI) permettant d'identifier un terminal (IMEI[4]), du numéro d'abonnement de son détenteur (IMSI) et de la localisation de l'appareil (l'Assemblée nationale voulait que ces appareils puissent livrer toutes les données de connexion, dont le carnet d'adresse, les numéros des appels émis et reçus, etc., mais le Gouvernement et le Sénat s'y sont opposés) ;
Pour des finalités limitées à l'indépendance nationale, l'intégrité du territoire, la défense nationale, la prévention du terrorisme et la prévention des atteintes à la forme républicaine des institutions, les *IMSI catchers* peuvent aussi être déployés pour des interceptions de sécurité, pour une durée de quarante-huit heures renouvelable (Art. L852-1-II CSI). Le nombre maximal de dispositifs pouvant être utilisés simultanément est arrêté par le Premier ministre. Ces dispositifs sont inscrits dans un registre spécial. Le Groupe Interministériel de Contrôle (GIC) centralise les informations et documents recueillis et les résultats des interceptions.

L'accès à un véhicule ou un lieu privé est strictement réglementé (Art. L. 853-3 CSI). Pour la pose de balises (Art. L.851-5 CSI), la sonorisation ou la captation d'images (Art. L.853-1 CSI), l'accès aux données informatiques et la captation sur écran (Art. L. 853-2 CSI), il ne peut être opéré que par des agents individuellement désignés et habilités des services désignés aux articles L.811-2 et L.811-4 du CSI. L'accès à un lieu d'habitation doit faire l'objet d'un avis exprès de la CNCTR statuant en formation plénière ou restreinte. L'autorisation du Premier ministre doit être spécialement motivée. S'il prend une décision contraire à l'avis de la CNCTR, la section spécialisée du Conseil d'État est immédiatement saisie et statue dans un délai de vingt-quatre heures pendant lequel la mesure ne peut être exécutée. Le législateur a ainsi renforcé les garanties respectant l'équilibre entre le principe constitutionnel d'inviolabilité du domicile et la prévention des infractions particulièrement graves.

On notera que s'établit une forme de parallélisme avec les investigations judiciaires opérées par les OPJ, sous le contrôle du juge judiciaire, dans le cadre des enquêtes.

3 -International Mobile Subscriber Indentity (identité internationale du souscripteur mobile stocké dans la carte SIM)
4 -International Mobile Equipment Identity (numéro d'identité internationale de l'équipement mobile)

Technique d'enquête/renseignement	Police judiciaire	Police administrative
Interception des correspondances émises par la voie des télécommunications	**Art. 100 à 100-7 du Code de procédure pénale** **Infractions relevant de la criminalité organisée (art 706-73 du code de procédure pénale)** **Infractions pour lesquelles la peine encourue est égale ou supérieure à deux ans d'emprisonnement** **Juge des libertés et de la détention saisi par le procureur de la République dans le cadre d'une enquête préliminaire ou de flagrance (un mois, renouvelable une seule fois)** **Juge d'instruction dans le cadre d'une information (quatre mois, renouvelable dans les mêmes conditions de forme)**	**Art. L.852-1 du Code de la sécurité intérieure** **Pour une finalité prévue par l'article 811-3 du Code de la sécurité intérieure**
Perquisition et saisie informatique	**Art 57-1, 76-3, 97-1 du Code de procédure pénale** **Procureur de la République ou juge d'instruction**	**Art. L.853-2 du Code de la sécurité intérieure** **Lorsque les renseignements ne peuvent être recueillis par un autre moyen légal** **Pour une finalité prévue par l'article 811-3 du Code de la sécurité intérieure**
Réquisition de données informatiques	**Art 60-2, 77-1-2, 99-4 du Code de procédure pénale** **Procureur de la République ou juge d'instruction**	**Art. L.851-1 à L.851-7 du Code de la sécurité intérieure** **Pour une finalité prévue par l'article 811-3 du Code de la sécurité intérieure** **Sauf :** **Art. L.851-2 : recueil en temps réel** **Art. L.851-3 : détection par algorithme** **Pour la seule finalité de la prévention du terrorisme**
Déchiffrage des données cryptées	**Art 230-1 à 230-5 du Code de procédure pénale**	**Art. L 871-1 du Code de la sécurité intérieure**
Cyberinfiltration	**Article 706-2-2 du Code de procédure pénale.** **Certaines infractions prévues du code de la santé publique et du code de la consommation.** **Art 706-35-1 du Code de procédure pénale.** **Infractions prévues aux articles 225-4-1 à 225-4-9 (*traite des êtres humains*), 225-5 à 225-12**	**Art. L.863-1 du Code de la sécurité intérieure** **Pour une finalité prévue par l'article 811-3 du Code de la sécurité intérieure**

	(*proxénétisme*) et 225-12-1 à 225-12-4 (*prostitution de mineurs ou de personnes vulnérables*) du Code pénal **Art. 706-47-3 du Code de procédure pénale** **Infractions prévues aux articles 227-18 à 227-24 du code pénal** **Art. 706-87-1 du Code de procédure pénale** **Infractions relevant de la criminalité organisée (art 706-73 du Code de procédure pénale)**	
Sonorisation et captation des données informatiques	**Art. 706-102-1 à 706-102-9 du Code de procédure pénale** **Infractions relevant de la criminalité organisée (art 706-73 du Code de procédure pénale)**	**Art. L.853-1 du Code de la sécurité intérieure** **Lorsque les renseignements ne peuvent être recueillis par un autre moyen légal** **Pour une finalité prévue par l'article 811-3 du Code de la sécurité intérieure** **Art. L853-3 : conditions particulières pour un accès à un domicile, à un véhicule ou à un lieu privé**
Géolocalisation en temps réel d'une personne, d'un véhicule ou d'un objet	**Article 230-32 à 230-44 du Code de procédure pénale** **Délit prévu au livre II (*atteintes aux personnes*) ou aux articles 434-6 et 434-27 du Code pénal, puni d'un emprisonnement d'au moins trois ans** **Enquête ou d'une instruction relative à un crime ou à un délit, à l'exception de ceux mentionnés au 1° du présent article, puni d'un emprisonnement d'au moins cinq ans ;** **Procédure d'enquête ou d'instruction de recherche des causes de la mort ou de la disparition prévue aux articles 74, 74-1 et 80-4 du Code de procédure pénale** **Procédure de recherche d'une personne en fuite prévue à l'article 74-2. du Code de procédure pénale**	**Art. L.851-4 et L.851-5 (balise) du Code de la sécurité intérieure** **Pour une finalité prévue par l'article 811-3 du Code de la sécurité intérieure**

Les techniques de renseignement soumises à un formalisme précis

Les techniques de renseignement sont, dans leur mise en œuvre, soumises au principe de légalité. C'est le respect de ce principe qui constitue l'ordre de la loi sans lequel les actes accomplis relèveraient de la loi pénale. Les techniques de renseignement :

1/ procèdent d'une autorisation du Premier ministre ou de collaborateurs directs ayant légalement compétence pour le faire (article L. 821-4) ;
2/ respectent une procédure minutieusement décrite au titre II du livre VIII et faisant intervenir a priori une autorité administrative indépendante ;
3/ sont compatibles avec les missions confiées aux services chargés de missions de renseignement ;
4/ sont justifiées par les menaces, risques et enjeux ;
5/ répondent à des finalités limitativement définies ;
6/ font l'objet de contraintes d'autant plus strictes qu'elles portent davantage atteinte au respect de la vie privée. Les lieux privés ou d'habitation font l'objet d'une protection renforcée ;
7/ sont placées sous le contrôle juridictionnel du Conseil d'État.

Sont particulièrement protégées certaines personnes en raison de leur profession ou mandat (parlementaire, magistrat, avocat, journaliste). Elles ne peuvent se voir appliquer les mesures prévues au titre de l'urgence absolue (Art. L. 821-7 CSI). Si l'une de ces personnes est visée par une demande, la CNCTR doit l'examiner en formation plénière. Celle-ci a connaissance de tous les renseignements collectés, afin d'exercer un contrôle de proportionnalité. La procédure d'urgence prévue à l'article L. 821-5 CSI n'est pas applicable aux professions protégées.

Les finalités des techniques de renseignement

Conformément aux dispositions de l'article 8, alinéa 2, de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, l'intrusion dans la vie privée par des techniques de renseignement doit respecter des finalités précises.
La loi (article L. 811-3 du Code de sécurité intérieure) se réfère à la défense et à la promotion des intérêts fondamentaux de la Nation ainsi énumérés :

1° L'indépendance nationale, l'intégrité du territoire et la défense nationale ;
2° Les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère ;
3° Les intérêts économiques, industriels et scientifiques majeurs de la France ;
4° La prévention du terrorisme ;
5° La prévention :
a) des atteintes à la forme républicaine des institutions ;
b) des actions tendant au maintien ou à la reconstitution de groupements dissous ;
c) des violences collectives de nature à porter gravement atteinte à la paix publique ;
6° La prévention de la criminalité et de la délinquance organisées ;
7° La prévention de la prolifération des armes de destruction massive.

Soucieux d'un contrôle de constitutionnalité annoncé, le législateur a délibérément choisi de qualifier ces finalités par référence à la Constitution ou au Code pénal. Ainsi, l'indépendance nationale, l'intégrité du territoire, la défense nationale, notions inscrites aux articles 5, 15, 20 ou 21 ont été préférées à celle de sécurité nationale, pourtant définie par l'article L. 1111-1 du code de la défense. Le respect des engagements de la France est également une exigence constitutionnelle (art 5 et 52). Les items se rapprochent aussi, sans être toujours identiques, de la définition des intérêts fondamentaux de la Nation, telle qu'elle est énoncée par l'article 410-1 du Code pénal.

TABLEAU COMPARATIF ENTRE LE CODE PÉNAL ET LA LOI SUR LE RENSEIGNEMENT

Art. 410-1 Code pénal	Loi renseignement
Indépendance	Indépendance nationale
Intégrité du territoire	Intégrité du territoire
Sécurité du territoire	
Forme républicaine des institutions	Atteintes à la forme républicaine des institutions
Moyens de la défense	Défense nationale
Moyens de la diplomatie	Intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère
Sauvegarde de la population en France et à l'étranger	
Eléments essentiels du potentiel scientifique et économique	Intérêts économiques, industriels et scientifiques majeurs de la France
Eléments essentiels du patrimoine culturel	
Equilibre du milieu naturel et de l'environnement	
	Prévention du terrorisme
	Actions tendant au maintien ou à la reconstitution de groupements dissous
	Violences collectives de nature à porter gravement atteinte à la paix publique
	Prévention de la criminalité et de la délinquance organisées
	Prévention de la prolifération des armes de destruction massive

L'inventaire des finalités est plus large que celui qui servait jusqu'alors de référence aux interceptions de sécurité et à l'accès administratif aux données de connexion. L'article L.241-2 du CSI ne visait que la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, la prévention du terrorisme, de la criminalité et de la délinquance organisée et la reconstitution ou le maintien de groupements dissous.
Lors des débats parlementaires, des craintes se sont exprimées s'agissant de la prévention des violences collectives de nature à porter gravement atteinte à la paix publique. Il a été précisé que cette finalité vise les violences liées aux agissements de groupes dangereux et subversifs et qu'il n'est pas question de remettre en cause le droit de manifester ou de placer sous surveillance les partis politiques, les syndicats et les mouvements sociaux. Les atteintes à la paix publique ont une définition juridique dans le Code pénal (art 431-1 à 432-21). L'adjectif « gravement » élève le seuil d'intervention des services.

Les finalités peuvent être différenciées selon les missions des services. Une technique d'enquête peut viser plusieurs finalités.

Un statut protecteur pour les agents des services

Tout en rappelant que les agents des services spécialisés sont pénalement responsables de leurs actes (Art. L.862-2 CSI), la loi sur le renseignement contient plusieurs dispositions assurant leur protection juridique.

Leur anonymat doit être préservé, notamment dans les actes réglementaires ou individuels les concernant.

L'article L. 861-3 CSI crée une procédure de « lanceur d'alerte » leur permettant de porter à la connaissance de la CNCTR les violations manifestes relatives à la mise en œuvre des techniques d'enquête.

La loi crée l'article 323-8 du Code pénal selon lequel n'est pas pénalement responsable des infractions commises sur des systèmes de traitement automatisés de données prévues par les articles 323-1 à 323-7 du Code pénal (loi Godfrain) l'agent des services spécialisés de renseignements qui, notamment dans le cadre de la cyberdéfense, agit hors du territoire national pour assurer la protection des intérêts fondamentaux de la Nation énumérés à l'article 811-3 du CSI.

Par analogie avec la procédure en vigueur pour les militaires, les faits, commis hors du territoire national, par un agent des services spécialisés de renseignement (Art. L.812-2 CSI) et susceptibles de constituer une infraction pénale, font l'objet d'une demande d'avis du ministre préalablement à tout acte de poursuite. La loi permet aussi au garde des Sceaux, de ne pas donner suite à une demande d'entraide pénale internationale pour des faits commis hors frontières par des agents des services de renseignement, dès lors que cette mesure serait de nature à porter atteinte aux intérêts fondamentaux de la Nation.

L'article 323-8 du Code pénal ne concerne que les agents des services spécialisés du « premier cercle ». L'institution d'une irresponsabilité pénale montre bien que le législateur inscrit les actions offensives dans le cyberespace dans le cadre juridique du droit commun. Cette protection est d'autant plus nécessaire que l'application du droit des conflits armés est très peu probable, compte tenu des difficultés qui s'attachent à l'attribution des cyberattaques et à la mise en œuvre de la légitime défense. Si l'emploi du « cyber dans la guerre » est désormais courant, la « cyberguerre » est une hypothèse peu probable, d'où l'importance d'une protection juridique en « temps de paix ».

<u>Un recueil et une conservation des données sous contrôle</u>

Selon l'article L.822-2-I, les données sont conservées pendant un délai qui varie en fonction de l'atteinte portée à la vie privée. Ce délai commence au moment de leur recueil et non de leur exploitation, à l'exception des documents cryptés (le délai commence dans ce cas au moment de leur déchiffrement sans pour autant excéder 6 ans). Les entreprises fournissant des prestations de cryptologie sont tenues de fournir aux services les conventions de déchiffrement dans un délai de soixante-douze heures (Art. L.871-1 CSI).
Les données issues des interceptions de sécurité (Art. L.851-1 CSI) et les paroles captées (Art. L.853-1 CSI) peuvent être conservées trente jours. Les autres renseignements sont conservés cent vingt jours, à l'exception des données de connexion qui bénéficient d'un délai de quatre ans. Passé le délai légal, les données doivent être détruites (sauf si une procédure les concernant est engagée devant le Conseil d'État), par des agents individuellement désignés et habilités, sous contrôle de la CNCTR (Art. L.822-4 CSI).
Pour les seuls besoins de l'analyse technique, les renseignements collectés qui « contiennent des éléments de cyberattaque » ou qui sont chiffrés et les renseignements déchiffrés qui leur sont associés peuvent être conservés au-delà des délais fixés au L.822-2-I.
Les renseignements collectés font l'objet d'une traçabilité et d'une centralisation (Art. L.822-1 CSI) au sein d'un service relevant du Premier ministre (GIC).

L'article L.851-1 du CSI reprend les dispositions de l'article L.246-1 et L.246-2 du même Code qui précisent les documents et informations qui peuvent être sollicités au titre de l'accès aux données de connexion :

- données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée ;
- données relatives à la localisation des équipements terminaux utilisés ;
- données techniques relatives aux communications d'un abonné portant sur la liste d'appel des numéros appelés et appelants, la durée et la date des communications.

Le terme « cyberattaque » n'est pas défini en droit français qui ne connaît que les atteintes aux systèmes de traitement automatisé de données (Art. 323-1 à 323-8 du Code pénal). Le législateur a fait le choix délibéré de ce terme un peu vague pour couvrir toutes les hypothèses. Cette dérogation à la durée de conservation, qui exclut toute utilisation pour la surveillance des personnes, permet des actions au titre de la cyberdéfense, notamment en disposant d'une base documentaire et de références techniques des attaques.

Une autorité administrative indépendante au cœur de la procédure

La Commission Nationale de Contrôle des Techniques de Renseignement est une autorité administrative qui, sauf cas particuliers, donne un avis préalable à toute autorisation délivrée par le Premier ministre pour l'usage sur le territoire national des techniques de renseignement. À chaque étape de la procédure, elle a un droit d'accès permanent, complet et direct à l'information recueillie ainsi qu'aux locaux où sont centralisés les renseignements (Art. L. 833-2 CSI) et à ceux dans lesquels sont mises en œuvre des techniques de recueil du renseignement (Art. L. 871-4 CSI).
Elle a un pouvoir de recommandation pouvant conduire à l'interruption de la mise en œuvre d'une technique et à la destruction des données recueillies.
Elle est composée de 9 membres (2 députés - 2 sénateurs - 2 membres du Conseil d'État - 2 membres de la Cour de Cassation – 1 personne qualifiée en matière de communications électroniques). Son président, nommé par le Président de la République, est un des membres du Conseil d'État ou de la Cour de cassation. Elle se réunit en séance plénière ou en séance restreinte (sans les parlementaires).
Le président ou trois de ses membres peuvent saisir le Conseil d'État en cas de litige. L'urgence absolue (Art. L.821-5) et l'accès administratif aux données de connexion (Art. L.821-1) suivent des procédures dérogatoires.

La demande écrite et motivée (Art. L.821-2) émane d'un ministre (ministre de la Défense, de l'Intérieur, ministre en charge de l'économie, du budget ou des douanes). Elle est communiquée au président de la CNCTR qui rend un avis dans les 24 heures (72 heures si l'avis est donné en commission plénière ou restreinte). Le Premier ministre intervient alors dans la procédure d'autorisation. S'il passe outre l'avis de la CNCTR, le Conseil d'État peut être saisi.
Cette procédure connaît quelques inflexions :

- En cas d'urgence absolue (Art. L.821-5), le Premier ministre peut accorder l'autorisation sans avis préalable de la CNCTR. Mais il ne peut le faire que si sont en cause l'indépendance nationale, l'intégrité du territoire et la défense nationale, la prévention du terrorisme et la prévention des atteintes à la forme républicaine des institutions. Les parlementaires, magistrats, avocats et journalistes ne peuvent être concernés par cette dérogation. La CNCTR est informée dans les 24 heures.
- Les demandes d'accès administratif aux données de connexion sont directement adressées par les services à la CNCTR et non par l'intermédiaire d'un ministre.

Le Premier ministre autorité de police administrative spéciale

Le Premier ministre donne l'autorisation de mise en œuvre des techniques de renseignement (Art. L. 821-4 CSI). Il est en charge d'une police administrative spéciale qui est de la compétence de l'exécutif, ce qui explique que la CNCTR ne formule qu'un avis et ne puisse avoir un pouvoir de décision et que le Conseil d'État soit juge de la légalité des décisions.
La durée de l'autorisation respecte le principe de proportionnalité : elle est d'autant plus courte que la technique d'enquête est intrusive :
-trente jours pour une technique mise en œuvre dans un véhicule ou un lieu privé (Art. L.853-3 III CSI) ou un accès aux données informatiques (Art. L. 853-2 I 1°CSI) ;
- 2 mois pour un suivi en temps réel des personnes identifiées (Art. L.851-2 CSI), pour la mise en place d'un algorithme (Art. L. 851-3 CSI) ou d'un IMSI catcher (Art. L. 851-6 CSI), la captation sur écran (Art. L 853-2 2° CSI) ou la captation d'image ou de son hors véhicule ou lieu privé (Art. L.853-1 CSI) ;
- 4 mois dans tous les autres cas.

Le Conseil constitutionnel considère que les techniques de renseignement relèvent de la police administrative et non de la police judiciaire. Le Premier ministre endosse donc la responsabilité de la politique publique de renseignement. C'est d'ailleurs l'absence d'intervention préalable du Premier ministre qui a entraîné la censure par le Conseil constitutionnel de l'article L.821-6 relatif à la procédure d'urgence opérationnelle.
Si la Premier ministre peut déléguer ses pouvoirs, ce ne peut être qu'à des collaborateurs directs, habilités au secret de la défense nationale. Le législateur a souhaité cette proximité pour éviter que ne se constitue « *une sorte de bureaucratie du droit du renseignement, où les carrières s'enchevêtrent, où l'on passerait des services sollicitant des autorisations à leur ministre aux conseillers des ministres qui font transiter la demande vers Matignon, aux membres des services de la commission nationale de contrôle et au cabinet du Premier ministre lui-même dans une sorte d'entre-soi complice qui diminuerait le niveau de garantie* »[5].

Un « service dépendant du Premier ministre », en fait le Groupe Interministériel de Contrôle (GIC), voit sa position renforcée. Déjà en charge des interceptions de sécurité (Art. L. 852-1 IV CSI), il bénéficie de compétences élargies puisqu'il lui revient désormais de recueillir les données de connexion (Art. L. 851-1 CSI) qui ne sont plus envoyées directement au service demandeur, d'assurer la traçabilité des techniques de renseignement et la centralisation des renseignements recueillis (Art. L.822-1 CSI).

Le juge administratif, gardien des libertés

Parmi les principales critiques émises par les adversaires de la loi figure l'absence de l'intervention dans la procédure du juge judiciaire, « gardien des libertés ». Le choix du juge administratif s'inscrit dans la logique du droit français qui s'organise autour de la « *summa divisio* » entre la police administrative et la police judiciaire. Ce choix, qui n'est pas réducteur pour les libertés, est conforme à la jurisprudence du Conseil Constitutionnel, réaffirmée par la décision n°2015-713 DC du 23 juillet 2015.

En France, la dualité de juridictions a été posée par la loi des 16 et 24 août 1790 et le décret du 16 fructidor an III. Le Code des délits et des peines du 25 octobre 1795 (3 brumaire An IV) distingue

5Philippe Bas, rapporteur de la loi. Sénat, séance du 4 juin 2015, JO Sénat p. 6031.

la police administrative de la police judiciaire :

- La police administrative a pour objet le maintien habituel de l'ordre public dans chaque lieu et dans chaque partie de l'administration générale. Elle tend principalement à prévenir les délits (Art. 19) ;
- La police judiciaire recherche les délits que la police administrative n'a pu empêcher de commettre, en rassemble les preuves et en livre les auteurs aux tribunaux chargés par la loi de les punir. (Art 20, auj. Art. 14 du Code de procédure pénale).

L'impact sur les libertés n'est pas l'élément discriminant. C'est le critère finaliste, dégagé par le Tribunal des Conflits (voir notamment Tribunal des Conflits, 12 juin 1978, Société Le Profil), qui crée la frontière entre les deux formes de police.
La mise en œuvre des techniques de renseignement, à caractère préventif, relève de la police administrative. La compétence juridictionnelle pour examiner, à titre principal, les mesures de police administrative est dévolue aux juridictions de l'ordre administratif. En effet, selon la jurisprudence du Conseil Constitutionnel, l'article 66 de la Constitution attribue au juge judiciaire une compétence exclusive limitée au droit à la sûreté, c'est-à-dire au droit de ne pas être arbitrairement détenu. Cela concerne en particulier la garde à vue, la détention, la rétention ou l'hospitalisation sans consentement. Les techniques de renseignement, ne constituant pas des mesures privatives de liberté, y compris lorsqu'elles impliquent une intrusion dans un lieu privé (véhicule, habitation), n'entrent pas dans le champ d'application de l'article 66 de la Constitution, de sorte que l'autorité judiciaire n'a pas compétence pour autoriser ou contrôler ces mesures de police, sauf si une infraction à la loi pénale est commise.

Le Conseil d'État, juge en premier et dernier ressort

L'article L. 311-4-1 (nouveau) du Code de justice administrative confie au Conseil d'Etat la connaissance en premier et dernier ressort, y compris en référé, du contentieux relatif au renseignement, qu'il s'agisse de la mise en œuvre des techniques de renseignement ou de la conservation des données. Le Conseil d'État, saisi par la CNCTR ou au moins trois de ses membres, est juge de plein contentieux. Il a un pouvoir d'annulation, d'indemnisation et d'injonction. Sauf renvoi à la Section du contentieux ou à l'Assemblée du contentieux, les affaires sont traitées par une formation spécialisée dont les membres sont habilités es qualité au secret de la défense nationale. Cette formation est également compétente pour les demandes d'accès aux fichiers intéressant la sûreté de l'État, la défense ou la sécurité publique (art. 41 de la loi n°78-17 du 6 janvier 1978).
Si la technique de renseignement contestée est illégale, le juge administratif peut annuler l'autorisation donnée par le Premier ministre et ordonner la destruction des données collectées à cette occasion.
Les articles L.773-1 à L.773-7 du même Code précisent une procédure dérogatoire en raison du secret de la défense nationale, mais qui respecte le principe du contradictoire.

La procédure contradictoire est asymétrique : 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 CJA). Elle entend les parties séparément lorsque le secret de la défense nationale est en cause.
Le président de la formation de jugement peut déroger à la publicité des audiences en ordonnant le huis-clos (article L. 773-4 CJA).
La motivation de la décision est réduite. Lorsqu'aucune technique de renseignement n'a été mise en œuvre ou lorsqu'elle l'a été de manière légale, le juge indique qu'aucune illégalité n'a été commise, sans confirmer ni infirmer la mise en œuvre d'une telle technique (article L. 773-6 CJA). Cette

motivation *a minima* évite de compromettre les finalités poursuivies ou la sécurité des services ou des sources.

La constitutionnalité de la loi

Pour la première fois de son histoire, le Conseil constitutionnel a été saisi par le Président de la République. Le Président du Sénat et 106 députés en ont fait de même. Pour les uns, il s'agissait de lever le doute sur la constitutionnalité de la loi sur le renseignement, pour les autres de faire censurer les articles qu'ils estimaient « liberticides ». Les Sages ont tranché !
La décision n°2015-713 DC du 23 juillet 2015, suivie de la décision n°2015-478 QPC du 24 juillet 2015 (recours relatif à l'article 20 de la loi de programmation militaire), déclare la loi, à l'exception de trois dispositions, conforme à la Constitution.

La légitimité du renseignement exige une loi précise, accessible à tous, et qui, par ses finalités et les moyens mis en œuvre, réponde à un besoin social impérieux, à une nécessité d'intérêt public, et respecte le principe de proportionnalité. Cette proportionnalité entre la fin et les moyens est, avec le strict encadrement par la loi des mesures intrusives, le « fil rouge » de la démonstration du Conseil, soit pour déclarer un article conforme à la Constitution, soit pour le censurer.
Est jugé non conforme à la Constitution l'article L. 821-6 du Code de la sécurité intérieure qui instituait une procédure « d'urgence opérationnelle » permettant aux services, en cas de menace imminente, de mettre en œuvre des techniques de renseignement, sans information du ministre concerné, sans autorisation du Premier ministre et sans avis préalable de la Commission Nationale de Contrôle des Techniques de Renseignement (CNCTR). La menace imminente ne justifie pas une telle disproportion par rapport au respect de la vie privée et au secret des correspondances.
En cas d'urgence liée à une menace imminente ou à un risque de ne pas pouvoir effectuer l'opération ultérieurement (Art. L.821-6), les services peuvent installer sans autorisation préalable des dispositifs techniques permettant de localiser en temps réel une personne, un véhicule ou un objet (Art. L.851-5), d'obtenir des données techniques de connexion (Art. L.851-6), ou mettre en œuvre des interceptions de sécurité si, dans ce dernier cas, sont en cause l'indépendance nationale, l'intégrité du territoire et la défense nationale, la prévention du terrorisme et la prévention des atteintes à la forme républicaine des institutions (Art.852-1 II). La procédure normale est néanmoins mise en œuvre dès que le Premier ministre et la CNCTR sont avisés .

Est également censuré l'article L. 854-1 relatif aux surveillances des communications émises ou reçues à l'étranger. Le Conseil reproche à la loi de n'avoir pas défini les règles concernant les garanties fondamentales. Le renvoi à un décret en Conseil d'État des conditions d'exploitation, de conservation et de destruction des renseignements, ainsi que des modalités d'exercice du contrôle par la CNCTR méconnaît l'article 34 de la Constitution qui définit le domaine de la loi.
Enfin, une censure plus technique affecte les dispositions de l'article L.832-4 relatives au budget de la CNCTR qui doivent relever d'une loi de finances.
Les opposants au texte espèrent désormais une condamnation de la France par la Cour européenne des droits de l'Homme. Mais celle-ci a déjà jugé que « *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*». Selon l'article 8, alinéa 2, de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, les dérogations au droit au respect de la vie privée et familiale, du domicile et des correspondances doivent être légitimes, nécessaires et proportionnées au but poursuivi : « *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 ».
S'il ne lui appartient pas de juger de la conventionnalité des lois, le Conseil constitutionnel n'a pas eu recours à un raisonnement différent pour déclarer conforme à la Constitution l'essentiel de la loi sur le renseignement.

Un nouveau fichier : Le Fichier Judiciaire national Automatisé des Auteurs d'Infractions Terroristes (FIJAIT)

La création de ce nouveau fichier n'était pas prévue dans le projet de loi initial. Il a été introduit par amendement du gouvernement lors des débats devant l'Assemblée nationale. Ce fichier s'inspire du FIJAISV qui concerne les auteurs d'infractions sexuelles ou violentes. Il a pour objectif de prévenir le renouvellement des infractions et d'identifier leurs auteurs.
Ce fichier est détenu par l'autorité judiciaire (service du casier judiciaire) et est placé sous l'autorité d'un magistrat. Il est accessible aux autorités judiciaires, aux agents des greffes pénitentiaires, aux officiers de police judiciaire et aux agents spécialement habilités des services de renseignement (Art. 811-2 et 811-4 du CSI), pour la seule finalité de la prévention du terrorisme. Des agents des préfectures ou d'administrations de l'Etat peuvent y accéder à l'occasion de certaines démarches (recrutement, affectation, autorisation, agrément, habilitation).
Sont inscrites au fichier les personnes ayant fait l'objet :

- **d'une condamnation, même non définitive ;**
- **d'une déclaration de culpabilité assortie d'une dispense ou d'un ajournement de peine ;**
- **d'une décision, même non définitive, relative à un mineur ;**
- **d'une décision d'irresponsabilité pénale pour trouble mental ;**
- **d'une mise en examen.**

Les informations sont conservées pendant 20 ans (majeur) ou 10 ans (mineur), le délai ne commençant qu'après la fin de l'incarcération. Elles sont effacées en cas de non-lieu, relaxe ou acquittement.
L'inscription au FIJAIT s'accompagne d'une inscription automatique au FPR et de la mise en œuvre de mesures de sûreté permettant de localiser la personne (déclaration d'adresse, changement d'adresse, voyages à l'étranger, voyages en France depuis l'étranger).

Dernière minute

Pour faire suite à la décision du Conseil constitutionnel du 23 juillet, le gouvernement a engagé le 15 septembre une procédure accélérée pour l'examen de la proposition de loi de Patricia Adam et de Philippe Nauche relative aux mesures de surveillance des communications électroniques internationales.

Retrouvez toutes nos publications sur:

http://www.gendarmerie.interieur.gouv.fr/crgn