N° 636

SÉNAT

SESSION EXTRAORDINAIRE DE 2016-2017

Enregistré à la Présidence du Sénat le 12 juillet 2017

AVIS

PRÉSENTÉ

au nom de la commission des affaires étrangères, de la défense et des forces armées (1) sur le projet de loi **renforçant** *la* **sécurité intérieure** *et la* **lutte contre** *le* **terrorisme** *(PROCÉDURE ACCÉLÉRÉE),*

Par M. Michel BOUTANT,

Sénateur

(1) Cette commission est composée de : M. Christian Cambon, *président ;* MM. Cédric Perrin, Daniel Reiner, Xavier Pintat, Mmes Nathalie Goulet, Josette Durrieu, Michelle Demessine, MM. Alain Gournac, Gilbert Roger, Robert Hue, Mme Leila Aïchi, *vice-présidents ;* M. André Trillard, Mmes Hélène Conway-Mouret, Joëlle Garriaud-Maylam, MM. Joël Guerriau, Alain Néri, *secrétaires ;* MM. Pascal Allizard, Michel Billout, Jean-Marie Bockel, Michel Boutant, Jean-Pierre Cantegrit, Bernard Cazeau, Pierre Charon, Robert del Picchia, Jean-Paul Émorine, Philippe Esnol, Hubert Falco, Bernard Fournier, Jean-Paul Fournier, Jacques Gillot, Gaëtan Gorce, Mme Sylvie Goy-Chavent, MM. Jean-Pierre Grand, Jean-Noël Guérini, Claude Haut, Mme Gisèle Jourda, M. Alain Joyandet, Mme Christiane Kammermann, M. Antoine Karam, Mme Bariza Khiari, MM. Robert Laufoaulu, Jacques Legendre, Jeanny Lorgeoux, Claude Malhuret, Jean-Pierre Masseret, Rachel Mazuir, Christian Namy, Philippe Paul, Mme Marie-Françoise Perol-Dumont, MM. Jean-Vincent Placé, Yves Pozzo di Borgo, Jean-Pierre Raffarin, Henri de Raincourt, Alex Türk, Raymond Vall, André Vallini.

Voir les numéros :

Sénat : **587**, **629** et **630** (2016-2017)

S O M M A I R E

Mesdames, Messieurs,

Notre pays vit sous le régime de l'état d'urgence depuis le 14 novembre 2015 en raison des attentats terroristes commis sur notre sol. L'article 1er de la loi du 3 avril 1955 modifiée instituant l'état d'urgence dispose ainsi que « *l'état d'urgence peut être déclaré sur tout ou partie du territoire métropolitain, des départements d'outre-mer, des collectivités d'outre-mer régies par l'article 74 de la Constitution et en Nouvelle-Calédonie, soit en cas de péril imminent résultant d'atteintes graves à l'ordre public, soit en cas d'événements présentant, par leur nature et leur gravité, le caractère de calamité publique* ».

En raison de la persistance d'un très haut niveau de menace, le Gouvernement a demandé au législateur de proroger l'état d'urgence à six reprises. Une prorogation pour une durée de trois mois a ainsi été effectuée par la loi n° 2015-1501 du 20 novembre 2015 ; pour la même durée, par la loi n° 2016-162 du 19 février 2016 ; ensuite pour deux mois par la loi du 20 mai 2016[1] ; pour six mois par la loi du 21 juillet 2016[2] ; à nouveau par la loi du 19 décembre 2016[3] pour une fin prévue le 15 juillet 2017 ; enfin, une sixième prorogation a été adoptée le 11 juillet 2017 pour une fin le 1er novembre de la même année[4].

L'utilisation des mesures de police administrative (perquisitions, mesures de sûreté, mesures de contrôle des personnes…) prévues par la loi du 3 avril 1955 constitue désormais l'un des piliers de la stratégie antiterroriste menée par les pouvoirs publics. Dès lors, le constat d'une persistance de la menace terroriste plus d'un an et demi après la première entrée en vigueur de l'état d'urgence a conduit le nouveau Gouvernement à proposer, sous la forme du présent projet de loi, la création de nouveaux instruments, permanents cette fois, de prévention et de lutte contre le terrorisme.

---

[1] *Loi n° 2016-629 du 20 mai 2016 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence.*

[2] *Loi n° 2016-987 du 21 juillet 2016 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et portant mesures de renforcement de la lutte antiterroriste. Il aurait dû être mis fin à l'état d'urgence à l'issue de la troisième période de prorogation, le 26 juillet 2016, ainsi que l'avait annoncé le Président de la République lors de sa traditionnelle interview du 14 juillet. Toutefois, la tragédie survenue à Nice dans la soirée du 14 juillet a conduit l'exécutif à changer de position et à saisir le Parlement d'une nouvelle demande de prorogation.*

[3] *Loi n° 2016-1767 du 19 décembre 2016 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence.*

[4] *Loi n° 2017-1154 du 11 juillet 2017 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence.*

Outre ces dispositions relatives à la police administrative, le présent texte fournit au Gouvernement l'occasion de proposer au Parlement de mener à bien certaines modifications nécessaires au sein de **deux dispositifs législatifs** ayant un lien avec la lutte contre le terrorisme. **Votre commission des affaires étrangères, de la défense et des forces armées a décidé de se saisir pour avis des cinq articles correspondants (articles 5 à 9) dans la mesure où ces deux dispositifs entrent dans son champ de compétence**.

Il s'agit en premier lieu du **cadre juridique du fichier dit « PNR »** (*Passenger name record*), créé par la loi de programmation militaire du 18 décembre 2013[1] pour permettre un meilleur contrôle des passagers du transport aérien, afin de lutter contre le terrorisme et contre d'autres infractions très graves (**articles 5 à 7**). En effet, d'une part, l'adoption récente de la directive européenne relative au PNR[2], au terme d'un très long processus, implique la mise à jour des dispositions qui avaient été introduites par anticipation au sein de la loi française en 2013. D'autre part, le présent projet de loi propose la création d'un fichier des passagers du transport maritime, destiné à permettre, aux mêmes fins de lutte contre le terrorisme et contre d'autres infractions graves, un contrôle des passagers des navires transitant par les ports français.

En second lieu, le présent projet de loi propose d'instaurer **un nouveau régime légal de surveillance des communications hertziennes** afin de tirer les conséquences de la décision n° 2016-590 QPC du 21 octobre 2016 par laquelle le Conseil constitutionnel a censuré, avec effet différé au 31 décembre 2017, les dispositions de l'article L. 811-5 du code de la sécurité intérieure fixant le régime juridique encadrant cette technique de renseignement. Ces dispositions trouvaient leur origine dans l'article 20 de la loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques[3], reprises par la loi n° 2015-912 du 24 juillet 2015 relative au renseignement au sein d'un article L. 811-5 du code de la sécurité intérieure. Dans la mesure où **la surveillance hertzienne peut notamment être mise en œuvre par les armées et par certains services de renseignement**, il était nécessaire pour votre commission de s'assurer que les nouvelles dispositions ainsi prévues par les **articles 8 et 9** du présent texte leur garantissent à la fois un fondement juridique stable et sûr et des prérogatives suffisantes pour mettre en œuvre leurs missions.

---

[1] *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.*

[2] *La directive (UE) 2016/681 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière (dite « directive PNR ») a été adoptée le 21 avril 2016 après plusieurs années de négociation.*

[3] *Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques.*

I. LES DISPOSITIONS RELATIVES AU FICHIER « PNR »

A. LA CRÉATION D'UN FICHIER « PNR » PAR LA LOI DE PROGRAMMATION MILITAIRE

L'article 17 de la loi de programmation militaire de 2013 avait prévu la possibilité de créer un nouveau fichier de données dites « PNR » (*Passenger name record*), anticipant le vote d'une directive européenne dont le projet avait été présenté en février 2011.

Les différents types de données collectables liées au transport aérien de passagers

1 - les données directement collectées à partir de la bande de lecture optique (dite « MRZ ») des documents de voyage, de la carte nationale d'identité et des visas des passagers de transporteurs aériens, maritimes ou ferroviaires. Cette technique rend possible l'enregistrement systématique et rapide des données contenues dans la bande optique.

2 - les données « APIS » ou « API » : numéro et type du document de voyage utilisé, nationalité, nom complet, date de naissance, point de passage frontalier utilisé pour entrer sur le territoire des États membres, code de transport, heures de départ et d'arrivée du transport, nombre total des personnes transportées et point d'embarquement initial.

3 - les données « PNR » : nom et prénom du client, renseignements sur l'agence de voyage auprès de laquelle la réservation est effectuée, itinéraire du déplacement qui peut comporter plusieurs étapes, indications des vols concernés (numéro des vols successifs, date, heures, classe économique, business...), groupe de personnes pour lesquelles une même réservation est faite, contact à terre du passager (numéro de téléphone au domicile, professionnel...), tarifs accordés, état du paiement effectué et ses modalités par carte bancaire, réservations d'hôtels ou de voitures à l'arrivée, services demandés à bord tels que le numéro de place affecté à l'avance, repas et services liés à la santé...), etc.

Le système français de PNR, dont la mise en place a été confiée à une mission interministérielle sous l'égide du préfet Évance Richard, est actuellement en fin d'expérimentation.

Sur le plan opérationnel, il est mis en œuvre, conformément au projet de directive, par une « unité d'information passagers » (UIP) composée de membres des services « clients » : douanes, police et gendarmerie, et qui reçoit les données API et PNR en provenance des transporteurs aériens. Comme l'a souligné Olivier Bardin, directeur de l'UIP, lors de son audition, le fichier PNR présente en effet une profonde originalité par rapport aux grands fichiers de police judiciaire : il n'est pas consulté directement par les services utilisateurs mais uniquement par le biais de

cette UIP, qui s'apparente ainsi à une sorte de « gardien du temple » du fichier. Cette originalité découle d'une spécificité importante : le PNR ne contient pas des données sur des personnes condamnées par la justice ou soupçonnées d'avoir commis des délits comme les autres fichiers, mais sur tous les usagers du transport aérien. Cette caractéristique, qui explique en partie la vigueur des débats initiaux autour de la création d'un tel fichier, s'est également traduite par la mise en place d'un processus de « masquage » des données permettant de retrouver l'identité de la personne sur laquelle des données ont été collectées, masquage qui intervient automatiquement au bout de deux ans.

Le fichier ainsi constitué est utilisé, sur requête auprès de l'UIP, par les services de police, de gendarmerie et par les services de renseignement, pour des finalités de prévention et de constatation de certaines infractions considérées comme particulièrement graves (criminalité organisée, terrorisme, atteintes aux intérêts fondamentaux de la Nation). Il assume à la fois des fonctions de « ciblage » et de « criblage».

Le « ciblage » consiste à **utiliser des grilles d'analyse du risque pour repérer des passagers statistiquement plus susceptibles de commettre des infractions graves**. Les critères de ciblage sont élaborés progressivement par les agents de l'UIP. Les résultats automatiques de la mise en œuvre du ciblage font ensuite systématiquement l'objet d'une analyse humaine avant de décider une action de surveillance, de contrôle ou d'interpellation. Comme l'a indiqué le directeur de l'UIP lors de son audition, l'efficacité de ce ciblage reste tributaire de la qualité des données fournies par les compagnies aériennes. Or, à l'origine, ces données sont recueillies à des fins commerciales et ont donc tendance à être d'une qualité insuffisante pour pouvoir être utilisées dans le domaine de la sécurité, à moins d'accepter un taux élevé de « faux négatifs » ou de « faux positifs ». Progressivement toutefois, la qualité des données fournies se serait améliorée.

Le « criblage » consiste quant à lui à croiser les données du fichier PNR avec plusieurs traitements dont le fichier des personnes recherchées (FPR), afin de repérer une personne recherchée au départ ou à l'arrivée du territoire français. Comme le directeur de l'UIP l'a indiqué, ce n'est pas l'ensemble du FPR mais une version expurgée des cas les moins graves, qui est concerné par le criblage. Seulement 15 % environ des fiches individuelles du FPR sont ainsi concernées.

Actuellement, le fichier PNR, encore en cours d'expérimentation, reçoit par le biais de l'UIP environ 300 demandes par jour des services utilisateurs. Ces demandes sont traitées par 35 personnes, l'effectif devant progresser à terme jusqu'à 75 personnes.

Pour le moment, le dispositif ne concerne que les vols extra-communautaires, mais il sera également appliqué aux vols intra-communautaires après notification à la Commission européenne, conformément à ce que prévoit l'article 2 de la directive.

B. LA NÉCESSAIRE MISE EN CONFORMITÉ AVEC LA DIRECTIVE EUROPÉENNE

Le processus d'adoption de la directive présenté en 2011, qui prévoyait l'obligation pour tous les États membres de se doter d'un fichier des passagers aériens, a été particulièrement long. En effet, la directive PNR devait être la première directive dans le domaine JAI (justice et affaires intérieures) à être adoptée selon le processus de codécision issu du traité de Lisbonne de 2009. Or, juste avant la présentation de cette directive, un accord très critiqué[1] de transfert des données PNR européennes aux autorités américaines avait été négocié par la Commission européenne dans le cadre pré-Lisbonne, si bien que le Parlement européen s'est immédiatement montré réticent à donner son accord à l'adoption du projet de PNR européen. La négociation au sein des instances européennes ne s'est ainsi achevée qu'en avril 2016 avec **l'adoption définitive de la directive 2016/681 du 27 avril 2016**[2].

Il est donc nécessaire de modifier la loi française pour deux raisons : d'une part, **afin de pérenniser le dispositif**, le fichier PNR n'ayant été créé par la loi de programmation militaire qu'à titre expérimental jusqu'au 31 décembre 2017[3] ; d'autre part, **afin d'assurer la pleine conformité des dispositions introduites par la loi de programmation militaire à celles de la nouvelle directive européenne**. Cette mise en conformité n'exige toutefois que des modifications mineures du droit positif dans la mesure où les dispositions de la loi de programmation militaire étaient très proches du projet de directive, cette conformité globale ayant d'ailleurs été renforcée par les amendements adoptés par le Sénat lors de l'examen de ce texte en 2013.

Les modifications résiduelles effectuées par **l'article 6** du présent texte au sein de l'article L. 232-7 du code de la sécurité intérieur[4] pour assurer la conformité du droit interne à la directive sont ainsi les suivantes :

- l'article L. 232-7 renverra désormais à la liste des formes graves de criminalité décrites dans l'annexe II de la directive, qui fixe la liste des infractions pour la prévention et la constatation desquels l'utilisation du PNR est possible, dès lors qu'elles sont punies dans l'Etat membre concerné d'une peine privative de liberté ou d'une mesure de sûreté d'une durée d'au moins trois ans. Le droit en vigueur renvoie en effet à l'article 695-23 du code pénal (les infractions visées sont toutefois quasiment les mêmes puisque l'article 695-23 renvoie aux infractions prévues pour la mise en œuvre du mandat d'arrêt européen, elles-mêmes proches de celles de la directive PNR).

---

[1] *Cf. les critiques exprimées par la résolution du 13 janvier 2012 de la Commission des affaires européennes du Sénat à ce sujet : https://www.senat.fr/ue/pac/E6869.html*

[2] *Directive (UE) 2016/681 du 27 avril 2016 relative à l'utilisation des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière.*

[3] *Cette pérennisation est effectuée par l'article 5 du présent projet de loi.*

[4] *Qui codifie l'article 17 de la loi de programmation militaire relatif au PNR.*

Notons que la référence aux « *atteintes aux intérêts fondamentaux de la nation* », qui ne figure pas dans la directive, est maintenue dans l'article L. 232-7. En effet, si cette finalité ne figure pas dans le champ de compétence de l'Union européenne, les États membres peuvent aller plus loin que la directive dans ce domaine et prévoir eux-mêmes que leur PNR peut être mis en œuvre pour cette finalité ;

- actuellement, en application de l'article 28 de la loi du 28 juillet 2015 actualisant la loi de programmation militaire[1], l'article L. 232-7 du code de la sécurité intérieure prévoit que les entités soumises à l'obligation de transmission des données PNR sont « *les opérateurs de voyage ou de séjour affrétant tout ou partie d'un aéronef* », conformément à la directive 2016/681 dont le considérant 33 dispose que « *la présente directive est sans préjudice de la possibilité pour les États membres de prévoir, en vertu de leur droit national, un système de collecte et de traitement des données PNR auprès d'opérateurs économiques autres que les transporteurs, tels que des agences ou des organisateurs de voyages qui fournissent des services liés aux voyages, y compris la réservation de vols, pour lesquels ils recueillent et traitent les données PNR (...)* ». Toutefois, **l'article L. 232-7 du code de la sécurité intérieure n'évoque pas expressément les « agences de voyages »**. Afin d'ôter toute ambiguïté, l'article 6 ajoute cette expression ;

- **le masquage des données, évoqué ci-dessus, intervient au terme d'un délai de deux ans alors que la directive prévoit six mois**. Cette modification est cependant d'ordre réglementaire : devra ainsi être modifié 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 et codifié aux articles R. 232-12 à R. 232-18 du même code. Cette modification devra intervenir avant le 25 mai 2018, date d'expiration du délai de transposition de la directive (UE) 2016/681 ;

- les articles 5 et 7 de la directive prévoient **la nomination d'un délégué à la protection des données** (« *data protection officer* » ou DPO) pour contrôler l'utilisation conforme du fichier. Le Gouvernement a toutefois décidé d'attendre la transposition de la directive « protection des données » du 27 avril 2016[2] car celle-ci prévoit, en son article 32, l'adoption de dispositions législatives généralisant, pour tous les traitements des données à caractère personnel à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, la désignation d'un délégué à la protection des données, doté d'un statut et de pouvoirs décrits par cette même directive.

---

[1] *Loi n° 2015-917 du 28 juillet 2015 actualisant la programmation militaire pour les années 2015 à 2019 et portant diverses dispositions concernant la défense.*

[2] *Directive n° 2016/680.*

Enfin, l'article 6 modifie également l'article L. 232-1 du code de la sécurité intérieure, relatif au traitement « SETRADER », qui collecte et traite uniquement les données API et les exploite pour des finalités autres que celles prévues pour le système PNR (amélioration du contrôle aux frontières et lutte contre l'immigration irrégulière). Afin de réserver cet article aux seules données API, comme c'est déjà le cas dans la pratique, l'article 6 prévoit ainsi de supprimer au sein de l'article L. 232-1 la référence aux données PNR.

Votre rapporteur se félicite de cette nouvelle étape dans la mise en œuvre du PNR, un tel fichier constituant un des instruments les plus utiles dans la lutte contre les formes actuelles de terrorisme marquées par des déplacements fréquents des criminels entre l'Europe et le Moyen-Orient. Il convient toutefois de souligner que **la valeur ajoutée d'une approche communautaire de ce sujet réside dans la possibilité, qui doit à présent constituer une priorité, d'organiser des échanges entre les unités information passagers (UIP) des États membres**, dès que ceux-ci se seront dotés d'un PNR. Actuellement, la France peut déjà coopérer avec le Royaume-Uni, dont le système est déjà ancien, avec la Roumanie et avec la Hongrie. L'Allemagne devrait rejoindre ces pays courant 2018, ainsi que l'Espagne, qui s'est déjà dotée d'une UIP. Il sera cependant nécessaire d'inciter l'Italie à poursuivre ses efforts dans ce domaine, tandis que la Grèce a malheureusement pris du retard pour des raisons essentiellement financières.

C. VERS UN NOUVEAU « PNR » MARITIME

La loi du 20 juin 2016 pour l'économie bleue[1] a déjà institué **un traitement automatisé de données à caractère personnel des passagers du transport maritime** en modifiant les articles L. 232-4 et L. 232-7 du code de la sécurité intérieure.

Le 4 novembre 2016, le Premier ministre a décidé, en comité interministériel de la mer, de poursuivre la construction de ce dispositif qui vise, tout comme le PNR aérien dont il s'inspire, à faire face à la menace terroriste élevée, dans un secteur qui présente des vulnérabilités en matière de sécurité.

Ce projet de fichier vise ainsi à prévenir d'éventuels actes terroristes à bord des navires, ainsi qu'à mieux connaître les routes maritimes empruntées par des personnes à risque dans le domaine du terrorisme et des formes graves de criminalité, tant à l'entrée qu'à la sortie du territoire national.

La cible de ce nouveau traitement est le transport maritime de passagers, au départ et à l'arrivée des liaisons France/France,

[1] *Loi n° 2016-816 du 20 juin 2016 pour l'économie bleue*.

France/étranger ou étranger/France, à bord des navires battant pavillon français ou étranger. Ceci recouvre à la fois des liaisons maritimes fixes et régulières par ferries et des activités de croisières plus saisonnières (paquebots), pour un volume annuel global de passagers qui s'établit, selon l'étude d'impact, à 32,5 millions (dont 17 millions de passagers environ pour le trafic transmanche, 4 millions pour les liaisons régulières entre la Corse et le continent).

Le présent projet de loi (**article 7**) propose ainsi de créer un article L. 232-7-1 du code de la sécurité intérieure créant un dispositif à part entière, distinct de celui du PNR aérien prévu à l'article L. 232-7, strictement national puisqu'aucune règle européenne ne réglemente le domaine maritime.

Il s'agit d'un dispositif moins lourd et complexe que le PNR. Le traitement automatisé se limitera à un effort de standardisation dans la réunion des données déjà collectées par les compagnies maritimes lors des enregistrements de passagers, puis à des modalités de transferts facilitées aux services de sécurité chargés d'en assurer le criblage, afin d'identifier préventivement des passagers présentant une menace potentielle. Les fichiers criblés seront le fichier des personnes recherchées, le système d'information Schengen et le fichier des objets et véhicules signalés.

Les services qui pourraient être autorisés à accéder au système et y effectuer des requêtes seraient les suivants :

- au niveau territorial, aux fins de criblage des fichiers de police, les unités du ministère de l'intérieur, y compris la gendarmerie maritime, placée pour emploi auprès du ministère des armées, ou du ministère des finances directement en charge de la sûreté des navires ;

- au niveau central, les services et directions en charge de la lutte anti-terroriste et contre les crimes graves, les ministères de l'intérieur, des armées, chargés des transports ou chargés des douanes. Cette centralisation n'aura lieu que dans un second temps, sous l'autorité d'une direction encore à déterminer.

Par ailleurs, si les dispositions de l'article L. 232-7-1 relatif au PNR maritime reprennent pour l'essentiel celles de l'article L. 232-7 relatives au PNR aérien, en revanche le décret d'application de l'article L. 232-7-1, qui sera pris après avis de la Commission nationale de l'informatique et des libertés, ne prévoira la création d'aucune « Unité information passagers ». Le système s'apparentera donc davantage à un fichier de police classique qu'au PNR aérien.

Si votre rapporteur se félicite de la création d'un tel système qui devrait permettre d'accroître la maîtrise du risque terroriste en matière de transport maritime de passager, il souligne toutefois que, comme dans le cas du PNR aérien, son efficacité serait nettement améliorée en cas de coopération entre les pays membres. À l'heure actuelle, le Royaume-Uni, l'Espagne, la Finlande, le Danemark et la Belgique disposent de systèmes

plus ou moins avancés. Il convient donc d'encourager ces pays et les autres partenaires européens de la France à poursuivre leurs efforts dans ce domaine.

II. LES DISPOSITIONS RELATIVES AUX TECHNIQUES DE RENSEIGNEMENT

Le chapitre du projet de loi a pour objet de compléter le code de la sécurité intérieure en instaurant un nouveau régime légal de surveillance des communications hertziennes, c'est-à-dire aux transmissions sans support filaire qui utilisent le champ électromagnétique pour transmettre un message d'une antenne émettrice vers une antenne réceptrice.

Il s'agit de tirer les conséquences de la décision du 21 octobre 2016[1] par laquelle le Conseil constitutionnel a censuré, avec effet différé au 31 décembre 2017, les dispositions de l'article L. 811-5 du code de la sécurité intérieure qui permettent aux pouvoirs publics de prendre, à des fins de défense des intérêts nationaux, des mesures de surveillance et de contrôle des transmissions empruntant la voie hertzienne. L'utilité opérationnelle de ces mesures est majeure, notamment dans le domaine militaire, mais aussi pour la prévention du terrorisme et des ingérences étrangères.

A. DE « L'EXCEPTION HERTZIENNE » À L'INSERTION DANS LE DISPOSITIF LÉGISLATIF PROPRE AUX TECHNIQUES DE RENSEIGNEMENT

1. Une surveillance légale assortie d'un encadrement minimal

Lorsque pour répondre aux exigences résultant de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales[2], le législateur a instauré, dans le cadre de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications électroniques, le régime légal, administratif et judicaire, de l'interception et de l'exploitation des correspondances émises par la voie des télécommunications, il avait choisi de faire un sort particulier aux transmissions hertziennes, en les excluant du champ d'application des dispositions nouvelles. « *Les mesures prises par les pouvoirs publics, pour assurer, aux seuls fins de défense des intérêts nationaux, la surveillance et le contrôle des transmissions empruntant la voie hertzienne ne sont pas soumises aux dispositions des titres Ier et II de la présente loi* [3]».

---

[1] *Décision n° 2016-590 QPC du 21 octobre 2016*

[2] *Exprimées dans l'arrêt de la cour européenne Kruslin/France du 24 avril 1990*

[3] *Article 20 de la loi n° 91-646 du 10 juillet 1991 devenu article L. 241-3 du code de la sécurité intérieure.*

L'instauration de cette « exception hertzienne » était justifiée par le fait que les opérations correspondantes consistaient en une surveillance générale du domaine radioélectrique sans viser des communications individualisables[1]. Dès lors, elles ne constituaient pas une atteinte au secret des correspondances au sens de l'article 8 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales. La loi consacrait donc cette mission de surveillance et de contrôle mais l'exemptait des dispositifs du régime de l'interception et de l'exploitation des correspondances émises par la voie des télécommunications, notamment en ne les soumettant à aucune autorisation préalable du Premier ministre, ni à aucun contrôle a posteriori de la Commission nationale de contrôle des interceptions de sécurité (CNCIS).

2. Un encadrement de fait mis en œuvre par la CNCIS

La CNCIS s'est accommodée de ce dispositif particulier en précisant toutefois, dès son premier rapport d'activité portant sur les années 1991 et 1992, qu'il ne pouvait se rattacher qu'à une mission générale de police des ondes. Par la suite, en s'appuyant sur les travaux parlementaires ayant précédé l'adoption de la loi du 10 juillet 1991, elle a exclu qu'il puisse procéder à des recherches ciblées destinées à intercepter des communications individualisables et permettre un contournement du régime légal plus contraignant que prévu pour les interceptions de sécurité. La CNCIS avait précisé, en 1998, qu'il ne pouvait servir de fondement légal à l'interception de communications échangées par un téléphone mobile, alors même qu'une partie de leur acheminement est assurée par voie hertzienne (entre le terminal et l'antenne-relai).

La CNCIS et l'exception hertzienne

Au regard des évolutions technologiques, s'est rapidement posée la question des téléphones portables, dont les communications passent par la voie hertzienne. Dès 1998, la CNCIS a précisé que **le principe de liberté publique primait sur l'évolution technologique**, l'exception de l'article L. 241-3 devant ainsi s'interpréter strictement. La CNCIS rappelait ainsi dans son rapport pour l'année 1998 que « *toute interception de correspondance échangée par la voie des télécommunications, qui n'entre pas dans le champ de l'article 20, est soumise quel que soit le mode de transmission filaire ou hertzien, aux conditions et aux procédures fixées par la loi du 10 juillet 1991* »[2].

[1] Henri Nallet, garde des sceaux : « *Cette surveillance, qui consiste en un balayage aléatoire du domaine hertzien, sans viser, a priori, des communications individualisables, ne peut se prêter, en raison même de sa nature technique, à des procédures d'autorisation préalable et de contrôle* »

[2] *Cette approche a été confirmée par le juge pénal, dans un jugement du tribunal correctionnel de Paris du 8 avril 2014 rendu à l'encontre d'un ancien directeur central du renseignement intérieur.*

Dans son vingtième rapport d'activité, la CNCIS[1] a rappelé que les dispositions de l'article L. 241-3 sont «*parfaitement distinctes des interceptions de sécurité et des procédures de recueil de données techniques de communications entrant dans le champ du contrôle de la CNCIS*. Elle a précisé que « *l'article L. 241-3 est relatif aux mesures générales de surveillance des ondes incombant au gouvernement pour la seule défense des intérêts nationaux et ne peut servir de base à la mise en œuvre d'interceptions de communications individualisables et portant sur une menace identifiée* ».

Cette surveillance est effectuée pour assurer la« *défense d'intérêts nationaux* » qui est une notion très large comme l'a rappelé la CNCIS : « *il appert que cette notion «d'intérêts nationaux » est très large et générique, incluant l'ensemble des « intérêts» de la communauté nationale, quel que soit le domaine considéré* ». Pour faire l'objet de cette surveillance, les transmissions concernées doivent emprunter la voie hertzienne et les mesures de surveillance et de contrôle doivent s'effectuer« *de manière aléatoire et non individualisée* ».

Ces mesures sont plus larges que les seules interceptions de sécurité ou le recueil de données techniques. Elles sont aussi par nature **aléatoires** et **non ciblées** sur une communication. Elles relèvent davantage d'une logique de prévention.

Dans ses deux derniers rapports d'activité, la CNCIS a finalement estimé que la définition de l'exception hertzienne par la loi était obsolète et recommandé sa suppression.

3. Un dispositif d'exception maintenu par la loi du 24 juillet 2015 relative au renseignement

Pour autant, en 2015 le Gouvernement, dans le projet de loi sur le renseignement qui étendait le système d'autorisation et de contrôle à de nouvelles techniques de renseignement, n'a pas proposé d'évolution de ce dispositif, estimant que, fondé sur la loi et précisé par la jurisprudence de la CNCIS, il semblait satisfaisant et suffisant. Ceci amena le législateur de 2015 à le reconduire dans le cadre de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement, la disposition figurant dès lors à l'article L. 811-5 du code de la sécurité intérieure. Ce choix semblait en outre conforté par l'avis rendu en assemblée générale, le 15 octobre 2015, par le Conseil d'État[2] saisi par le président du Sénat sur la proposition de loi de M. Philippe Bas sur la surveillance des communications internationales[3].

---

[1] *p.40 et suiv.*

[2] *Conseil d'État, avis du 15 octobre 2015 (considérant 4) : http://www.senat.fr/rap/l15-097/l15-0977.html#toc34 : « la référence au II de l'article L.854-1, au terme de « réseaux de communications électroniques n'a ni pour effet de modifier le champ d'application des mesures de surveillance tel qu'il a été défini par la loi n° 2015-912 du 24 juillet 2015 relative au renseignement » (…) « les mesures prises par les pouvoirs publics pour assurer, aux seules fins de défense des intérêts nationaux, la surveillance et le contrôle des transmissions empruntant la voie hertzienne continuent en effet, en application de l'ensemble du livre VIII du code de la sécurité intérieure, comme c'était déjà le cas dans la législation applicable antérieurement. »*

[3] *Sénat- Proposition de loi n°700 déposée par M. Philippe Bas déposée le 21 septembre 2015.*

Dans son rapport pour 2015 (*publié en février 2016*), la Délégation parlementaire au renseignement (DPR), poursuivant la réflexion posée par la CNCIS dans son rapport de 2011-2012 rappelée par le président Philippe Bas dans son rapport sur le projet de loi relative au renseignement[1] et prenant acte de la position exprimée par le Conseil d'État dans son avis sur la proposition de loi relative à la surveillance des communications internationales, avait néanmoins appelé l'attention du Président de la République et du Premier ministre. Elle soulignait « *les altérations déjà subies par le concept d' « exception hertzienne* » (l'interprétation donnée par la CNCIS dès 1998, l'insertion dans les procédures d'autorisation et de contrôle du recueil de renseignement au moyen de dispositif de proximité). **Elle estimait que « *l'interprétation de la CNCIS devrait être confirmée par la CNCTR* *« et que dans l'hypothèse d'une confirmation, il lui faudra décider, le cas échéant, par analogie, selon la nature des communications ou la localisation des points d'émissions et de réceptions du régime applicable (régime de communication nationale ou régime des communications internationales*). *Dans la mesure où ces captations seraient réalisées à partir du territoire national, il est légitime de s'interroger sur la capacité des services à réaliser sur les ondes hertziennes des interceptions qui concerneraient des communications rattachables au territoire national, du moins à en exploiter et à en conserver les données, si ces interceptions ne permettent pas d'identifier a priori les communications interceptées (sauf les dérogations introduites par l'art. L 854-1 du CSI s'agissant des communications électroniques internationales) ou les modalités selon lesquelles pourraient être exploitées des communications mixtes* »[2].

D'ailleurs, ayant pris acte du maintien de l'« exception hertzienne », la CNCTR a fait sienne la conception restrictive de la CNCIS et a en particulier, considéré que « *l'article L.811-5 du CSI ne saurait en aucun cas être utilisé pour recueillir des renseignements susceptibles d'être collectés aux moyens de techniques de renseignement prévues par le livre VIII du même code et soumises à autorisation du Premier ministre sous le contrôle de la commission*[3]».

4. Un dispositif d'exception jugé non conforme par le Conseil constitutionnel

Le Conseil constitutionnel, saisi par la voie d'une question prioritaire de constitutionnalité posée par plusieurs associations de défense des libertés publiques et transmise par le Conseil d'État, a répondu en droit à ces interrogations par une décision du 21 octobre 2016[4] et a invité le législateur à parfaire le dispositif d'encadrement de l'usage de ces techniques. Relevant l'écart entre l'interprétation restrictive rappelée par le

---

[1] *Sénat – 2014-2015 - Rapport n°460 p 109 et suiv.*

[2] *Rapport de la Délégation parlementaire au renseignement pour l'année 2015 p.71 et suiv. (Sénat 015-2016 n°423)*

[3] *Rapport d'activité de la CNCTR pour 2015/2016 p.49*

[4] *N°2016-590 QPC*

Gouvernement dans son mémoire en défense et la rédaction de l'article L. 811-5 du CSI qui ne reflétait pas ces restrictions d'usage, le Conseil a considéré que **dès lors qu'elles permettent aux pouvoirs publics de prendre des mesures de surveillance et de contrôle de toute transmission empruntant la voie hertzienne, sans exclure que puissent être interceptées des communications ou recueillies des données individualisables, les dispositions contestées portent une atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances résultant de l'article 2 de la Déclaration des droits de l'Homme et du citoyen de 1789.**

Il a considéré également que leur mise en œuvre *« aux seuls fins de défense des intérêts nationaux »* était moins restrictive que la référence justifiant l'utilisation des autres techniques à savoir « *les menaces, les risques ou les enjeux liés aux intérêts fondamentaux de la Nation* ». Enfin, il a considéré que les dispositions :

- **ne définissaient pas la nature des mesures de surveillance et de contrôle que les pouvoirs publics sont autorisés à prendre**. Dans ses observations, le Premier ministre n'a pas contesté toutes les potentialités que recèle cet article et qui étaient relevées par les associations requérantes : trafic entre ordinateurs, Smartphones, tablettes et bornes wifi, trafic satellite, trafic entre téléphones portables et antennes relais, trafic Bluetooth. **Le Conseil a précisé que les dispositions législatives, sans entrer dans le détail des mesures techniques, devaient au moins définir la nature des mesures de surveillance et de contrôle qu'elles autorisent** (mesures aléatoires et non individualisées ou au contraire, mesures ciblées et individualisées) ;
- **ni ne soumettaient le recours à ces mesures à aucune condition de fond ni de procédure et n'encadrent leur mise en œuvre d'aucune garantie, à la différence des dispositions relatives au renseignement pour les autres techniques.** Il ne définit pas « *les pouvoirs publics* » pouvant autoriser le recours à ces mesures (l'autorisation du Premier ministre n'est pas requise contrairement à l'ensemble des autres techniques). Il ne présente aucune garantie de procédure (principe de proportionnalité des techniques aux objectifs poursuivis, contrôle spécifique par la CNCTR ou un juge).

Il a dès lors déclaré la disposition contraire à la Constitution mais considérant que son abrogation immédiate aurait pour effet de priver les pouvoirs publics de toutes possibilités de surveillance des transmissions hertziennes, **il a donné au législateur jusqu'au 31 décembre 2017 pour remédier à cette inconstitutionnalité constatée.**

Il a soumis immédiatement l'utilisation de ces techniques à certaines procédures et garanties applicables aux autres techniques. Pour préserver l'effet utile de sa décision, les dispositions en cause ne sauraient être interprétées comme pouvant servir de fondement à des mesures d'interceptions de correspondances, de recueil de données de connexion ou de captation de données informatiques soumises par ailleurs à autorisation

sans qu'aient été mises en œuvre les procédures et garanties prévues pour ces techniques (autorisation du Premier ministre, avis ou information de la CNCTR et que la commission soit régulièrement informée sur le champ et la nature des mesures prises).

L'intervention du Conseil constitutionnel montre que le dispositif de contrôle de l'usage des techniques de renseignement est complet : procédure d'autorisation avec avis et intervention de la CNCTR, possibilité de recours devant la juridiction spécialisée du Conseil d'Etat qui a déjà rendu plusieurs décisions, possibilité de recours jusqu'à la saisine du Conseil constitutionnel par voie de QPC. C'est un signe de maturité. Il est possible de donner aux services de renseignement des capacités de surveillance importantes, tout en garantissant l'Etat de droit.

5. Le dispositif transitoire en vigueur jusqu'au 31 décembre 2017

Cette décision a conduit la CNCTR à adopter une délibération n°2/2016 du 10 novembre 2016[1] sur les mesures de contrôle et de surveillance des transmissions empruntant la voie hertzienne, prévues à l'article L 811-5 du CSI en attendant l'intervention du législateur.

Dans cette délibération, elle recommande au Premier ministre de veiller à ce que toutes les techniques de renseignement prévues au titre V du livre VIII du code de la sécurité intérieure soient mises en œuvre dans le respect de la procédure d'autorisation et de contrôle instituée par ce même livre.

Elle recommande également que chacun des ministres dont relèvent les services de renseignement concernés définisse, dans des instructions soumises à son avis, les conditions dans lesquelles ces services pourront appliquer les dispositions de l'article L.811-5 du code de la sécurité intérieure au plus tard au 31 décembre 2017, en particulier le champ et la nature des mesures mises en œuvre ainsi que les motifs invoqués pour y recourir.

Elle prévoit enfin que soient examinées avec chacun des services de renseignement concernés les modalités précises permettant à la commission d'être régulièrement informée des mesures prises par eux en application de l'article L.811-5 du code, cette information devant mettre la CNCTR à même de vérifier la conformité de ces mesures à la réserve d'interprétation formulée par le Conseil constitutionnel, de recommander, si elle les estime non conformes à cette réserve, l'interruption et la destruction des renseignements collectés et, dans l'hypothèse où sa recommandation ne serait pas ou insuffisamment suivie, de saisir le Conseil d'État d'un recours en application de l'article L.833-8 du code.

[1] *Rapport d'activité de la CNCTR pour 2015/2016, p.133*

Ainsi, jusqu'au 31 décembre 2017, l'article L. 811-5 du code de la sécurité intérieure ne permet plus que des mesures générales de surveillance des réseaux, en excluant le recueil de toute donnée individualisable en dehors du cadre des lois du 24 juillet et du 30 novembre 2015.

Comme l'indique la DPR dans son dernier rapport[1], « *cette décision n'est pas sans incidence sur l'activité de certains services de renseignement, par exemple la Direction du renseignement militaire. Aujourd'hui, en effet, celle-ci procède à des interceptions de communications internationales sur le réseau hertzien au titre de ses activités de renseignement d'origine électromagnétique (ROEM) en se servant d'antennes qui peuvent être installées sur le territoire national* ».

Actuellement, en vertu de la décision du Conseil constitutionnel et de la délibération de la CNCTR, les services doivent, pour procéder, depuis le territoire national, à des interceptions de communications individualisées transmises par voie hertzienne, disposer d'autorisations de recueil et d'exploitation.

En matière de communications transmises par voie hertzienne, il convient cependant de distinguer plusieurs techniques qui engendrent des conséquences différentes :

- ainsi les communications relayées par satellites constituent, en dehors de la diffusion audiovisuelle par satellite, des communications individualisables internationales ; leur interception sur le territoire national doit donc être encadrée par la loi du 30 novembre 2015 à la suite de la décision du Conseil constitutionnel ;
- en revanche, les communications radio, dont la transmission s'effectue exclusivement par voie hertzienne par émission d'un signal sans identification d'un destinataire individualisable par un opérateur de communications électroniques, sont des communications d'une autre nature ; leur interception sur le territoire national n'est plus encadrée par aucun dispositif légal depuis la décision du Conseil constitutionnel.

Il convient de noter que les communications dont la transmission par voie hertzienne constitue l'élongation sans fil d'un accès, soit à un opérateur (par exemple, en matière de téléphonie mobile), soit à un réseau privatif (par exemple, une communication wifi) ont toujours été régulées. Leur interception sur le territoire national est encadrée par la loi du 24 juillet 2015, comme elle l'était, historiquement, par la loi du 10 juillet 1991.

Le Gouvernement était placé aujourd'hui face à un choix :

- soit il ne proposait aucun texte avant le 31 décembre 2017. Dans ce cas, les interceptions hertziennes réalisées sur le territoire national auraient été régies, selon les cas, soit par la loi du 24 juillet 2015, soit par celle du 30 novembre 2015.

---

[1] *Rapport de la Délégation parlementaire au renseignement pour l'année 2016 p.71 et suiv. (Sénat 2016-2017 n°448) p.74 et suiv.*

Cependant, les mesures induites par une telle assimilation restaient à mettre en place ; en outre, le régime de la surveillance des ondes radio restait imprécis ;

- soit le Gouvernement proposait un texte. Dans ce cas, en matière de communications par voie hertzienne, il devra prendre des dispositions prévoyant des modes d'intervention et de contrôle qui garantissent le bon exercice des libertés publiques tout en permettant aux services de conserver leur efficacité.

La DPR recommandait pour sa part cette seconde solution, étant entendu qu'il lui apparaît comme fondamental de maintenir une exception hertzienne encadrée par la loi qui garantisse la continuité de l'activité de renseignement d'origine électromagnétique, notamment opérées par la DRM – émissions qui concernent essentiellement les communications institutionnelles (forces armées, gouvernements ....).

B. LA MISE EN PLACE DE NOUVELLES MODALITÉS D'AUTORISATION ET DE CONTRÔLE

Afin de recréer la base légale pour les mesures de surveillance des communications hertziennes, avant que l'abrogation de l'article L. 811-5 ne devienne effective, le Gouvernement a introduit dans le projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme, un chapitre 2 « Techniques de renseignement » comprenant deux articles 8 et 9.

Même si la nature et l'ampleur des mesures prises au nom de l'autorisation conférée par les dispositions de l'article L. 811-5 du code de la sécurité intérieure sont limitées, le maintien de cette possibilité de surveillance des communications hertziennes reste indispensable.

1. Le nécessaire maintien d'une capacité de surveillance

Cette base légale doit constituer le fondement à l'ensemble des mesures de surveillance des communications empruntant la voie hertzienne sans l'intervention d'un quelconque opérateur exploitant un réseau de télécommunications ouvert au public. L'étude d'impact énumère un certain nombre de cas comme l'interception et l'exploitation des communications radio très longue distance (gamme VLF, très basses fréquences), longue distance (gamme « HF », hautes fréquences) et courte distance (gamme V/UHF, très et ultra hautes fréquences). La surveillance de ces communications radio, depuis le territoire national, conserve une évidente utilité, et même un caractère stratégique, notamment dans trois champs majeurs d'intervention que sont l'action militaire, la lutte contre le terrorisme - à laquelle l'action militaire contribue d'ailleurs de plus en plus - et la contre-ingérence.

Si les communications radio ne représentent aujourd'hui qu'une part infime des flux mondiaux de communications, elles restent en effet couramment utilisées par des acteurs qui présentent un intérêt majeur pour les services de renseignement et pour les forces armées françaises : forces armées étrangères, groupes armés non étatiques, services spéciaux étrangers, réseaux institutionnels d'intérêt, organisations terroristes, personnes communiquant depuis des zones de conflit ou de crise dans lesquelles les infrastructures plus classiques (réseaux filaires, GSM, ...) ont disparu.

A ces acteurs s'ajoutent tous ceux qui, connaissant les risques de surveillance des communications empruntant des réseaux filaires exploités par des opérateurs susceptibles de répondre aux réquisitions légales des pouvoirs publics, choisissent de recourir à la technique plus artisanale de la radio pour éviter cette surveillance. Il convient à ce titre de souligner aussi que la voie hertzienne permet de véhiculer des communications sur de longues (HF), voire très longues distances (VLF), si bien que les interceptions réalisées depuis le territoire national, qui sont donc régies par la loi française, permettent en réalité de surveiller des communications émises ou reçues parfois très loin de notre territoire qui a l'avantage de comporter des portions sur plusieurs continents.

Dans le domaine militaire – et comme le rappelait le président Philippe Bas dans son rapport sur le projet de loi devenu ensuite la loi relative au renseignement du 24 juillet 2015 – ce sont des interceptions de communications VLF ou HF, en partie réalisées depuis le territoire national, qui permettent aux forces armées françaises de connaître les mouvements de troupes, de sous-marins, de bâtiments ou d'aéronefs militaires étrangers. Il en va de même lorsque des groupes armés terroristes emploient ce mode de communication sur les théâtres de conflits armés, ou encore pour communiquer avec les « combattants » qu'ils chargent d'aller commettre des attentats en Europe ou ailleurs.

Dans le domaine de la contre-ingérence, les interceptions HF permettent de détecter des instructions diffusées par des puissances étrangères vers leurs agents.

Quant aux communications radio courte distance, elles peuvent, comme il a été dit plus haut, être utilisées par des acteurs qui y voient l'occasion de communiquer sans être connectés à un réseau d'opérateur de télécommunications, en utilisant des moyens de communication très faciles à acquérir et qui assurent l'anonymat des utilisateurs. Des individus impliqués dans une prise d'otage, une opération terroriste ou une activité extrémiste violente peuvent ainsi utiliser des talkies-walkies ou des PMR (gamme V/UHF, la PMR – *private mobile radio* - étant une version numérique du talkie-walkie analogique) pour se coordonner ou communiquer avec des complices.

2. La nature de la communication comme fondement de la législation proposée

Pour procéder à l'élaboration du dispositif législatif nouveau, et pour clarifier la législation, le Gouvernement ne s'est pas fondé sur le caractère individualisable ou non individualisable des communications hertziennes interceptées, étant entendu que l'utilisation de ce critère, qui aurait pu le dispenser effectivement d'une intervention législative, n'est discriminant qu'a posteriori, non dans la phase d'interception, mais au stade de l'exploitation, comme il est exposé dans l'étude d'impact[1], mais sur la nature privée ou confidentielle ou, au contraire, ouverte et publique, de la communication car c'est bien de cette nature que naît l'atteinte au secret des correspondances ou au respect de la vie privée.

Bien que la communication hertzienne se définisse par l'utilisation du domaine public, il apparaît possible d'identifier et de distinguer les cas dans lesquels la communication radio est parfaitement ouverte et publique et d'autres dans lesquelles elle peut être regardée comme présentant un caractère privatif, alors même qu'elle est diffusée dans l'espace public.

« *Ce caractère privatif ou non peut dépendre de la portée de la communication : il est clair par exemple qu'un message diffusé sur les gammes VLF et HF et donc sur une longue ou très longue distance (plusieurs milliers de kilomètres) relève de la même logique que la diffusion audiovisuelle et ne peut être regardé comme destiné à un nombre restreint de destinataires. A l'inverse l'utilisation d'appareils radio à très faible portée donne un indice fort de l'intention de réserver le message à un nombre de destinataires restreint. De la même façon, l'intégration dans certains appareils radio de mécanismes automatiques d'authentification et de partage de clés de chiffrement (tel est le cas pour la PMR) révèle l'intention de réserver la communication échangée entre les seuls usagers de ces appareils.* »

3. La nouvelle législation opère la distinction de deux domaines[2] et établit deux régimes différents applicables aux communications électroniques empruntant exclusivement la voie hertzienne et n'impliquant pas l'intervention d'un opérateur de communication électronique

a) Les communications relevant du régime général régissant les techniques de renseignement

(1) Les communications assimilables aux techniques de communication existante

Le Livre VIII du code de la sécurité intérieure est modifié pour permettre aux services de renseignement d'intercepter et d'exploiter les communications électroniques empruntant la voie exclusivement hertzienne et n'impliquant pas l'intervention d'un opérateur de communications

[1] *Projet de loi Étude d'impact p.74*

[2] *Voir tableau de l'annexe 3*

électroniques exploitant un réseau ouvert au public dans un cadre légal doté des garanties appropriées.

La définition restrictive de ces communications garantit que l'ensemble des mesures d'interception et d'exploitation des communications n'empruntant qu'accessoirement la voie hertzienne ou transitant par un opérateur de communication électronique, demeure soumis aux dispositions du Livre VIII du code de la sécurité intérieure, applicables aux techniques de renseignement et aux mesures de surveillance des communications électroniques internationales.

De fait, il valide l'interprétation de la CNCIS et de la CNCTR pour ce type de communication1 dont il assimile la surveillance aux techniques visées par les lois de 2015 et la soumet donc au régime d'autorisation du Premier ministre et à l'intervention pour avis et/ou contrôle de la CNCTR et aux différents régimes concernant la conservation, l'extraction et la destruction des données figurant dans le Livre VIII du code de la sécurité intérieure.

(2) La création d'une cinquième technique de renseignement

S'agissant des communications électroniques empruntant la voie exclusivement hertzienne et n'impliquant pas l'intervention d'un opérateur de communications, le Gouvernement opère une distinction selon que les correspondances sont échangées ou non, au sein d'un réseau conçu pour une utilisation privative par une personne ou un groupe privé d'utilisateurs, lesquelles font l'objet de la création d'une nouvelle technique de renseignement dans la cadre du régime général.

L'article L. 852-2 nouveau du code de la sécurité intérieure crée ainsi une nouvelle technique de renseignement pour l'interception et l'exploitation de correspondances échangées au sein d'un réseau de communications électroniques empruntant exclusivement la voie hertzienne et n'impliquant pas l'intervention d'un opérateur de communications électroniques, lorsque ce réseau est conçu pour une utilisation privative par une personne ou un groupe fermé d'utilisateurs.

Ces mesures, du fait du caractère privatif du réseau, sont susceptibles de porter atteinte au droit au respect de la vie privée des personnes concernées et au secret des correspondances. Elles devaient, à l'évidence, faire l'objet d'un nouveau cadre légal puisque le caractère fermé ou privatif du réseau est le signe du caractère privé ou confidentiel de la communication ou des données interceptées et donc, l'indice de l'existence, d'une atteinte au secret de la correspondance et au respect de la vie privée. Elles seront encadrées par l'ensemble des garanties applicables dans le régime général régissant les techniques de renseignement (chapitres I[er] et III

[1] *Il s'agit des communications utilisant sur un segment la voie hertzienne, mais aussi de la quasi-totalité des communications par satellites, lesquelles passent par un opérateur ou encore le trafic entre un terminal et une borne Wifi transitant via l'Internet.*

du titre V du code de la sécurité intérieure) et donc soumises à une autorisation préalable du Premier ministre prise après avis de la Commission nationale de contrôle des techniques de renseignement au nom d'une ou plusieurs finalités mentionnées à l'article L. 811-3.

Toutefois, une disposition particulière est introduite pour adapter l'objet de l'autorisation qui pourrait être le réseau privatif surveillé plutôt qu'une personne individuellement désignée.

L'interception serait autorisée pour une durée maximale de quatre mois renouvelable et soumise aux obligations classiques en termes d'exploitation, de durées de conservation - l'article L. 822-2 prévoit 30 jours pour les correspondances et 4 ans pour les données de connexion -, de régimes de transcription, extraction et destruction et enfin en termes de contrôle par la CNCTR et, le cas échéant, par le juge.

Dans l'esprit déjà à l'œuvre pour la loi relative au renseignement, la rédaction de ce nouvel article L. 852-2 du CSI resterait, d'un point de vue technique, selon l'étude d'impact, suffisamment neutre pour ne pas être rapidement dépassée par le développement de nouveaux outils technologiques. A ce jour, le principal mode de communication qui entrerait dans son champ d'application est celui de la PMR déjà citée plus haut (technique de *talkie-walkie* numérique qui allie portée limitée et mécanismes d'authentification et de chiffrement automatiques, et donc existence d'identifiants techniques permettant une individualisation *a priori*), mais il concerne également le trafic entre un terminal et une borne Wifi, le trafic entre téléphones sans fil, le trafic des abonnés par satellites[1], le trafic Wimax, le trafic entre un téléphone portable et une antenne relais, le trafic d'un ordinateur utilisant une clé 3G/4G, le trafic relevant du protocole Bluetooth, l'échange de données entre une borne et un objet connecté.

Cet élargissement de la couverture du régime légal encadrant l'usage des techniques de renseignement issu de la loi sur le renseignement du 24 juillet 2015 et de la loi sur la surveillance des communications électroniques internationales de novembre 2015, la quasi-totalité des différentes techniques de communications hertziennes ou partiellement hertziennes dont la surveillance inquiétait les associations de défense des libertés publiques, requérante devant le Conseil d'Etat, puis le Conseil constitutionnel contre l'article L. 811-5 du code de la sécurité intérieure.

[1] *Qui pourra dans de nombreux cas être intercepté et exploité sur le fondement des dispositions des articles L. 854-1 et suivants eu égard au caractère international des communications empruntant la voie satellitaire.*

(3) La clarification du champ d'application de l'article relatif à la captation de données informatiques émises ou reçues par tout type de périphérique

L'article L. 853-2 est modifié à la marge[1] afin de clarifier son champ d'application, qui couvre la captation de données informatiques émises ou reçues par tout type de périphérique, anticipant en cela les évolutions techniques dans ce domaine où les protocoles sans fil sont employés pour une diversité croissante de types d'objets connectés. La modification proposée permettrait d'entourer de garanties strictes le recueil de tout type de données échangées par protocole sans fil, et non uniquement celles échangées avec des périphériques audiovisuels, étant rappelé que le recours au régime de l'article L. 853-2 est encore plus protecteur sur celui des interceptions de sécurité puisqu'il suppose le respect du principe de subsidiarité. Cette suppression confirmerait aussi la pratique qui a consisté, depuis la mise en œuvre de la loi du 24 juillet 2015, à admettre que l'interception de protocoles sans fil puisse entrer dans le champ de l'article L. 853-2 dans certaines configurations et sous le contrôle préalable de la CNCTR qui peut orienter les services vers la technique la plus pertinente et la moins attentatoire aux libertés publiques.

(4) Une économie générale approuvée par la CNCTR

En réponse à la saisine du Premier ministre, la CNCTR, dans sa délibération n° 4/2017 du 9 juin 2017, approuve l'économie générale du nouveau régime juridique, qui consiste, d'une part, à intégrer toutes les mesures de surveillance des transmissions hertziennes attentatoires à la vie privée dans le droit commun de la mise en œuvre des techniques de renseignement et, d'autre part, à rendre d'application résiduelle les mesures pouvant être prises sans autorisation spécifique préalable et constituant une nouvelle « exception hertzienne » d'ampleur nettement plus limitée que celle prévue à l'article L. 811-5 du code de la sécurité intérieure.

Elle constate que « *les communications concernées par la nouvelle « exception hertzienne » sont celles empruntant exclusivement la voie hertzienne et n'impliquant pas l'intervention d'un opérateur de communications électroniques. Il en résulte que les communications acheminées successivement par la voie hertzienne et la voie filaire ne pourront être légalement interceptées sur le fondement de ces dispositions, ce qui, de l'avis de la commission, lève définitivement l'ambiguïté que pouvait contenir la rédaction de l'article L. 811-5 du code de la sécurité intérieure* ».

[1] *La suppression du terme « audiovisuel » qui qualifiait les périphériques sur les écrans desquels des données informatiques peuvent être captées permet d'élargir l'objet de l'article à toutes les formes de communications.*

b) Les communications électroniques empruntant exclusivement la voie hertzienne et n'impliquant pas l'intervention d'un opérateur de communications électroniques, lorsque cette interception et cette exploitation n'entrent dans le champ d'application d'aucune des techniques de renseignement

(1) Un régime général dit du « hertzien ouvert »

Pour l'interception et l'exploitation des communications électroniques empruntant exclusivement la voie hertzienne et n'impliquant pas l'intervention d'un opérateur de communications électroniques, lorsque cette interception et cette exploitation n'entrent dans le champ d'application d'aucune des techniques de renseignement prévues par les chapitres I à IV, le chapitre V du titre V prévoit, à titre résiduel, une autorisation de nature législative (article L. 854-9-1).

La CB, les radio-amateurs, les talkies-walkies analogiques[1], ainsi que les communications radio VLF et HF et les moyens radio militaires tactiques V/UHF qui empruntent exclusivement la voie hertzienne et n'impliquant pas l'intervention d'un opérateur de communications électroniques relèvent de ce régime.

Un dispositif adapté à des appareils dont l'acquisition et la détention ne sont pas soumis à autorisation au titre des dispositions des articles 226-1 et suivants du code pénal

De façon très logique, il s'agit de communications qui peuvent être interceptées et exploitées par des appareils ne relevant pas du champ de l'autorisation prévue à l'article 226-3 du code pénal. Cet article prévoit en effet que la fabrication et la détention d'appareils ou de dispositifs techniques permettant de porter atteinte au secret des correspondances sont subordonnées à la délivrance, par le Premier ministre, d'une autorisation préalable. Or, pour l'application de ce régime défini aux articles R. 226-1 et suivants du code pénal, les appareils permettant l'interception des communications hertziennes publiques et ouvertes ne sont pas considérés comme permettant de commettre une telle infraction, faute pour les communications en cause d'être regardées comme des correspondances au sens strict - et donc pénal - du terme.

Selon l'étude d'impact, cette seconde catégorie aurait pu ne pas faire l'objet d'un régime légal[2]. Toutefois, compte tenu de l'historique de

[1] *Le principe même de la CB ou du radio-amateurisme est la diffusion publique de messages. Quant aux* talkies-walkies *analogiques, ils ne permettent aucune authentification ni aucun partage de clés de chiffrement et leurs émissions peuvent donc être reçues par toute antenne réceptrice réglée sur la bonne fréquence.*

[2] *Ainsi, aux termes de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, les communications radio « ouvertes et publiques » ne sont regardées comme des « communications ». La directive définit, en effet, une communication*

l'exception hertzienne en droit français, **le choix a cependant été fait de régir également par la loi les mesures d'interception et d'exploitation concernant ces communications**, dès lors qu'elles permettent l'accès au contenu du message ou de l'information diffusé et dans l'objectif d'en donner au moins une définition restrictive explicite, mais aussi **pour l'assortir d'un certain nombre de garanties.**

Ce régime est cependant logiquement allégé par rapport au droit commun des techniques de renseignement.

Ce régime résiduel applicable au hertzien public et ouvert a pour caractéristique majeure de ne pas prévoir d'autre autorisation préalable que celle conférée par la loi elle-même (article L. 854-9-1).

Il serait cependant assorti de garanties en termes de finalités (celles prévues à l'article L. 811-3), de délais de conservation des données (délais calqués sur ceux applicables aux communications électroniques internationales (article L. 854-9-2) à savoir :

- une durée maximale de six ans étendue à huit si les renseignements sont chiffrés.

De nombreuses interceptions HF sont des interceptions de forces de sécurité ou d'armées (la différence n'étant d'ailleurs pas toujours explicite dans certains pays). Ces organisations savent pertinemment que la HF est largement écoutable par tout un chacun. Leurs communications sont donc le plus souvent sibyllines et très courtes, par exemple par échange d'indicatifs, de mots codes. La compréhension repose donc sur la capacité des services de renseignement à conserver sur de très longues périodes ces quelques communications pour comprendre qui parle à qui et de quoi, remonter les réseaux...

- un régime de transcription/extraction (conforme au droit commun des techniques de renseignement).

Enfin, l'article L. 854-9-3 donnerait à la CNCTR les moyens de s'assurer du caractère résiduel du régime applicable aux communications hertziennes ouvertes et publiques et du respect des conditions de finalités et d'exploitation. Elle aurait à ce titre le même droit de regard sur les mesures prises en application de l'article L. 854-9-1 que celui que le Conseil constitutionnel lui avait accordé dans sa décision du 16 octobre 2016 pour la période transitoire ménagée par le report de l'abrogation de l'article L. 811-5 (droit d'information sur le « champ et la nature des mesures » en cause). Ce droit d'information serait accompagné d'un droit d'accès aux capacités d'interception et d'un pouvoir de sollicitation du Premier ministre pour avoir accès à tous les éléments nécessaires à l'accomplissement de sa mission, y compris à seule fin de s'assurer le respect des champs d'application, la

comme « toute information échangée ou acheminée entre un nombre fini de parties au moyen d'un service de communications électroniques accessible au public ».

communication des renseignements collectés et les transcriptions et extractions réalisées.

Le texte de l'article prévoit également un pouvoir de recommandations et d'observations adressées au Premier ministre ainsi qu'à la délégation parlementaire au renseignement. **Il y aurait lieu de prévoir dès lors une coordination avec les dispositions de l'article 6 *noniès* de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires (amendement ETRD.1)[1].**

Les mesures prises sur le fondement de l'autorisation conférée aux services de renseignement par l'article L. 854-9-1 ne seraient, en revanche, pas justiciables de la voie de recours spéciale créée devant la formation spécialisée du Conseil d'Etat. La nature non attentatoire au secret des correspondances ou au respect de la vie privée des mesures en cause ne justifie en effet pas que le droit commun - voies de droit devant le juge administratif ou le juge pénal - soit écarté à leur égard.

La CNCTR dans sa délibération n° 4/2017 a formulé deux observations qui n'ont pas été retenues par le Gouvernement :

- **la première sur la longueur de la durée de conservation des données recueillies** qu'elle proposait d'abaisser de six ans à quatre ans à compter du recueil des communications ;
- **la seconde, pour demander qu'elle puisse se faire communiquer directement les éléments utiles et les renseignements collectées ou les transcriptions et extractions réalisées, sans devoir les solliciter du Premier ministre.**

(2) Le régime spécifique aux forces armées (article 9)

Enfin**, le projet de loi règle le cas des interceptions et exploitations de communications hertziennes réalisées par les unités des armées.**

(a) Un usage spécifique

L'usage des communications radio est très répandu dans le monde militaire, comme la pratique de leur interception/exploitation.

En France, la surveillance militaire des communications radio est au premier chef le fait de la Direction du renseignement militaire, qui est l'un des services spécialisés de renseignement (article R. 811-1 du code de la sécurité intérieure) et relève donc du livre VIII dudit code.

Mais la Direction du renseignement militaire n'est pas la seule entité du ministère des armées à procéder à des fins militaires à des opérations d'interception et d'exploitation de communications radio.

Les militaires de certaines unités des armées mettent également en œuvre de telles mesures, pour l'exercice de leurs missions de défense

[1] *Voir Annexe n°2*

militaire (dissuasion, posture permanente de sûreté aérienne, posture permanente de sauvegarde maritime) **et d'action de l'Etat en mer**[1]. Les mesures de surveillance des communications pratiquées dans le cadre de ces missions ont pour objet d'identifier, en temps réel, la présence d'intrus ou d'éléments faisant peser une menace sur ou à proximité du territoire national, afin d'intervenir pour empêcher un acte hostile. Les illustrations les plus parlantes sont celles qui mettent en scène l'hypothèse d'aéronefs étrangers communiquant entre eux et manifestant des intentions hostiles à proximité de notre territoire ou des embarcations qui chercheraient à suivre un sous-marin nucléaire lanceur d'engin quittant sa base. Au demeurant, les missions des armées dans la défense du territoire ne sont pas des missions de renseignement (au sens de surveillance administrative) et donc n'entrent pas dans le domaine du Livre VIII du CSI. Les activités renseignement dans ce domaine sont plus à considérer comme des activités d'autoprotection ou d'alerte avancée que des missions de surveillance en vue d'acquérir une connaissance sur un adversaire (missions de la DRM). Il s'agit pour les armées d'être capable en permanence de détecter une menace hostile à proximité ou dans notre espace aérien ou nos eaux territoriales afin de réagir dans les plus brefs délais. Dans le cas de la dissuasion, il s'agit de protéger une sortie/entrée de nos SNLE dans le goulet de Brest (mesures d'autoprotection).

Il convenait donc de préserver leur droit à procéder ainsi, alors même qu'elles ne constituent pas des services de renseignement - le renseignement qu'elles pratiquent étant indissociable de l'action militaire - et n'ont dès lors pas le droit de mettre en œuvre, sur le territoire national en tout cas - d'autres techniques prévues par le livre VIII du CSI.

Afin de protéger leurs spécificités, la reconstitution de la base légale relative à leur activité a été insérée au sein du code de la défense (article L. 2371-1) qui autorisera les militaires des armées à pratiquer sans autorisation spécifique préalable les interceptions résiduelles prévues à l'article L. 854-9-1 du code de la sécurité intérieure

> (b) Un régime qui impose les mêmes obligations que celle du régime dit « hertzien ouvert » du code de la sécurité intérieure

Y a ainsi été « importée », par le biais d'un renvoi au code de la sécurité intérieure, l'autorisation légale prévue à l'article L. 854-9-1 du code de la sécurité intérieure pour le hertzien public et ouvert, accompagnée des mêmes durées de conservation et des mêmes règles concernant les transcriptions et extractions et leur destruction.

---

[1] *Et donc à l'exclusion des missions confiées aux armées dans le cadre de réquisitions par les autorités civiles (opération Sentinelle par exemple).*

(c) Un dispositif de contrôle plus léger

En revanche, le projet de loi prévoit un dispositif allégé de contrôle spécifique de la CNCTR sur cette activité d'interception et d'exploitation des communications hertziennes ouvertes (en fait des communications radio VLF, HF et V/UH tactiques) pratiquées par les unités des armées.

Selon le ministère des Armées, cet allègement ne pose pas de difficulté juridique puisque cette activité n'est pas attentatoire aux libertés publiques, les communications étant interceptables et enregistrables par n'importe quelle personne (radio-amateur par exemple) ou entité pourvu qu'elle dispose des moyens nécessaires et se cale sur les fréquences utilisées au moment opportun.

Ce contrôle sera mis en œuvre par le biais du contrôle internes aux armées qu'il relève du commandement hiérarchique direct, ou des missions des inspections de chacune des armées et de l'inspection des armées sollicitée par le ministre ou encore du contrôle général des armées.

Il est procèdé par ailleurs d'une certaine logique dans la mesure où la création de la CNCTR a répondu à un besoin spécifique de contrôle indépendant de l'usage par les services de renseignement des différentes techniques de renseignement et de respect de leurs champs d'application respectifs, contrôle qui perd de son sens à l'égard d'unités militaires qui ne pratiquent aucune autre technique de renseignement sur le territoire national.

La CNCTR est toutefois informée du champ et de la nature des mesures de surveillance mises en œuvre sur le fondement de cet article. Toutefois l'alinéa ne prévoit pas les modalités précises de cette information et notamment la capacité pour la CNCTR de se faire présenter sur place les capacités d'interception mises en œuvre comme prévu au deuxième alinéa de l'article L.854-9-3, **ni de solliciter du Premier ministre tous les éléments nécessaires à l'accomplissement de sa mission** y compris, à seule fin de s'assurer du respect des champs d'application mentionnés au premier alinéa de l'article 854-9-1, la communication des renseignements collectés et les transcriptions et extractions réalisées.

La CNCTR dans sa délibération n° 4/2017, tout en reconnaissant la légitimité de cette faculté dès lors qu'elle est limitée par la loi aux besoins de la défense militaire et de l'action de l'Etat en mer et a indiqué qu'elle veillera au respect de ce champ d'application particulier. La question reste de savoir si la qualité de l'information transmise lui permettra d'exercer un contrôle efficient. C'est pourquoi, il est préférable de prévoir dans le dispositif législatif de lui donner la possibilité de se faire présenter les capacités d'interception mises en œuvre, et, à la seule fin de s'assurer du respect du champ d'application, les renseignements collectés et les transcriptions réalisées. La CNCTR opérant en règle générale par sondage, ce mode de contrôle ne devrait pas constituer une charge lourde pour les

Armées. Cet ajout constituera un moyen de se prémunir contre d'éventuelles et mêmes très hypothétiques dérives (amendement ETRD.3).

(d) Le cas particulier des essais de matériels

Enfin l'article L. 2371-2 du code de la défense prévoit que le service chargé de la qualification des appareils et dispositifs techniques employés par les forces armées, la direction générale de l'armement (DGA), dispose lui aussi, pour l'exercice de cette mission, de l'autorisation légale prévue pour les militaires, réservée toutefois à la seule activité d'interception et aux seules fins de procéder aux tests de qualification des matériels utilisés par les forces armées et sans possibilité d'exploiter les interceptions à des fins de renseignement.

*

* *

Sur proposition de son rapporteur, la Commission des affaires étrangères, de la défense et des forces armées a adopté deux amendements.

Le premier, de coordination (ETRD.1), inscrit, par un article additionnel après l'article 8, au sein de l'article 6 *nonies* de l'ordonnance n° 58-1100 du 17 novembre 1958 consacré à la délégation parlementaire au renseignement, le fait qu'elle sera désormais destinataire des recommandations et observations que la CNCTR jugera nécessaire de lui transmettre au titre du contrôle de la mise en œuvre par les services de renseignement des dispositions du nouveau régime hertzien ouvert prévu au troisième alinéa du nouvel article L.854-9-3 du code de la sécurité intérieure.

Le second amendement (ETRD.3) prévoit une extension des moyens de la CNCTR concernant le contrôle du respect du champ d'application de l'article 9 par les militaires des armées. Il tend ainsi à lui donner la possibilité de se faire présenter sur place les capacités d'interception mises en œuvre et, pour s'assurer du respect du champ d'application, les renseignements collectés et les transcriptions et extractions réalisées.

La Commission des affaires étrangères, de la défense et des forces armées a donné un avis favorable à l'adoption du présent projet de loi.

EXAMEN EN COMMISSION

Réunie le mercredi 12 juillet 2017, sous la présidence de M. Christian Cambon, président, la commission des affaires étrangères, de la défense et des forces armées, a procédé à l'examen du rapport pour avis de M. Michel Boutant sur le projet de loi n° 587 (2016-2017) renforçant la lutte contre le terrorisme et la sécurité intérieure.

M. Christian Cambon, président. – Nous examinons à présent le rapport pour avis de M. Michel Boutant sur le projet de loi renforçant la lutte contre le terrorisme et la sécurité intérieure.

M. Michel Boutant, rapporteur pour avis. – En raison de la persistance du risque terroriste sur notre sol, le Gouvernement a demandé au législateur de proroger l'état d'urgence à six reprises depuis novembre 2015. La dernière prorogation, jusqu'au 1er novembre 2017, a été adoptée par le Sénat le 4 juillet dernier.

La mise en œuvre des mesures de police administrative prévues par la loi du 3 avril 1955 a constitué un instrument important de la stratégie antiterroriste des pouvoirs publics. La persistance de la menace depuis plus d'un an et demi conduit toutefois le Gouvernement à proposer aujourd'hui la création de nouvelles dispositions, permanentes cette fois. Il s'agit essentiellement de pérenniser les éléments les plus utiles de l'état d'urgence, tout en atténuant leur caractère attentatoire aux libertés publiques. La mise en place de périmètres de protection et de mesures individuelles de surveillance, la réalisation de perquisitions administratives – même si elles portent un autre nom – et la fermeture de lieux de culte deviendraient ainsi des possibilités permanentes, sous certaines conditions qui découlent notamment des décisions récentes du Conseil constitutionnel.

Outre ces dispositions, qui relèvent davantage de la commission des lois, le présent texte comporte deux dispositifs qui justifiaient la saisine de notre commission pour avis. Il s'agit d'une part du cadre juridique du fichier dit « PNR » (Passenger name record), créé par les articles 5 à 7 de la loi de programmation militaire du 18 décembre 2013. Les modifications ici proposées sont essentiellement liées à l'adoption récente de la directive européenne – tant attendue ! Il nous est en outre proposé de valider la création d'un PNR maritime simplifié. En second lieu, les articles 8 et 9 instaurent un nouveau régime légal de surveillance des communications hertziennes – pouvant notamment être mise en œuvre par les armées et par certains services de renseignement –, afin de tirer les conséquences d'une question prioritaire de constitutionnalité du 21 octobre 2016.

Quelques mots d'abord sur les articles 5 à 7 relatifs aux fichiers dits « PNR ». L'article 17 de la loi de programmation militaire de 2013 avait

rendu possible la création d'un tel fichier pour rassembler les données sur les passagers du transport aérien, pour la prévention et la constatation des infractions terroristes ou d'autres infractions très graves. La France anticipait ainsi le vote d'une directive européenne dont le projet avait été présenté dès février 2011. Ce système français de PNR permet soit de croiser les données des passagers avec celles d'un certain nombre de fichiers de police, soit, grâce à l'élaboration progressive de critères de dangerosité, d'identifier des profils dangereux. Actuellement, le fichier est en fin d'expérimentation et reçoit déjà 300 demandes par jour de la part des services utilisateurs. Ces demandes sont traitées par une « unité information passagers » (UIP) dont nous avons auditionné le directeur et dont l'effectif est de 35 personnes – 75 à terme.

Après des années de négociations, la directive PNR a enfin été adoptée le 27 avril 2016, obligeant tous les pays membres à se doter d'un tel fichier. Les dispositions du présent texte visent donc d'abord à pérenniser ce dispositif, qui n'avait été créé qu'à titre expérimental jusqu'au 31 décembre 2017 ; ensuite à se mettre en conformité avec le texte définitif de la directive. Fort heureusement, le PNR français s'est conformé dès le départ au projet de directive en cours de négociation, de sorte qu'il ne reste que quelques détails à corriger au sein du code de la sécurité intérieure, notamment en mettant à jour la liste des infractions visées.

Nous pouvons nous féliciter de cette nouvelle étape dans la mise en œuvre de cet instrument parmi les plus utiles dans la lutte contre les formes actuelles de terrorisme. Il faut toutefois souligner que la valeur ajoutée d'une approche communautaire réside surtout dans la possibilité, qui doit à présent constituer une priorité, d'organiser des échanges entre les PNR des États membres, dès que ceux-ci s'en seront dotés. Actuellement, la France peut déjà coopérer avec le Royaume-Uni, avec la Roumanie et avec la Hongrie. L'Allemagne devrait rejoindre ces pays courant 2018, ainsi que l'Espagne. Il sera cependant nécessaire d'inciter l'Italie à poursuivre ses efforts dans ce domaine, tandis que la Grèce a malheureusement pris du retard pour des raisons essentiellement financières.

Deuxième apport du texte dans ce domaine, l'ébauche de la création d'un PNR maritime. Le projet de loi ne fait ici que développer des dispositions déjà créées par la loi du 20 juin 2016 pour l'économie bleue. Il s'agit de prévenir d'éventuels actes terroristes à bord des navires, ainsi que de mieux connaître les routes maritimes empruntées par des personnes à risque.

Ce nouveau fichier concernera les passagers au départ et à l'arrivée des liaisons France/France, France/étranger ou étranger/France, à bord des navires battant pavillon français ou étranger. Ceci recouvre à la fois des liaisons maritimes régulières par ferries et des activités de croisières saisonnières, pour un volume annuel global de 32,5 millions de passagers,

dont 17 millions environ pour le trafic transmanche et 4 millions pour les liaisons régulières entre la Corse et le continent.

Le dispositif est moins complexe et moins coûteux que le PNR aérien. Il se limitera, au moins dans un premier temps, à un effort de standardisation des données déjà collectées par les compagnies maritimes lors des enregistrements, puis à des modalités de transfert facilitées aux services de sécurité pour qu'ils puissent consulter les fichiers de police. Comme dans le cas du PNR aérien, l'efficacité de ce système serait nettement améliorée en cas de coopération entre les pays membres. À l'heure actuelle, le Royaume-Uni, l'Espagne, la Finlande, le Danemark et la Belgique disposent de systèmes plus ou moins avancés. Il faut donc encourager ces pays et les autres partenaires européens de la France à poursuivre leurs efforts dans ce domaine.

J'en viens maintenant aux dispositions concernant l'« exception hertzienne ». N'étant pas un spécialiste, j'ai participé aux auditions réalisées par la commission des lois et pris l'initiative de consulter des ingénieurs et les magistrats de la CNCTR… Comme vous le savez, la loi du 10 juillet 1991 sur les interceptions de sécurité avait choisi de les exclure en leur donnant une base légale mais ne les soumettant à aucune procédure d'autorisation ni de contrôle. Or le spectre hertzien est très large et nous concerne tous : radioamateurs ou professionnels, bluetooth, réglage des montres électroniques…

L'instauration de cette « exception » était justifiée par le fait que les opérations correspondantes consistaient en une surveillance générale du domaine radioélectrique sans viser des communications individualisables. Même si elles ne portent pas sur des moyens de communication majoritairement utilisées, la surveillance des communications hertziennes est utile notamment dans le domaine militaire, du contre-espionnage et parfois dans le cadre de la lutte contre la grande criminalité et de la lutte anti-terroriste. L'hertzien constitue un moyen discret de transmission d'ordres – en haute ou basse fréquence, comme c'est le cas dans le domaine militaire – et un moyen de communication dans l'action – par talkies-walkies par exemple. Il est très utile également dans les zones dépourvues d'infrastructures de télécommunication.

Lors de l'examen de la loi relative au renseignement de juillet 2015 et de celle sur la surveillance des communications électroniques internationales de novembre 2015, il a été décidé de maintenir ce régime dit de l'« exception hertzienne ». Après les avis rendus par la CNCIS et la CNCTR, le Conseil constitutionnel, saisi sur le fondement d'une QPC posée par des associations en octobre 2016, a jugé ce dispositif non conforme à la Constitution. Il a en effet considéré que dès lors que peuvent être interceptées des communications individualisables, les dispositions portent une atteinte au droit au respect de la vie privée et au secret des correspondances. Il a donné au législateur jusqu'au 31 décembre 2017 pour remédier à cette situation et

demandé à la CNCTR de mettre en place avant cette date un dispositif transitoire. La CNCTR a recommandé diverses procédures au Premier ministre.

Le projet de loi, aux articles 8 et 9 vise donc à établir une législation conforme à la Constitution. D'une part, il valide l'interprétation de la CNCIS et de la CNCTR s'agissant des communications mixtes utilisant la voie hertzienne sur un segment seulement ou transitant par un opérateur, les assimilant aux techniques visées par les lois de 2015 et les soumettant donc au régime d'autorisation du Premier ministre avec intervention pour avis et/ou contrôle de la CNCTR. D'autre part, il distingue les correspondances échangées au sein d'un réseau conçu pour une utilisation privative par une personne ou un groupe fermé d'utilisateurs et crée donc une cinquième technique de renseignement qui sera soumise au régime d'autorisation de droit commun par le Premier ministre et de contrôle par la CNCTR, et aux mêmes règles d'exploitation et de conservation des données recueillies.

La grande majorité des interceptions réalisées sur les communications hertziennes sont donc soumises au régime de droit commun, ce qui constitue une avancée importante du contrôle sur les services pour le bon respect de la vie privée et des libertés.

S'agissant ensuite, à titre résiduel, des communications empruntant exclusivement la voie hertzienne et n'impliquant pas l'intervention d'un opérateur de communications électroniques, elles sont transmises de façon ouverte, c'est-à-dire qu'elles peuvent être captées et enregistrées par n'importe quelle personne, pourvu qu'elle soit dotée d'un appareil de réception des fréquences d'émissions – appareil en vente libre utilisé par les radioamateurs, les cibistes, les utilisateurs de talkies-walkies analogiques, mais aussi les utilisateurs de radio VLF, HF ou les moyens militaires de communication tactique.

Le projet de loi confirme la légalité des interceptions par les services de renseignement et par les unités militaires dans le cadre de leur mission de défense militaire : dissuasion, postures permanentes de sûreté aérienne et de sauvegarde maritime, action de l'État en mer. Il n'instaure pas de dispositifs d'autorisation du Premier ministre, mais les soumet à un régime allégé d'obligations : durée de conservation maximale de six ans, transcriptions et extractions conformes aux finalités inscrites dans la loi relative au renseignement, principe de destruction de ces transcriptions et extractions. Il confie en outre à la CNCTR la mission de veiller au respect des champs d'application respectifs des techniques de droit commun et du régime spécifique – hertzien ouvert – ainsi créé. Pour ce faire, la CNCTR est informée du champ et de la nature des mesures prises.

L'article 8 du projet de loi prévoit que la CNCTR peut se faire présenter par les services de renseignement les capacités d'interception mises en œuvre, et solliciter du Premier ministre tous les moyens

nécessaires, y compris pour s'assurer le respect des champs d'application respectif, obtenir la communication des renseignements collectés et les transcriptions et extractions réalisés. Elle peut aussi formuler des recommandations et observations adressées au Premier ministre et à la Délégation parlementaire au renseignement.

Ces deux dernières dispositions ne sont pas incluses dans l'article 9 s'agissant des unités militaires. En effet, le Gouvernement, notamment le ministère des armées, - je vous livre son point de vue - considère que les éléments étant accessibles par tout le monde, il ne peut y avoir atteinte à la vie privée ou aux libertés ; il estime en outre que la mise en œuvre du contrôle de la CNCTR est potentiellement lourde, notamment dans un contexte opérationnel, et que le contrôle interne par les corps d'inspection de chacune des armées et l'inspection générale des armées est suffisant. Enfin, le Gouvernement considère que la CNCTR a été créée pour répondre au besoin spécifique de contrôle indépendant de l'usage par les services de renseignement des différentes techniques de renseignement et de respect de leurs champs d'application respectifs, contrôle qui perd de son sens à l'égard d'unités militaires qui ne pratiquent aucune autre technique de renseignement sur le territoire national.

Au demeurant, les missions des armées dans la défense du territoire ne sont pas des missions de renseignement – au sens de surveillance administrative – et n'entrent donc pas dans le domaine du code de la sécurité intérieure. Les activités de renseignement dans ce domaine sont plus à considérer comme des activités d'autoprotection ou d'alerte avancée que des missions de surveillance en vue d'acquérir une connaissance sur un adversaire – ce que fait en revanche la DRM qui est un service de renseignement. Il s'agit pour les armées d'être capables en permanence de détecter une menace hostile à proximité ou dans notre espace aérien ou nos eaux territoriales afin de réagir dans les plus brefs délais.

Saisie pour avis, la CNCTR a émis une délibération le 9 juin 2017 dont nombre de recommandations ont été reprises, mais s'agissant des moyens à sa disposition pour réaliser le contrôle du respect des champs d'application, elle considère qu'elle doit disposer de la faculté d'agir de sa propre initiative sans avoir à solliciter le Premier ministre – ce qui fait l'objet d'un amendement du rapporteur de la commissions des lois - et qu'elle devra veiller au respect du champ particulier d'interventions des militaires des armées, à savoir les besoins de la défense militaire et de l'action de l'État en mer.

Pour ce faire, même si la CNCTR ne l'a pas explicitement demandé dans sa délibération, il me semble qu'elle devrait disposer de la capacité de se faire présenter sur place les capacités d'interception mises en œuvre et, à la seule fin de s'assurer du respect du champ d'application, les renseignements collectés et les transcriptions et extractions réalisées.

Le projet de loi constitue une avancée significative dans la protection de la vie privée et des libertés publiques, puisqu'il étend de manière considérable le périmètre de contrôle de la CNCTR, et il répond aux objections du Conseil constitutionnel. Je propose donc à la commission un avis favorable à son adoption. Néanmoins, je ne verrais que des avantages à soumettre l'ensemble au contrôle de la CNCTR ce qui constituerait une garantie de son bon fonctionnement et un moyen de se prémunir contre d'éventuelles et même très hypothétiques dérives. Nous moderniserions ainsi notre démocratie ; la confiance placée dans notre armée ne fait pas obstacle à la réalisation d'échantillonnages ponctuels dans certains services pour prévenir tout débordement. D'où les deux amendements que je vous propose.

Le premier amendement ETRD.1, de pure coordination, inscrit dans l'article de l'ordonnance du 17 novembre 1958 consacré à la délégation parlementaire au renseignement, comme nous le faisons régulièrement, le fait qu'elle sera désormais destinataire des recommandations et observations que la CNCTR jugera nécessaire de lui transmettre au titre du contrôle de la mise en œuvre par les services de renseignement des dispositions du nouveau régime hertzien ouvert.

L'amendement proposé à l'article 9 ETRD.3 étend les moyens de la CNCTR concernant le respect du champ d'application de l'article 9 par les militaires des armées. Il consiste à lui donner la possibilité de se faire présenter sur place les capacités d'interception mises en œuvre et pour s'assurer le respect du champ d'application, celle de se faire présenter également les renseignements collectés et les transcriptions et extractions réalisées, comme dans celui déposé par le rapporteur de la commission des lois Michel Mercier à l'alinéa 14 de l'article 8

Avant la loi sur le renseignement de juillet 2015, les services de renseignement agissaient dans un cadre peu régulé. Ils sont dotés d'un cadre légal solide, destiné à éviter que leurs activités soient juridiquement contestées et soumises à la critique. Nous complétons et rendons ce cadre plus efficace encore, sans freiner pour autant le travail des services de renseignement.

M. Christian Cambon, président. – Merci pour cet éclairage précis sur ce texte technique.

M. André Trillard. – Le mieux est parfois l'ennemi du bien. Ce sujet devient d'une complexité effrayante. Des moyens de surveillance sont utilisés par les militaires à des fins opérationnelles de défense du territoire national et de ses approches. Sachons fixer des limites à un contrôle administratif pesant. Les unités militaires, qui agissent pour notre protection contre des menaces militaires, devraient être exclues du dispositif. Je ne suis pas du tout favorable à ce genre d'amendements, qui partent sans doute

d'une bonne intention. Faisons confiance à nos officiers plutôt que de soumettre nos militaires à une surveillance bureaucratique.

M. Michel Billout. – Mon groupe n'ayant pas voté la loi de 2015, nous serons peu enclins à voter celle-ci… Nous nous exprimerons plus longuement en séance et, pour l'heure, nous nous abstiendrons sur ces amendements, comme sur le texte qui nous est soumis en commission.

La commission adopte les deux amendements présentés.

ANNEXE 1 -
AMENDEMENTS PRÉSENTÉS PAR LA COMMISSION DES AFFAIRES ÉTRANGÈRES, DE LA DÉFENSE ET DES FORCES ARMÉES

Article additionnel après l'article 8

Après l'article 8

Insérer un article additionnel ainsi rédigé :

Après le 5 ° du I de l'article 6 *noniès* de l'ordonnance n°58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires**,** insérer l'alinéa suivant :

« 6° Les observations que la Commission nationale de contrôle des techniques de renseignement adresse au Premier ministre en application de l'article L.854-9-3 du même code. »

Article 9

Alinéa 3

Remplacer les mots :

"*mises en œuvre sur le fondement du présent article*"

par les mots :

"p*rises en application du présent article. Elle peut également se faire présenter sur place les capacités d'interception mises en œuvre et, à la seule fin de s'assurer du respect du champ d'application mentionné au premier alinéa, les renseignements collectés et les transcriptions et extractions réalisées*".

ANNEXE 2 -
LISTE DES PERSONNES AUDITIONNÉES

Auditions conjointes avec le rapporteur au fond de la commission des lois

28 juin 2017

M. Francis Delon, président de la Commission nationale de contrôle des techniques de renseignement (CNCTR) et **M. Marc Antoine**, conseiller auprès du président.

M. Olivier Bardin, directeur de l'Unité Information Passagers (UIP) du système PNR (Passenger name record).

Mme Claire Landais, directrice des affaires juridiques du ministère des armées, **M. Mathieu Rhee**, chef du bureau des données personnelles de cette direction, **M. Éric Vidaud,** chef du bureau des affaires réservées et **M. Christophe Junqua**, adjoint au chef du bureau, **Mme Animya N'Tchandy**, conseillère parlementaire au cabinet du ministre des armées, ainsi que des représentants de la direction générale des services extérieures et de la direction du renseignement militaire.

6 juillet 2017

M. Pierre Bousquet de Florian, coordonnateur national du renseignement et de la lutte contre le terrorisme et **Mme Agnès Deletang**, conseillère juridique.

ANNEXE 3

Régimes applicables aux différents modes de communication par voie hertzienne dans le projet de loi déposé par le gouvernement

Régimes applicables	**Régime de droit commun** des interceptions de sécurité (art. L 852-1) ou du recueil et de la captation de données informatiques (art L. 853-2) ou de surveillance internationale (L. 854-1 et suiv.)	**Régime spécifique hertzien** (art. L.852-2 ou 853-2) rattaché au régime de droit commun (5ème technique)	**Régime hertzien « ouvert » allégé** (art. L. 854-9-1 et suiv. du code de la sécurité intérieure, art. L 2371-1 du code de la défense s'agissant des missions opérées par des unités militaires
Modes de communication hertzienne	Non exclusivement hertzien et/ou intervention d'un opérateur de communication électroniques exploitation un réseau ouvert au public	Exclusivement hertzien, sans intervention d'un opérateur de communication électroniques exploitation un réseau ouvert au public, lorsque le réseau est conçu pour une utilisation privative ou un groupe fermé d'utilisateurs	Exclusivement hertzien, sans intervention d'un opérateur de communication électroniques exploitation un réseau ouvert au public, usage, utilisation non privative, non couverte par le régime applicable aux autres techniques de renseignement
Trafic entre terminal et borne Wifi ou Wimax	X (si via Internet)	X (si non relié à Internet)	
Téléphones sans fil	X (via opérateur)	X (entre deux pièces)	
Radioamateurs, Cibistes, Talkies-Walkies analogiques			X
PMR (talkies-walkies numériques)		X	
Téléphones satellitaires	X (principalement L.854-1)	X (en direct entre deux téléphones satellitaires)	
Téléphones mobiles et ordinateurs portables GSM/3G/4G	X		

Bluetooth		X	
Trafic entre objets connectés et borne		X	
GPS	(idem L.851-5 balises)		
Radio VLF et HF et moyens militaires tactiques			X