N° 161

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUINZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 14 septembre 2017.

AVIS

FAIT

AU NOM DE LA COMMISSION DE LA DÉFENSE NATIONALE ET DES FORCES ARMÉES
SUR LE PROJET DE LOI (n° 104), ADOPTÉ PAR LE SÉNAT APRÈS ENGAGEMENT DE LA PROCÉDURE ACCÉLÉRÉE,
renforçant la **sécurité intérieure** *et la* **lutte** *contre le* **terrorisme**,

PAR M. Guillaume GOUFFIER-CHA,

Député.

Voir les numéros :

Sénat : 1ère lecture : **587, 629, 630, 636** et TA **115 (2016-2017).**

Assemblée nationale : **164.**

SOMMAIRE

___

Pages

INTRODUCTION

La menace terroriste reste grave en France ainsi que l'ont notamment démontré, en 2017, les attaques du Carrousel du Louvre et de Levallois-Perret, qui ont pris pour cible des militaires, l'attaque des Champs-Élysées au cours de laquelle un policier a trouvé la mort et, encore récemment, le projet d'attentat, heureusement déjoué, en préparation à Villejuif. Elle l'est également à l'étranger et notamment chez nos amis et alliés européens, comme l'ont douloureusement rappelé les attaques qui ont frappé la Suède, à Stockholm, le Royaume-Uni, à Londres – par trois fois –, et à Manchester, l'Allemagne, à Hambourg, l'Espagne à Barcelone et Cambrils, et la Finlande, à Turku.

C'est dans ce contexte que le Gouvernement a présenté, dès juin 2017, un projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme. Un texte nécessaire car il nous permet de sortir de l'état d'urgence, qui doit rester un état d'exception, et responsable car à l'équilibre entre la protection des libertés publiques et la garantie de la sécurité des Françaises et des Français.

Au-delà des dispositions intégrant dans le droit commun, en les adaptant, certaines mesures jusqu'alors exceptionnelles mises en œuvre dans le cadre de l'état d'urgence [(1)] prorogé à six reprises par le Parlement depuis le 14 novembre 2015, le présent projet de loi comporte un certain nombre de mesures concernant la défense nationale.

C'est pourquoi notre commission a décidé de se saisir, pour avis, des articles 5 à 7 et 8 à 9 du projet de loi, lesquels concernent les deux domaines suivants :

– les systèmes de traitement des données API et/ou PNR (articles 5 à 7) ;

– les techniques de renseignement (articles 8 à 9).

Les articles 5 à 7 visent à pérenniser les systèmes expérimentaux actuellement en vigueur dans le domaine aérien et dans le domaine maritime, et qui arrivent à échéance au 31 décembre 2017. Deux dispositifs qui ont démontré leur utilité pour nos services de renseignement pour prévenir et détecter les formes les plus graves de criminalité : actes terroristes, traite d'êtres humains, trafic d'armes par exemple.

Pour ce qui concerne le domaine aérien, il s'agit en outre d'assurer la transposition de la directive 2016/681 dite directive PNR [(2)], afin de mettre le droit

(1) Cf. loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence.

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

national et le système « API-PNR aérien » français en conformité avec le droit communautaire. Pour ce qui concerne le domaine maritime, il s'agit d'autoriser la création d'un système automatisé de traitement des données passagers – le « PNR maritime » –, distinct de celui mis en place dans le secteur aérien. Ces deux systèmes ont les mêmes finalités – la lutte contre les actes de terrorisme, contre les formes de criminalités les plus graves, et contre les atteintes aux intérêts fondamentaux de la Nation – et constituent des outils précieux tant pour les services habilités à y recourir que pour la justice.

Par ailleurs, les articles 8 à 9 redéfinissent le régime légal de surveillance des communications hertziennes afin de mettre le droit en conformité avec une récente censure du Conseil constitutionnel. Dès lors que les mesures de surveillance du domaine hertzien peuvent notamment être mises en œuvre par les armées et les services de renseignement relevant du ministère des Armées, il était légitime que la commission de la Défense se saisisse de ces articles afin de garantir, à l'avenir, un régime juridique à la fois sécurisant pour nos forces et nos services pour la bonne conduite de leurs missions, mais également respectueux des droits et libertés garantis par notre Constitution.

LES DISPOSITIONS DU PROJET DE LOI

I. LES DISPOSITIONS RELATIVES AUX SYSTÈMES API ET PNR

Le projet de loi comporte trois articles 5 à 7 relatifs aux systèmes de traitement de données API [(1)] et/ou PNR [(2)]. Deux concernent le domaine aérien, le troisième ayant trait au domaine maritime.

A. LA PÉRENNISATION ET L'ADAPTATION DU SYSTÈME « API-PNR AÉRIEN FRANCE » AU DROIT DE L'UNION EUROPÉENNE

Les articles 5 et 6 ont trait au système « API-PNR aérien ». Ils visent :

– d'une part, à **pérenniser le système actuellement en vigueur** et qui arrive à échéance à la fin de l'année 2017 ;

– d'autre part, à **mettre en conformité le droit national avec le droit communautaire** à la suite de l'adoption définitive de la directive dite PNR, la transposition d'une directive constituant une obligation communautaire en vertu des traités, ainsi qu'une exigence constitutionnelle [(3)].

Il s'agit de permettre aux différents services de sécurité et de renseignement concernés d'utiliser ce système de suivi des données des passagers aux fins de prévenir et détecter un certain nombre d'actes pénalement répréhensibles parmi les formes les plus graves de criminalité (infractions terroristes notamment).

1. La pérennisation du système (article 5)

L'article 17 de la loi n° 2013-1168 de programmation militaire 2014-2019 [(4)] avait prévu la création, à titre expérimental jusqu'au 31 décembre 2017, d'un nouveau système automatisé de traitement des données API et PNR (système « API-PNR France » dont le fonctionnement est détaillé ci-après). Ce dispositif avait été codifié à l'article L. 232-7 du code de la sécurité intérieure.

L'article 5 du projet de loi procède simplement à l'**abrogation du II de l'article 17 précité, permettant ainsi la pérennisation de ce système** dont le régime est modifié par l'article 6 du projet de loi afin de le mettre en conformité

(1) Advanced Passenger Information*, données d'enregistrement et d'embarquement.*
(2) Passenger Name Record*, données de réservation.*
(3) Cf. notamment Conseil constitutionnel, décision n° 2004-496 DC du 10 juin 2004.
(4) 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.

avec la directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016.

Le commentaire ci-après de l'article 6 du projet de loi donne une présentation plus précise du système « API-PNR aérien » et des évolutions prévues au titre de la transposition de la directive.

2. L'adaptation au droit de l'Union européenne (article 6)

L'article 6 du projet de loi a pour objet de mettre en conformité avec le droit européen le régime français relatif aux fichiers de réservation et d'enregistrement des passagers aériens, en transposant la directive précitée du 27 avril 2016 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.

a. Le régime français actuel : principes et finalités

i. Définitions préalables

Les **données PNR**, pour *Passenger Name Record*, ou **« données de réservation »**, regroupent l'ensemble des informations fournies par une personne physique ou un opérateur [(1)] lors de la réservation d'un voyage auprès d'un transporteur aérien. Il s'agit d'**informations déclaratives**, recueillies à l'origine par les opérateurs à des fins commerciales. Leur fiabilité n'est donc pas systématiquement garantie.

Les **données API**, pour *Advanced Passenger Information*, ou **« données d'enregistrement et d'embarquement »**, sont collectées, comme leur nom l'indique, lors de l'enregistrement et de l'embarquement des passagers. Il s'agit des données contenues sur la bande de lecture optique du passeport et de certaines données relatives aux vols empruntés.

Les données PNR et API se recoupent partiellement (items totalement partagés, ou similaires) mais ne se confondent pas, ainsi qu'en témoigne le tableau suivant.

(1) Transporteur aérien, opérateur de séjour ou de voyage affrétant un aéronef notamment.

COMPARAISONS DES DONNÉES PNR ET API

Données PNR	Données API
1. Code repère du dossier passager	
2. Date de réservation/d'émission du billet	
3. Date(s) prévue(s) du voyage	
4. Nom(s), prénom(s), date de naissance	2. Nationalité, nom, prénom, date de naissance, sexe
5. Adresse et coordonnées (numéro de téléphone, adresse électronique)	
6. Moyens de paiement, y compris l'adresse de facturation	
7. Itinéraire complet pour le dossier passager concerné	
	3. Point de passage frontalier utilisé pour entrer sur le territoire français ou en sortir
	4. Point d'embarquement initial et de débarquement final des passagers
	5. Point de départ et d'arrivée du vol
	6. Code de transport (numéro du vol et code du transporteur aérien)
	7. Date du vol
	8. Heures de départ et d'arrivée du transport
8. Informations « grands voyageurs » tels que les programmes de fidélité	
9. Agence de voyages/agent de voyages	
10. Statut du voyageur tel que confirmation, enregistrement, non-présentation, passager de dernière minute	9. Statut de la personne embarquée (membre d'équipage, passager : toute information sur les correspondances)
	10. Numéro d'identification du passager
	11. Numéro et type du document de voyage utilisé
	12. Date d'expiration du document de voyage
	13. État ou organisation émetteur du document de voyage
11. Indications concernant la scission/division du dossier passager	
12. Toute autre information, à l'exclusion des données à caractère personnel visées au second alinéa du I de l'article L. 232-7 du code de la sécurité intérieure (1)	
13. Établissement des billets (numéro du billet, date d'émission, allers simples, décomposition tarifaire)	
14. Numéro du siège	
15. Informations sur le partage de code	
16. Toutes les informations relatives aux bagages	15. Nombre, poids et identification des bagages
17. Nombre et autres noms de voyageurs figurant dans le dossier passager	16. Nombre total des personnes transportées dans l'aéronef
18. Tout renseignement préalable sur les passagers (API) qui a été collecté	
19. Historique complet des modifications des données PNR précitées	

Source : rapporteur pour avis, d'après les données de la Commission nationale de l'informatique et des libertés.

(1) Données susceptibles de susceptibles de révéler l'origine raciale ou ethnique d'une personne, ses convictions religieuses ou philosophiques, ses opinions politiques, son appartenance à un syndicat, ou les données qui concernent la santé ou la vie sexuelle de l'intéressé.

ii. La mise en place du régime français actuel s'est fondée sur deux directives européennes.

● Dans un premier temps, afin d'améliorer les contrôles aux frontières et de lutter contre l'immigration clandestine, l'Union européenne avait adopté la **directive 2004/82/CE** [(1)] qui :

– oblige les transporteurs à transmettre aux États membres les renseignements relatifs aux passagers qu'ils vont transporter ;

– permet aux États membres de créer des traitements automatisés de données à caractère personnel recueillies à l'occasion de déplacements internationaux en provenance ou à destination d'États n'appartenant pas à l'Union européenne, **à l'exclusion des déplacements intra-communautaires**.

En application de l'article 6 de la directive, les données personnelles pouvaient également être utilisées par les États membres « *pour répondre aux besoins des services répressifs* ».

Sur ce fondement, la France a d'abord procédé à la création de plusieurs fichiers à l'occasion de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers [(2)]. En application de ces dispositions législatives, le fichier dénommé système européen de traitement des données d'enregistrement et de réservation **(SETRADER)** a été créé, **alimenté par les seules données API**, aux fins de prévenir et réprimer l'immigration clandestine, les actes de terrorisme, et d'assurer le contrôle aux frontières [(3)].

● Dans un second temps, en février 2011, la Commission européenne a présenté un projet de directive sur le PNR européen (directive dite PNR). Il prévoyait que les transporteurs aériens fourniraient aux États membres les données contenues dans le dossier de voyage de chaque passager empruntant un vol international à destination ou en provenance de l'Union européenne. Ces données seraient exploitées par les États membres pour prévenir et détecter les infractions terroristes et les formes graves de criminalité.

Le processus d'adoption de la directive PNR s'étant révélé long et complexe – le texte final est celui de la directive 2016/681 dont l'article 6 du projet de loi assure la transposition – **la France a choisi de mettre en place, à titre expérimental jusqu'au 31 décembre 2017, un système de traitement de données à caractère personnel concernant les données API et PNR fondé sur les dispositions de la proposition de directive.**

---

(1) Directive 2004/82/CE du Conseil concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers.

(2) Dispositions codifiées aux articles L. 232-1 à L. 232-6 du code de la sécurité intérieure.

(3) Arrêté du 11 avril 2013 portant autorisation d'un traitement automatisé de données à caractère personnel dénommé SETRADER.

Prévu par l'article 17 de la loi n° 2013-1168 de programmation militaire 2014-2019 et placé sous la responsabilité du ministre de l'Intérieur, du ministre des Armées, du ministre chargé des transports et du ministre chargé des douanes, ce système « API-PNR France » [(1)] a pour objet de prévenir et réprimer les actes de terrorisme, les atteintes aux intérêts fondamentaux de la Nation, et les infractions pour lesquelles un mandat d'arrêt européen peut être émis [(2)].

iii. Fonctionnement du système « API-PNR France »

● Dans le cadre du système « API-PNR France », codifié à l'article L. 232-7 du code de la sécurité intérieure, **les transporteurs sont tenus de transmettre à un service à compétence nationale dénommé « Unité Information Passagers » (UIP) les données** pour l'ensemble des vols à destination et en provenance du territoire national, à l'exception des déplacements reliant deux points de la France métropolitaine. Sont donc concernés **les vols internationaux, les vols intra-européens, ainsi que les vols en provenance et à destination des collectivités et territoires ultramarins.**

L'UIP est rattachée au ministère chargé des douanes. Seuls les personnels qui y sont affectés et qui sont individuellement désignés et spécialement habilités par le directeur de l'UIP ont accès aux informations figurant dans le système. **Les différents services de police, de gendarmerie et de renseignement** – limitativement énumérés et pour des finalités expressément prévues [(3)] – susceptibles d'utiliser ces informations **ne peuvent interroger directement le fichier**. **Ils doivent adresser des requêtes à l'UIP**, auxquelles les personnels habilités répondent après en avoir vérifié la conformité au regard des attributions légales des services concernés dans le cadre des finalités prévues. Chaque requête doit préciser la période de temps demandée et peut porter sur les éléments suivants : zones géographiques, vols, personnes, catégories de données.

● **L'exploitation des données** contenues dans le système s'effectue, dans le cadre des finalités prévues, selon les **deux modalités** suivantes :

– par **criblage** des individus et des objets, technique qui consiste à croiser les informations API-PNR avec certains fichiers relatifs à des personnes ou des objets recherchés ou surveillés (fichier des personnes recherchées – FPR, fichier des objets et des véhicules signalés – FOVeS, système d'information Schengen II – SIS II, système informatisé de lutte contre les fraudes – SILCF,

(1) 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.

(2) Pour les agissements punis d'une peine privative de liberté d'une durée égale ou supérieure à trois ans d'emprisonnement ou d'une mesure de sûreté privative de liberté d'une durée similaire et entrant dans l'une des 32 catégories d'infractions prévues par l'article 694-32 du code de procédure pénale (exemples : traite des êtres humains, trafic d'armes, de munitions et d'explosifs ou encore blanchiment des produits du crime).

(3) Article R. 232-15 du code de la sécurité intérieure.

base de données ASF-SLTD [1] d'Interpol sur les documents de voyage volés et perdus) ;

– par **ciblage** des individus et des objets, avec l'application de grilles d'analyse des risques comprenant différents critères et leur pondération, par exemple l'existence de trajets atypiques : passager se présentant à l'embarquement sans avoir réservé (« *go-show* ») ou, au contraire ne s'y présentant pas après avoir réservé (« *no-show* »), fractionnement volontaire d'un itinéraire en plusieurs dossiers de réservation (vols dits « risés »), etc. Élaborés par les services intéressés, ces profils sont validés – ou non – par l'UIP.

Sont naturellement exclues du système « API-PNR France » les données à caractère personnel les plus sensibles, susceptibles de révéler l'origine raciale ou ethnique d'une personne, ses convictions religieuses ou philosophiques, ses opinions politiques, son appartenance à un syndicat, ou les données qui concernent la santé ou la vie sexuelle d'un individu [2].

● Les **données sont conservées pendant une période de cinq ans** à compter de leur réception dans le système. **Les données susceptibles de révéler l'identité des passagers font l'objet d'un traitement spécifique (masquage) : à l'issue d'un délai de deux ans**, elles sont conservées mais ne peuvent plus être communiquées aux agents appartenant aux services demandeurs, sauf autorisation expresse du directeur de l'UIP après formulation d'une demande motivée. **En application du point 2 de l'article 12 de la directive 2016/681, ce délai sera réduit à six mois.**

D'après les informations fournies par le directeur de l'UIP, la collecte des données API-PNR concerne, à l'heure actuelle, 78 compagnies aériennes représentant 92 % des vols commerciaux extra-UE et 60 millions de voyageurs. À terme, le flux annuel atteindra 100 millions de dossiers passagers.

b. La transposition de la directive 2016/681 : des ajustements marginaux du système français

i. Les principales dispositions de la directive

● Aux termes de l'article 18 de la directive 2016/681, **les États membres doivent transposer celle-ci au plus tard le 25 mars 2018**.

Les principales dispositions de la directive sont les suivantes :

– **l'obligation faite aux transporteurs aériens de transmettre les données PNR de leurs passagers aux UIP de tous les États-membres concernés par les vols extra-UE** (décollage ou atterrissage au sein d'un État membre à destination ou en provenance d'un pays tiers, ou escale dans un ou plusieurs États membres) ;

(1) Automated Search Facility – Stolen and Lost Travel Documents.
(2) Alinéa 2 de l'article L. 232-7 du code de la sécurité intérieure.

– **l'autorisation donnée aux États membres d'étendre cette obligation à tout ou partie des vols intra-UE**, sous réserve d'en notifier la Commission européenne [(1)] ;

– **l'obligation faite aux États membres de mettre en œuvre des traitements de données à caractère personnel alimentés par les informations PNR** aux seules fins de prévenir et détecter les infractions terroristes et les formes graves de criminalité et de permettre les enquêtes et les poursuites en la matière.

En termes de procédure pour le transfert et l'accès aux données, l'article 8 de la directive retient la méthode dite « *push* », selon laquelle les opérateurs concernés transmettent les données PNR à l'autorité requérante. L'autre méthode, dite « *pull* », aurait permis aux autorités compétentes d'un État membre d'accéder directement au système de réservation d'un opérateur pour en extraire une copie des données. De fait, la méthode « *push* » offre un niveau de protection des données plus élevé, les opérateurs gardant le contrôle sur les données transmises. C'est également la méthode qui est actuellement retenue par le système français.

Naturellement, **le système atteindra sa pleine efficacité dès lors que chacun des États membres aura mis en œuvre son propre traitement national** en l'étendant, le cas échéant, aux vols intra-UE. L'article 9 de la directive prévoit d'ailleurs des modalités d'échange d'informations entre États membres.

● **La France s'étant, à l'époque, fortement inspirée du projet de directive pour mettre en place son système expérimental national, seuls des ajustements marginaux sont à opérer** afin d'assurer cette transposition. Il s'agit :

– d'adapter les finalités du système PNR national au cadre de la directive ;

– et de donner aux autorités publiques la possibilité de soumettre d'autres opérateurs à l'obligation de transmission des données, ainsi que le permet la directive.

ii. L'adaptation des finalités du système : la définition des formes de criminalité concernées par le système PNR

● **L'alinéa 5 de l'article 6** du projet de loi autorise les ministres de l'Intérieur et des Armées ainsi que les ministres chargés des transports et des douanes à mettre en œuvre un système automatisé de données, conformément aux exigences de la directive. Tel est déjà le cas actuellement sous l'empire du système national expérimental.

● **L'alinéa 6** procède à la première et principale modification de fond du système national, qui concerne les finalités du fichier.

(1) Article 2 de la directive (UE) 2016/681.

En l'état du droit en vigueur, le système « API-PNR France » permet la prévention et la répression des actes de terrorisme, des atteintes aux intérêts fondamentaux de la Nation et des infractions pour lesquelles un mandat d'arrêt européen peut être émis en application de l'article 695-23 du code de procédure pénale.

La **directive 2016/681 retient un champ plus restreint**, en limitant le recours au système PNR aux seules fins de **prévenir et détecter les infractions terroristes et les « formes graves de criminalité » passibles d'une peine privative de liberté ou d'une mesure de sûreté d'une durée maximale d'au moins trois ans au titre du droit national d'un État membre** (1). Elle établit la liste de ces « formes graves de criminalité » en procédant par renvoi à son annexe II, laquelle ne couvre pas l'ensemble des infractions mentionnées à l'article 695-23 du code de procédure pénale (2).

L'alinéa 6 renvoie donc à l'annexe II de la directive pour établir la liste des formes graves de criminalité que l'utilisation du système PNR a vocation à prévenir et détecter**.**

S'y ajoutent, naturellement, les actes de terrorisme – prévus par l'article premier de la directive – **ainsi que** les **« atteintes aux intérêts fondamentaux de la Nation »**. Cette finalité est déjà prévue dans le cadre du système national actuel. Il s'agit d'une notion bien connue en droit français prévue à l'article 410-1 du code pénal (3), absente du texte de la directive mais parfaitement conforme à celle-ci. Le Conseil d'État (4) a en effet estimé qu'un tel ajout n'était pas contraire au droit de l'Union européenne dès lors que la défense des intérêts fondamentaux de la Nation ne relève pas de la compétence de l'UE mais de chaque État membre de manière souveraine (article 3 du Traité sur le fonctionnement de l'Union européenne).

● Constatant que le renvoi direct à l'annexe II de la directive ne faisait pas formellement apparaître le quantum de peine minimal de trois ans pour qu'une infraction soit incluse dans son champ d'application, le Sénat a adopté un amendement de précision en ce sens. Le rapporteur pour avis s'interroge toutefois sur la portée de cet ajout, observant que ce critère est bien prévu à l'article 3 de la directive qui, en définissant les notions-clés du texte, lie les États membres pour leur interprétation et leur application (5).

---

(1) Point 9 de l'article 3 de la directive 2016/681.

(2) Ainsi, ne figurent pas à l'annexe II de la directive les infractions suivantes : terrorisme (infraction qui est toutefois expressément prévue à l'article premier de la directive), racisme et xénophobie, escroquerie, extorsion, falsification des moyens de paiement et incendie volontaire.

(3) Les intérêts fondamentaux de la Nation s'entendent comme : son indépendance, l'intégrité de son territoire, sa sécurité, la forme républicaine de ses institutions, les moyens de sa défense et de sa diplomatie, la sauvegarde de sa population en France et à l'étranger, l'équilibre de son milieu naturel et de son environnement et les éléments essentiels de son potentiel scientifique et économique et de son patrimoine culturel.

(4) Conseil d'État, avis sur un projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme (n° 393348).

(5) Point 9 de l'article 3 pour ce qui concerne les « formes graves de criminalité ».

iii. La possibilité de soumettre d'autres opérateurs aux obligations de transmission des données PNR

En l'état du droit en vigueur et outre les transporteurs aériens pour lesquels une obligation légale est prévue, **les opérateurs de voyage ou de séjour affrétant un aéronef peuvent également être soumis à l'obligation de transmission des données PNR**.

Comme le considérant 33 de la directive le permet, **les alinéas 7 et 8** de l'article 6 complètent cette liste en y ajoutant les **agences de voyage** et modifient l'article L. 232-7 du code de la sécurité intérieure en ce sens.

Liste des données PNR dont le recueil et la transmission sont prévus par la directive 2016/681 (annexe I)

La liste des données PNR comprend 19 catégories représentant environ 280 données. Il convient de préciser qu'aux termes de l'article 13 de la directive, et à l'image des dispositions législatives françaises (article L. 232-7 du code de la sécurité intérieure), est interdit le traitement de données PNR qui révéleraient l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle.

1. Code repère du dossier passager
2. Date de réservation/d'émission du billet
3. Date(s) prévue(s) du voyage
4. Nom(s)
5. Adresse et coordonnées (numéro de téléphone, adresse électronique)
6. Toutes les informations relatives aux modes de paiement, y compris l'adresse de facturation
7. Itinéraire complet pour le PNR concerné
8. Informations « grands voyageurs »
9. Agence de voyages/agent de voyages
10. Statut du voyageur, y compris les confirmations, l'enregistrement, la non-présentation ou un passager de dernière minute sans réservation
11. Indications concernant la scission/division du PNR
12. Remarques générales (notamment toutes les informations disponibles sur les mineurs non accompagnés de moins de 18 ans, telles que le nom et le sexe du mineur, son âge, la ou les langues parlées, le nom et les coordonnées du tuteur présent au départ et son lien avec le mineur, le nom et les coordonnées du tuteur présent à l'arrivée et son lien avec le mineur, l'agent présent au départ et à l'arrivée)
13. Informations sur l'établissement des billets, y compris le numéro du billet, la date d'émission, les allers simples, les champs de billets informatisés relatifs à leur prix
14. Numéro du siège et autres informations concernant le siège
15. Informations sur le partage de code
16. Toutes les informations relatives aux bagages
17. Nombre et autres noms de voyageurs figurant dans le PNR
18. Toute information préalable sur les passagers (données API) qui a été recueillie (y compris le type, le numéro, le pays de délivrance et la date d'expiration de tout document

d'identité, la nationalité, le nom de famille, le prénom, le sexe, la date de naissance, la compagnie aérienne, le numéro de vol, la date de départ, la date d'arrivée, l'aéroport de départ, l'aéroport d'arrivée, l'heure de départ et l'heure d'arrivée)
19. Historique complet des modifications des données PNR énumérées aux points 1 à 18

iv. Une transposition qui reste à achever

Aux termes de son article 5, **la directive 2016/681 impose aux États membres de désigner un « délégué à la protection des données » au sein de leurs UIP nationales respectives.** Cette « autorité de contrôle nationale indépendante » sera chargée « *de fournir des conseils et de surveiller la manière dont les données PNR sont traitées* ».

La création d'une telle autorité n'est pas prévue par le projet de loi. Le Gouvernement souhaite se conformer à cette obligation dans le cadre du projet de loi qui assurera la transposition d'une autre directive, la directive 2016/680 (1), dont l'article 32 prévoit l'adoption de dispositions de droit national généralisant la création d'un tel délégué, doté d'un statut et de pouvoir spécifiques décrits par ce même texte, et ce pour tous les traitements de données à caractère personnel relevant du champ de la sécurité publique (2).

En tout état de cause, la France devra avoir mis en place cette autorité avant l'expiration du délai de transposition de la directive 2016/681, le 25 mai 2018.

c. La clarification du champ des données transmises à SETRADER

En 2013 la France a créé un fichier dénommé système européen de traitement des données d'enregistrement et de réservation, alimenté par les seules données API aux fins de prévenir et réprimer l'immigration clandestine, les actes de terrorisme, et d'assurer le contrôle aux frontières.

Ce fichier est mis en œuvre sur le fondement de l'article L. 232-1 du code de la sécurité intérieure qui, outre ces données API, dispose que SETRADER peut également être destinataire des données « enregistrées dans les systèmes de réservation », soit les données PNR.

En pratique, **SETRADER ne recueille et n'exploite que les données API**. Aussi, afin de mettre les dispositions législatives en accord avec la réalité opérationnelle – l'article 2 de l'arrêté portant autorisation de SETRADER ne

(1) Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes 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, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

(2) Soit les traitements servant à la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces.

mentionne d'ailleurs que les données API –, **l'alinéa 2 de l'article 6 supprime la référence aux données PNR** dans l'article L. 232-1 précité.

B. LA PÉRENNISATION DU « PNR MARITIME FRANCE » (ARTICLE 7)

a. La nécessité de pérenniser le système actuel

La loi relative à l'économie bleue [(1)] avait modifié le champ de l'article L. 232-7 du code de la sécurité intérieure relatif au système « API-PNR aérien » afin de l'étendre au secteur maritime, et ce de manière expérimentale jusqu'au 31 décembre 2017.

L'article 7 du présent projet de loi prévoit :

– de **pérenniser l'autorisation de collecte des données pour les passagers du secteur maritime** au-delà de cette date ;

– d'**autoriser la création d'un système automatisé de traitement de ces données** distinct du système mis en place dans le secteur aérien.

Le rapporteur pour avis juge légitime le fait de rendre permanent un tel système préventif à l'embarquement. La menace terroriste reste malheureusement encore vive, et le secteur maritime présente des vulnérabilités auxquelles il est nécessaire de remédier. Des mesures ont d'ailleurs été mises en œuvre ces dernières années en France avec, notamment :

– dans le domaine de la sécurité portuaire : le renforcement des pelotons de sûreté maritime et portuaire (PSMP) de la gendarmerie maritime [(2)] ;

– dans le domaine de la sûreté des navires en mer : la mise en place, depuis le 1er août 2016, d'équipes de protection des navires à passagers (EPNAP) [(3)].

Il convient de rappeler **l'importance de l'activité de transport à passagers pour la France en termes de flux de passagers**, qu'il s'agisse des liaisons maritimes fixes et régulières – les ferries – ou des activités de croisières, saisonnières – les paquebots. En tout, ces activités représentent un **volume annuel de 32,5 millions de passagers**. Le trafic transmanche est le plus important, avec 17 millions de passagers environ, suivi par les liaisons entre la Corse et le continent avec quatre millions de passagers, les liaisons opérées avec d'autres destinations méditerranéennes (Espagne, Italie, Maghreb) représentant quant à elles 3,5 millions de passagers. Au-delà du trafic métropolitain, les outre-mer sont

(1) Article 63 de la loi n° 2016-816 du 16 juin 2016 pour l'économie bleue.

(2) Le quatrième PSMP, basé à Dunkerque a été mis en place en septembre 2017 (les trois autres sont basés au Havre, à Port-de-Bouc et à Marseille). Les PSMP de Nantes Saint-Nazaire et Calais doivent être créés respectivement au premier semestre 2018 et début 2019.

(3) Équipes mixtes, composées à la fois de gendarmes maritimes et de fusiliers-marins et embarquant sur les navires à passagers.

également concernés : ainsi l'activité de croisière représente-t-elle 1,6 million de passagers aux Antilles.

L'article 7 du projet de loi créé donc un nouvel article L. 232-7-1 au sein du code de la sécurité intérieure afin de permettre la mise en œuvre d'un système de traitement automatisé des données permanent et distinct du système « API-PNR aérien » prévu à l'article L. 232-7 du même code.

b. Les finalités du système

● **L'alinéa 3** dresse la liste limitative des finalités pour lesquelles le système de traitement sera mis en place. Il s'agit de la prévention et de la constatation des actes de terrorisme, des atteintes aux intérêts fondamentaux de la Nation et d'un certain nombre d'infractions parmi les formes les plus graves de criminalité mentionnées à l'article 694-32 du code de procédure pénale, ainsi que de la conduite des enquêtes et des poursuites en ces matières. De fait, **les finalités du système « PNR maritime » seront les mêmes, à une exception près – l'espionnage industriel –, que celles prévues pour le système « API-PNR aérien »**.

Par parallélisme avec les dispositions prévues pour le système « API-PNR aérien » en application de la directive 2016/681, **le Sénat a précisé que la finalité du traitement automatisé devait se limiter aux infractions punies d'une peine d'emprisonnement ou d'une mesure de sûreté privative de liberté d'au moins trois ans** [(1)]**.**

En l'état actuel du projet de loi, la liste des infractions prévues pour le système maritime hors terrorisme et atteintes aux intérêts fondamentaux de la Nation est la même que pour le système aérien en application de la directive 2016/681 par renvoi à son annexe II, à l'exception d'une seule : l'espionnage industriel.

Comme c'est le cas actuellement dans le cadre du dispositif expérimental, le traitement automatisé des données pour le secteur maritime sera mis en œuvre par les ministres de l'Intérieur et des Armées ainsi que les ministres chargés des transports et des douanes.

Conformément au droit en vigueur et à l'image des dispositions prévues pour le système « API-PNR aérien », **l'alinéa 4** précise que sont exclues de système « PNR maritime » les données à caractère personnel « sensibles ».

c. Les dispositions relatives aux données collectées

● L'obligation de transmission des données et le champ des données collectées

L'obligation de transmission s'applique par principe, en vertu de **l'alinéa 5**, aux **exploitants de navires pour les passagers à destination ou en**

(1) Amendement de M. le sénateur Michel Mercier, rapporteur de la commission des Lois.

provenance du territoire national, quel que soit l'État du pavillon, français ou étranger. Seront donc concernés les liaisons maritimes entre l'étranger et la France, mais également les trajets entre deux points du territoire national.

Ces exploitants sont tenus de transmettre les données de réservation **(alinéa 10)** et les données d'enregistrement [(1)] **(alinéa 5)**.

Les données d'enregistrement sont les informations requises dans les formulaires n° 5 (liste d'équipage) et n° 6 (liste des passagers) de la convention visant à faciliter le trafic maritime international (convention FAL) ainsi que, le cas échéant, le numéro de visa ou de titre de séjour **(alinéa 9**, par renvoi indirect aux dispositions communautaires applicables [(2)]).

INFORMATIONS PRÉVUES PAR LES FORMULAIRES 5 ET 6 DE LA CONVENTION FAL

Formulaire n° 5 – liste d'équipage	Formulaire n° 6 – liste des passagers
1. Nom du navire 2. Indicatif d'appel 3. Numéro OMI [(3)] 4. Numéro du voyage 5. Port d'arrivée/de départ 6. Date d'arrivée/de départ 7. État du pavillon 8. Dernier port d'escale 9. N° 10. Nom(s), prénom(s) 11. Grade ou qualification 12. Nationalité 13. Date et lieu de naissance 14. Nature et numéro du document d'identité	1. Nom du navire 2. Indicatif d'appel 3. Numéro OMI 4. Numéro du voyage 5. Port d'arrivée/de départ 6. Date d'arrivée/de départ 7. État du pavillon 8. Nom(s), prénom(s) 9. Nationalité 10. Nature du document d'identité ou de voyage 11. Numéro du document d'identité ou de voyage 12. Port d'embarquement 13. Port de débarquement 14. Passager en transit ou non

Rapporteur pour avis, d'après la convention FAL.

Actuellement, cinq compagnies de transport de passagers participent au système « PNR maritime » transitoire. À terme, 13 compagnies seront concernées par le système pérennisé.

Au-delà des exploitants de navires à passagers et sur le modèle des dispositions applicables au système « API-PNR aérien », **les autorités publiques pourront également demander la transmission des données de réservation aux agences de voyages et aux opérateurs de voyage ou de séjour affrétant tout ou partie d'un navire (alinéa 11)**.

(1) Qui, en réalité, ne sont que les données de réservation mais mises à jour et contrôlées à l'embarquement.

(2) Paragraphe 3.1.2 de l'annexe VI au règlement (CE) n° 2016/399 du Parlement européen et du Conseil du 15 mars 2006 établissant un code communautaire relatif au régime de franchissement des frontières par les personnes (code frontières Schengen).

(3) Organisation maritime internationale.

Les données obligatoirement collectées à terme dans le cadre du « PNR maritime »
D'après les informations fournies au rapporteur pour avis, ces données seront les suivantes :
1. Type et numéro de document d'identité
2. Nationalité, nom, prénom, date de naissance, lieu de naissance, sexe
3. Nom du navire, n° OMI, n° MMSI [(1)], indicatif
4. Pavillon du navire
5. Numéro du voyage
6. Port d'arrivée/de départ
7. Date d'arrivée/de départ
8. Téléphone
9. Immatriculation du véhicule
10. Nom du propriétaire du véhicule
11. Moyen de paiement, y compris l'adresse de facturation
12. Nombre et noms des autres voyageurs figurant dans le dossier passager

Source : Secrétariat général de la Mer – réponses au questionnaire du rapporteur pour avis.

● Comme c'est le cas pour le système « API-PNR aérien », deux méthodes d'exploitations des données seront possibles : par criblage et par ciblage.

D'après les informations transmises au rapporteur pour avis, le criblage s'effectuera par le croisement des informations avec les mêmes fichiers que ceux prévus pour le système aérien (FPR, FOVeS, SIS II, base ASF-SLTD d'Interpol).

● **Les alinéas 12, 13 et 14** reprennent les dispositions en vigueur dans le cadre du système expérimental actuel :

– en prévoyant que les personnes concernées par le système de transmission des données passagers en sont informées par les différents opérateurs **(alinéa 12)** ;

– en précisant que la durée de conservation de ces données n'excède pas cinq ans **(alinéa 13)** ;

– en précisant les sanctions applicables aux opérateurs en cas de méconnaissance de leurs obligations **(alinéa 14)**.

d. Les modalités d'accès au fichier par les services habilités

L'alinéa 15 prévoit que les modalités d'application de l'article 7 seront fixées par décret en Conseil d'État après avis de la Commission nationale de l'informatique et des libertés.

Souhaitant écarter toute possibilité d'accès direct au système « PNR maritime », le Sénat a complété cet article en précisant que ce décret

(1) Maritime Mobile Service Identity – *Identité du service mobile maritime.*

déterminerait les services qui seront autorisés à interroger l'unité de gestion chargée de la collecte, de la conservation et de l'analyse de ces données [(1)], à l'image de l'UIP dans le cadre du système « API-PNR aérien ».

À cet égard, **le rapporteur pour avis** :

– **relève que le système « PNR maritime » sera alimenté par des données qui présentent un degré de sensibilité moindre que le système « API-PNR aérien »**. La seule information potentiellement sensible étant la communication des moyens de paiement et de l'adresse de facturation (donnée de réservation). Dès lors, **cela ne justifie pas la mise en œuvre des mêmes modalités de connexion au fichier**, telle que l'interdiction d'accès direct au système par les services ;

– observe, à titre de comparaison, que les agents des services habilités disposent d'un accès direct au système SETRADER, alors que celui-ci est alimenté par des données de type API ;

– et souhaite insister sur le fait que **si un service équivalent à l'UIP devait être créé dans le domaine maritime, les délais incompressibles pour sa mise en place auraient pour conséquence de priver notre pays, durant cette période, des possibilités offertes par le système expérimental**. En effet, celui-ci fonctionne actuellement sans unité de gestion, et ce jusqu'au 31 décembre 2017 au plus tard. Si la création d'une unité de gestion devait être confirmée, le dispositif expérimental deviendrait caduc dès la promulgation de la loi alors que le système pérennisé par la loi ne pourrait en réalité pas fonctionner avant la mise en place, relativement longue et coûteuse, d'une « UIP maritime ». Notre pays se priverait donc, dans l'intervalle, d'un outil précieux de prévention des formes graves de criminalité.

Il conviendrait donc sans doute de revenir aux dispositions initiales du projet de loi prévoyant un accès direct au système « PNR maritime ».

e. Les dispositions de coordination

Les alinéas 16 à 23 sont des dispositions de coordination. **Les alinéas 16 à 22** suppriment logiquement les références au système « PNR maritime » dans l'article L. 232-7 du code de la sécurité intérieure dès lors que, d'une part, ledit article sera *in fine* uniquement relatif au système « API-PNR aérien » et que, d'autre part, le système « PNR maritime » sera dorénavant expressément codifié dans un article spécifique, l'article L. 232-7-1 du même code créé par l'article 7 du projet de loi objet du présent commentaire.

Enfin, **l'alinéa 23** procède à la mise à jour d'une référence à l'article L. 232-4 du code la sécurité intérieure pour tenir compte de l'évolution des normes communautaires que ledit article mentionne.

---

(1) Amendement de M. le sénateur Michel Mercier, rapporteur de la commission des Lois.

II. LES DISPOSITIONS RELATIVES AUX TECHNIQUES DE RENSEIGNEMENT

Le chapitre II du projet de loi, en ses articles 8 et 9, a trait aux techniques de renseignement. Ces articles procèdent à la redéfinition du régime légal de surveillance des communications hertziennes afin de mettre le droit positif en conformité avec une récente censure du Conseil constitutionnel à l'occasion d'une question prioritaire de constitutionnalité [(1)] (QPC).

Le Sénat a par ailleurs introduit un article 8 *bis* nouveau de coordination relatif aux observations adressées par la Commission nationale de contrôle des techniques de renseignement (CNCTR) à la Délégation parlementaire au renseignement (DPR).

A. LE RÉGIME DE « L'EXCEPTION HERTZIENNE » : HISTORIQUE ET PRINCIPES

La notion d' « exception hertzienne » renvoie à l'existence d'un régime dérogatoire du droit commun pour les techniques de surveillance menées dans le domaine hertzien. Il convient dès lors de rappeler brièvement les principes qui encadrent l'utilisation des techniques de surveillance, avant de souligner en quoi et pourquoi le régime applicable au domaine hertzien en diffère.

a. Le régime de droit commun applicable aux techniques de renseignement sur le territoire national

Les dispositions législatives relatives aux activités et techniques de renseignement ont récemment été codifiées au sein d'un livre VIII nouveau du code de la sécurité intérieure. C'est la loi n° 2015-912 du 24 juillet 2015 relative au renseignement qui a introduit ce nouveau livre et redéfini le cadre légal de la mise en œuvre des techniques de renseignement.

● En vertu des dispositions législatives en vigueur, deux types de services peuvent mettre en œuvre de telles techniques.

Les **« services spécialisés de renseignement »** [(2)]**, qui constituent le « premier cercle » de la communauté du renseignement française**, disposent d'une **habilitation générale à mettre en œuvre l'ensemble des techniques** de surveillance pour l'exercice de leurs missions respectives et **pour l'ensemble des finalités limitativement prévues par la loi** concourant à la défense et à la promotion des intérêts fondamentaux de la Nation, pour peu, naturellement, que cette mise en œuvre respecte les dispositions législatives en vigueur (finalités, respect des procédures, etc.).

(1) Décision n° 2016-590 QPC du 21 octobre 2016.
(2) Article L. 811-3 du code de la sécurité intérieure.

Désignés par décret en Conseil d'État [1], ces **six services** sont :

– la direction générale de la sécurité extérieure **(DGSE)** ;

– la direction du renseignement et de la sécurité de la défense **(DRSD)** ;

– la direction du renseignement militaire **(DRM)** ;

– la direction générale de la sécurité intérieure **(DGSI)** ;

– la direction nationale du renseignement et des enquêtes douanières **(DNRED)** ;

– et le service dénommé « traitement du renseignement et action contre les circuits financiers clandestins » **(TRACFIN)**.

Par ailleurs, **certains services dits du « deuxième cercle »**, également désignés par décret en Conseil d'État [2] et relevant des ministres chargés de la défense [3], de l'intérieur [4], de la justice [5], de l'économie, du budget ou des douanes, peuvent également être autorisés à recourir à de telles techniques. Contrairement aux services du premier cercle, ceux du second ne bénéficient pas d'une habilitation générale, l'autorisation étant délivrée **uniquement pour certaines finalités** [6] **et pour une liste définie de techniques** [7]**.** Ainsi les sections de recherches de la gendarmerie nationale ne peuvent-elles y recourir que pour les deux finalités suivantes : la prévention du terrorisme et la prévention de la criminalité et de la délinquance organisées.

● Par principe, toute demande d'utilisation d'une technique de renseignement destinée à surveiller le territoire national, qu'elle émane d'un des six services spécialisés de renseignement ou d'un service du « deuxième cercle », fait l'objet d'une **procédure d'autorisation préalable**. Cette procédure comprend **deux étapes** :

– la demande doit être formulée par le ministère de tutelle du service concerné, ou son délégué ;

---

(1) Codifié à l'article R. 811-1 du code de la sécurité intérieure.

(2) Codifié à l'article R. 811-2 du code de la sécurité intérieure.

(3) Sections de recherches de la gendarmerie maritime, de la gendarmerie de l'air et de la gendarmerie de l'armement (ces gendarmeries spécialisées sont placées pour emploi respectivement auprès du chef d'état-major de la marine, du chef d'état-major de l'armée de l'air et du délégué général pour l'armement).

(4) À titre d'exemples :

– sous l'autorité du directeur général de la police nationale : l'unité de coordination de la lutte antiterroriste (UCLAT), la sous-direction de la lutte contre la criminalité organisée et la délinquance financière, la sous-direction antiterroriste ou encore les services du renseignement territorial ;

– sous l'autorité du directeur général de la gendarmerie nationale : la sous-direction de l'anticipation opérationnelle, la sous-direction de la police judiciaire et les sections de recherches ;

– sous l'autorité du préfet de police de Paris : la sous-direction de la sécurité intérieure ou encore la sous-direction du renseignement territorial.

(5) Notamment le bureau central du renseignement pénitentiaire.

(6) Limitativement énumérées, pour chaque service, à l'article R. 811-2 du code de la sécurité intérieure.

(7) Voir les dispositions codifiées au titre V du livre VIII du code de la sécurité intérieure (articles R. 851-1 à R. 853-3).

– l'autorisation est délivrée par le Premier ministre, après avis préalable obligatoire – mais simple, qui ne lie pas le Premier ministre – de la CNCTR [(1)]. Si elle est délivrée, l'autorisation est valable pour une durée maximale de quatre mois renouvelable [(2)].

Il convient de souligner que la demande doit être suffisamment étayée puisqu'elle doit préciser : la ou les techniques à mettre en œuvre ; le service pour lequel elle est présentée ; la ou les finalités poursuivies ; le ou les motifs des mesures ; la durée de validité de l'autorisation ; la ou les personnes, le ou les lieux ou véhicules concernés [(3)].

Cette procédure s'applique, sauf exceptions [(4)], à l'ensemble des techniques destinées à surveiller le territoire national : recueil des données de connexion, interceptions de sécurité, sonorisation des lieux privés et captation des données informatiques.

● **Le contrôle de la CNCTR** sur les techniques de renseignement mises en œuvre sur le territoire national s'effectue en application des articles L. 833-1 à L. 833-11 du code de la sécurité intérieure :

– elle reçoit de plein droit communication de toutes les autorisations délivrées par le Premier ministre et par les personnes que ce dernier délègue ;

– elle dispose d'un accès permanent à tous les registres, relevés, enregistrements et transcriptions issus de la mise en œuvre des techniques de recueil de renseignement soumises à autorisation préalable, aux dispositifs de traçabilité des renseignements collectés et aux locaux où sont centralisés les renseignements collectés ;

– elle peut également demander à être informée à tout instant des modalités d'exécution des autorisations en cours ;

– elle peut solliciter du Premier ministre tous les éléments nécessaires à l'accomplissement de sa mission, notamment les rapports de l'inspection des services de renseignement ou d'autres rapports d'inspections générales. Sont seuls exclus du champ des éléments communicables ceux qui auraient été communiqués par des services étrangers ou par des organismes internationaux, ou qui pourraient directement ou indirectement donner à la CNCTR connaissance de l'identité des sources des services spécialisés de renseignement.

---

(1) Si l'autorisation est délivrée malgré un avis défavorable de la CNCTR, elle doit indiquer les motifs pour lesquels cet avis n'a pas été suivi.

(2) Article 821-4 du code de la sécurité intérieure.

(3) Article 821-2 du code de la sécurité intérieure.

(4) Il existe une procédure dite d'« urgence absolue » qui, par exception, permet au Premier ministre de délivrer l'autorisation sans solliciter l'avis préalable de la CNCTR, celle-dit devant toutefois être informée sans délai et se voir présenter, dans les 24 heures, tout élément justifiant le caractère d'urgence absolue (article L. 821-5 du code de la sécurité intérieure).

● La surveillance des communications électroniques internationales [1], reçues ou émises de l'étranger, est quant à elle soumise à une procédure d'autorisation différente : si elle reste délivrée par le Premier ministre, l'avis de la CNCTR n'est pas légalement requis [2].

b. L'existence d'un régime dérogatoire : justifications et principes de l' « exception hertzienne »

Le premier cadre légal relatif à la mise en œuvre des techniques de renseignement a été établi par la **loi n° 91-646 du 10 juillet 1991** relative au secret des correspondances émises par la voie des télécommunications électroniques. **Le législateur avait alors fait le choix d'exclure les mesures de surveillance transmissions empruntant la voie hertzienne de la procédure de droit commun d'autorisation préalable et de contrôle**.

Ce régime dérogatoire – ou « exception hertzienne » – a été maintenu par la loi du 24 juillet 2015 relative au renseignement et **codifié dans le code de la sécurité intérieure en son article L. 811-5.**

Cette exclusion du régime de droit commun avait été justifiée par le fait que les interceptions réalisées dans le domaine hertzien constituaient une **mesure de surveillance générale, sans viser de communications individualisables, et que, par conséquent, elles ne portaient pas atteinte au secret des correspondances**.

En effet, techniquement, **de telles communications s'effectuent sans support filaire** [3]. Utilisant le champ électromagnétique pour transmettre un message depuis un émetteur vers un récepteur, elles se propagent dans l'espace public et **peuvent donc être captées par quiconque dispose d'un récepteur branché sur la bonne fréquence et situé dans le périmètre d'émission**. En outre, contrairement à d'autres types de communications – par exemple celles qui empruntent le réseau d'un opérateur de communications électroniques – les communications hertziennes ne comportent pas, sauf cas particuliers (cf. *infra*), d'élément d'identification ou de localisation de l'émetteur ou du destinataire du message.

La Commission nationale de contrôle des interceptions de sécurité (CNCIS) puis la CNCTR [4] **avaient par ailleurs adopté une conception restrictive de la notion d' « exception hertzienne »** afin d'éviter tout contournement du régime de droit commun prévu pour les autres techniques de renseignement. En effet un certain nombre de communications empruntent, mais seulement partiellement, la voie hertzienne.

---

(1) Prévue par la loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales et dont les dispositions sont codifiées aux articles L. 854-1 à L. 854-9 du code de la sécurité intérieure.

(2) Article L. 854-2 du code de la sécurité intérieure.

(3) Via *un câble en cuivre ou en fibre optique.*

(4) Qui a succédé à la CNCIS en application de la loi du 24 juillet 2015 relative au renseignement.

B. LA CENSURE DU CONSEIL CONSTITUTIONNEL ET SES CONSÉQUENCES

● En dépit des restrictions successivement posées par la CNCIS et la CNCTR, le Conseil constitutionnel, saisi d'une QPC, a censuré les dispositions relatives à l' « exception hertzienne » en déclarant **l'article L. 811-5 du code de la sécurité intérieure contraire à la Constitution**.

Les griefs retenus étaient les suivants :

– le Conseil a d'abord estimé que cet article **n'excluait pas l'interception de communications ou le recueil de données individualisables** ;

– il a ensuite considéré que **les finalités au titre desquelles les mesures de surveillance pouvaient être opérées étaient définies de manière trop générale**, l'article L. 811-5 du code de la sécurité intérieure faisant référence à « *la défense des intérêts nationaux* » alors que les autres techniques de renseignement ne peuvent être justifiées que par « *les menaces, les risques et les enjeux liés aux intérêts fondamentaux de la Nation mentionnés* » limitativement énumérés à l'article L. 811-3 du même code. De fait le Conseil a estimé que les mesures mises en œuvre au titre de l' « exception hertzienne » pouvaient potentiellement être utilisées à des fins plus larges que celle prévue ;

– enfin, le Conseil a relevé que **les dispositions contestées ne définissaient pas la nature des mesures de surveillance et de contrôle susceptibles d'être mises en œuvre, qu'elles n'en soumettaient le recours à aucune condition de fond ou de procédure** – il s'agissait de la seule technique pour laquelle l'autorisation du Premier ministre n'était pas requise [(1)] –, **et que leur mise en œuvre n'était encadrée par aucune garantie** [(2)].

Le Conseil constitutionnel a déduit de ces griefs que, dans sa rédaction en vigueur, l'article L. 811-5 du code de la sécurité intérieure portait « *une atteinte manifestement disproportionné au droit au respect de la vie privée et au secret des correspondances résultant de l'article 2 de la Déclaration de 1789* », qu'il était inconstitutionnel et devait dès lors être censuré.

● Toutefois afin, d'une part, de ne pas priver les services de toute possibilité de surveillance dans ce domaine et, d'autre part, de permettre au Législateur de tirer les conséquences de cette censure, le Conseil constitutionnel en a reporté les effets au 31 décembre 2017.

---

(1) L'article L. 811-5 ne précise pas les autorités pouvant décider de leur mise en œuvre, se bornant à évoquer les « pouvoirs publics *».*

(2) Avec le respect du principe de proportionnalité entre les techniques mises en œuvre et les objectifs poursuivis, et l'existence d'un contrôle spécifique par une autorité administrative indépendante ou par un juge. Ces exigences sont posées, pour les autres techniques de renseignement hors « exception hertzienne », par l'article L. 801-1 du code de la sécurité intérieure.

Il a par ailleurs formulé deux réserves d'interprétation pour l'application du régime de l'exception hertzienne au cours de cette phase transitoire :

– l'interdiction de recourir à ce régime pour des interceptions qui relèveraient du droit commun ;

– la mise en place d'un contrôle par la CNCTR, laquelle doit être « *régulièrement informée sur le champ et la nature des mesures prises* » en application de l'article L. 811-5.

C. LA CRÉATION D'UN NOUVEAU RÉGIME JURIDIQUE CONCILIANT EFFICACITÉ OPÉRATIONNELLE ET PROTECTION DES LIBERTÉS

Le chapitre II du projet de loi en ses articles 8 et 9 tire les conséquences de la censure du Conseil constitutionnel en définissant un nouveau cadre légal pour la surveillance des communications hertziennes.

1. Le maintien de « l'exception hertzienne » : une exigence opérationnelle

D'après les informations fournies par l'étude d'impact et confirmées par les services lors de leur audition par le rapporteur pour avis, les possibilités de surveillance d'un tel domaine de communication doivent être maintenues car elles répondent à une **nécessité opérationnelle dans trois secteurs** :

– **dans le domaine militaire** : les interceptions de communications radio longues et très longues distances (HF et VLF) permettant aux forces armées de disposer d'informations précieuses [(1)], y compris lorsqu'elles sont menées depuis le territoire national, lequel ne se limite pas à la France métropolitaine ;

– **en matière de lutte contre le terrorisme** : les communications radio pouvant être utilisées par les organisations terroristes et les groupes djihadistes ;

– **dans le domaine de la contre-ingérence** : par exemple en permettant l'interception de communications entre les puissances étrangères et leurs agents.

Il convient par ailleurs de souligner que certains acteurs, pas toujours bien intentionnés et conscients des risques de surveillance dans les domaines autres que l'hertzien, choisissent de recourir à des communications exclusivement hertziennes avec des méthodes sans doute plus « artisanales » (utilisation de simples radios par exemple), mais qui permettent de réduire le risque d'interception.

(1) Mouvements de troupes, de bâtiments et d'aéronefs militaires étrangers par exemple.

2. Un nouveau champ limité au strict nécessaire : vers une « exception hertzienne » résiduelle (article 8)

L'article 8 procède à la création d'un **dispositif à double entrée qui restreint le champ de l' « exception hertzienne »** :

– pour les communications qui, bien qu'empruntant exclusivement la voie hertzienne et ne faisant intervenir aucun opérateur de communications électroniques, revêtent un caractère privé, les demandes de surveillance seront soumises au droit commun, c'est-à-dire avec autorisation préalable du Premier ministre après avis de la CNCTR [(1)] ;

– pour les communications qui empruntent exclusivement la voie hertzienne, sans intervention d'un opérateur de communications électroniques, mais qui ne relèvent d'aucun réseau privatif, leur surveillance restera soumise à un régime allégé sans autorisation préalable [(2)], mais avec des modalités inédites de contrôle *a posteriori* par la CNCTR dans ce domaine de l'hertzien « public ».

a. La création d'une nouvelle technique de renseignement soumise au régime de droit commun pour l' « hertzien privatif »

● **Les alinéas 3 à 5** créent une nouvelle technique de renseignement, codifiée à l'article L. 852-2 nouveau du code de la sécurité intérieure pour « *les 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.* »

Deux critères cumulatifs et une condition permettent de déterminer le caractère privé des correspondances empruntant la voie hertzienne et de soumettre, en conséquence, les mesures de surveillance susceptible de les concerner aux règles de droit commun, avec autorisation préalable après avis de la CNCTR :

– premier critère : les correspondances doivent emprunter exclusivement la voie hertzienne. Celles qui ne l'emprunteraient qu'à titre accessoire et qui devraient faire l'objet de mesures de surveillance ont vocation à être couvertes par les dispositions en vigueur relatives aux techniques de renseignement existantes ;

– second critère : les correspondances doivent emprunter un réseau qui ne fait pas intervenir d'opérateur de communications électroniques exploitant un réseau ouvert au public [(3)] ;

---

(1) Sont par exemple concernées les communications radio « de point à point », comme celles effectuées via *des* talkie-walkies *numériques.*

(2) Seraient par exemple concernées les communications radio longues et très longues distances.

(3) En principe, s'agissant d'un domaine public, aucun opérateur n'est impliqué dans le transport d'une communication hertzienne. Le contre-exemple est celui des communications satellitaires.

– condition : les correspondances sont échangées au sein d'un réseau réservé à l'usage d'un groupe fermé d'utilisateurs.

Selon les données publiées par l'Autorité de régulation des communications électroniques et des postes (ARCEP), on compte en France quelque **2 294 opérateurs télécoms déclarés** et attributaires de numéros, ainsi que **32 opérateurs MVNO** (1).

D'après les informations communiquées au rapporteur pour avis, **le principal mode de communication qui aurait vocation à entrer dans le champ de l' « hertzien privatif » serait le *talkie-walkie* numérique ou PMR** (*Private Mobile Radio*). Se caractérisant, d'une part, par sa **portée limitée** et, d'autre part, par l'intégration dans l'appareil de **mécanismes d'authentification et de partage de clés de chiffrement**, le recours à la PMR **révèle l'intention des utilisateurs de conférer un caractère privé à leurs échanges**, quand bien même ceux-ci empruntent le domaine public que constitue l'hertzien.

● En modifiant l'article L. 822-2 du code de la sécurité intérieure, **l'alinéa 2 de l'article 8** prévoit que, comme c'est le cas pour les interceptions de sécurité, les **correspondances interceptées** sur le fondement de la nouvelle technique de surveillance de l' « hertzien privatif » seront **détruites à l'issue d'un délai de trente jours.**

En définitive et fort logiquement s'agissant de mesures susceptibles de porter atteinte à la vie privée des personnes et au secret des correspondances, les actions mises en œuvre au titre de la nouvelle technique de renseignement relative à l' « hertzien privatif » seront encadrées par l'ensemble des dispositions de droit commun applicables aux techniques de renseignement existantes, qu'il s'agisse des finalités, de la procédure, des régimes d'utilisation et de gestion des données interceptées – exploitation, transcription, conservation – ou du contrôle.

b. La nouvelle « exception hertzienne » : un champ expressément limité au seul « hertzien public », des nouvelles garanties

Les alinéas 7 à 15 de l'article 8 créent un nouveau chapitre V dans le code de la sécurité intérieure qui définit le nouveau régime juridique applicable aux mesures de surveillance des communications empruntant exclusivement la voie hertzienne et ne faisant intervenir aucun opérateur de communication électronique, mais ne relevant d'aucun réseau privatif. Ils définissent ainsi le nouveau champ de l' « exception hertzienne ».

Demeurant soumise à un régime d'autorisation allégé par rapport au droit applicable à l' « hertzien privatif », **la surveillance de ces communications**

---

(1) Pour Mobile Virtual Network Operator. *Il s'agit opérateurs qui ne disposent pas de leur propre réseau radio et qui utilisent celui de l'un des opérateurs mobiles « historiques » en leur achetant des minutes de conversation en gros afin d'offrir des services de communication mobile à leurs abonnés. Les établissements bancaires ou les enseignes de la grande distribution proposant des services de téléphonie entrent dans cette catégorie particulière d'opérateurs.*

se voit expressément et légalement limitée au seul « hertzien public », conformément aux prescriptions du Conseil constitutionnel.

● Les services susceptibles de mettre en œuvre ces mesures et leurs finalités

Aux termes de l'article L. 854-9-2 nouveau du code de la sécurité intérieure **(alinéa 10)**, les services pouvant recourir à de telles mesures sont les six services spécialisés de renseignement (le « premier cercle ») ainsi que les services du « second cercle » de la communauté du renseignement. **Les finalités sont celles du droit commun applicable à l'ensemble des techniques de renseignement**, à savoir **la défense et la promotion des intérêts de la Nation** (1).

Le nouveau champ de l' « exception hertzienne » sera résiduel puisque ne seront concernées par les nouvelles dispositions législatives :

– que les communications exclusivement hertziennes,

– qui ne nécessitent pas l'intervention d'un opérateur de communications électroniques,

– qui ne relèvent d'aucun réseau privatif,

– et qui ne peuvent être interceptées et exploitées sur le fondement d'aucune des autres techniques de renseignement : ni celles prévues par la loi relative au renseignement du 24 juillet 2015, ni celle prévue par la loi relative à la surveillance des communications internationales, ni celle prévue par le présent projet de loi concernant l' « hertzien privatif ».

Les mesures prises sur ce fondement ne sont soumises à aucune autorisation autre que l'autorisation légale d'y recourir prévue par le présent projet de loi. Comme sous le régime de l'ancienne « exception hertzienne », aucune autorisation préalable du Premier ministre après avis de la CNCTR n'est requise.

Au total, l' « exception hertzienne » et le régime dérogatoire qui y est attaché deviendront réellement « exceptionnels ». Le nouveau champ de l' « exception hertzienne » couvrirait uniquement la CB, les radioamateurs, les *talkie-walkies* analogiques ainsi que les communications radio des gammes VLF (2) et HF (3) et les moyens radio militaires tactiques de la gamme V/UHF (4).

Le tableau suivant fait état des différents régimes applicables en matière de surveillance des communications hertziennes (dispositions existantes et dispositions proposées par le projet de loi). Il témoigne du fait que le régime de

(1) Article L. 811-3 du code de la sécurité intérieure.
(2) Très basses fréquences.
(3) Hautes fréquences.
(4) Très et ultra hautes fréquences.

l' « exception hertzienne » nouvelle ne s'appliquerait qu'à un nombre de cas très réduits.

LES DIFFÉRENTS RÉGIMES APPLICABLES À LA SURVEILLANCE DES COMMUNICATIONS HERTZIENNES

Régimes applicables	**Régime de droit commun** : – interceptions de sécurité (art. L. 852-1 du code de la sécurité intérieure – CSI) ; – recueil et captation des données informatiques (art. L. 853-2 CSI) ; – ou surveillance des communications électroniques internationales (art. L. 854-1 et s. CSI)	**Régime « hertzien privatif » rattaché au régime de droit commun** (art. L. 852-2 CSI)	**Régime « hertzien public » allégé – nouvelle « exception hertzienne »** (art. L. 854-9-1 et s. CSI et art. L. 2371-1 du code de la défense)
Mode de communication hertzienne	Communications non exclusivement hertziennes et/ou avec intervention d'un opérateur de communications électroniques exploitant un réseau ouvert au public	• Communications exclusivement hertziennes et sans intervention d'un opérateur de communications électroniques exploitant un réseau ouvert au public • Lorsque le réseau est conçu pour une utilisation privative	• Communications exclusivement hertziennes et sans intervention d'un opérateur de communications électroniques exploitant un réseau ouvert au public • Utilisation non privative du réseau • Communications non couvertes par l'une des autres techniques de renseignement
Trafic entre un terminal et une borne WiFi ou WiMax	Si trafic acheminé par Internet, témoignant de l'intervention d'un opérateur	Si trafic non acheminé par Internet, témoignant d'une absence d'intervention d'opérateur *Exemple :* trafic interne à une entreprise (possibilité de recours subsidiaire à l'art. 853-2 CSI)	Non applicable
Téléphones sans fil	Si communications *via* un opérateur	Si communications sans intervention d'un opérateur *Exemple :* mode interphone, entre deux pièces d'un domicile (possibilité de recours subsidiaire à l'art. 853-2 CSI)	Non applicable
Radioamateurs, CB, *talkie-walkies* analogiques	Non applicable	Non applicable	• CB et radioamateurs : principe de diffusion publique des communications • *Talkie-walkies* analogiques : absence de mécanisme d'authentification ou de partage de clés de chiffrement

Talkie-walkies numériques (PMR)	Non applicable	• Absence d'opérateur • Portée limitée • Présence de mécanismes d'authentification et de chiffrement automatiques	Non applicable
Téléphones satellitaires	Trafic téléphonique ou Internet *via* un opérateur (recours aux art. L. 854-1 et s. CSI)	Non applicable	Non applicable
Téléphones mobiles avec antenne relais GSM/3G/4G et ordinateurs portables avec clé 3G/4G	Intervention d'un opérateur	Non applicable	Non applicable
Bluetooth	Non applicable	• Absence d'opérateur • Portée limitée	Non applicable
Trafic entre des objets connectés et une borne	Si intervention d'un opérateur	• Si absence d'opérateur • Portée limitée	Non applicable
Radio VLF et HF, et moyens militaires tactiques V/UHF	Non applicable	Non applicable	

Source : rapporteur pour avis d'après l'étude d'impact et les informations recueillies.

● Les modalités de conservation, de transcription et d'extraction des renseignements collectés

L'article L. 854-9-2 nouveau du code de la sécurité intérieure (alinéas 11 et 12) prévoit la **destruction des renseignements recueillis** en application des mesures mises en œuvre dans le cadre de la nouvelle « exception hertzienne » **à l'issue d'une période de six ans, portée à huit ans s'il s'agit de données chiffrées (alinéa 11)**.

Le rapporteur pour avis a jugé nécessaire de préciser le point de départ des délais de conservation en prévoyant qu'ils courent :

– à compter de leur recueil pour les renseignements non chiffrés ;

– à compter de leur déchiffrement pour les renseignements chiffrés.

Le **régime de transcription et d'extraction** des renseignements **(alinéa 12)** est le régime de droit commun prévu pour les autres techniques de renseignement à l'article L. 822-3 du code de la sécurité intérieure : ces renseignements ne peuvent être transcrits ou extraits que pour la poursuite de l'une des finalités expressément prévues à l'article L. 811-3 du même code, et ces transcriptions et extractions doivent être détruites dès lors que leur conservation n'est plus indispensable à la poursuite de ces finalités.

● La définition d'un régime de contrôle inédit

Se conformant à la censure du Conseil constitutionnel, le présent projet de loi dispose que, **dorénavant, les mesures relevant de l' « exception hertzienne » feront l'objet d'un contrôle de la part de la CNCTR** (article L. 854-9-3 nouveau du code de la sécurité intérieure). Il s'agit d'un **contrôle *a posteriori***, ces mesures restant dispensées de l'autorisation préalable délivrée après avis de la CNCTR.

Celle-ci veillera tout d'abord au respect du champ d'application des mesures mises en œuvre sur le fondement de l' « exception hertzienne » relativement aux autres techniques de renseignement de droit commun **(alinéa 13)**.

Elle sera tenue informée du champ et de la nature des mesures prises, le projet de loi consacrant dans le droit positif la réserve d'interprétation posée par le Conseil constitutionnel au titre de la période transitoire. Elle pourra également demander aux services concernés de lui présenter, sur place, les capacités d'interception qu'ils mettent en œuvre à cet égard **(alinéa 14)**.

Le projet de loi initial avait en outre prévu que la CNCTR puisse solliciter le Premier ministre afin d'avoir accès à « *tous les éléments nécessaires à l'accomplissement de sa mission* ». Sur ce fondement, elle pouvait notamment se voir communiquer les renseignements collectés et les transcriptions et extractions réalisées afin de s'assurer du respect des champs d'application des différentes techniques de renseignement. À l'initiative du rapporteur de la commission des Lois, M. Michel Mercier, **le Sénat a simplifié cette procédure en supprimant ce mécanisme de sollicitation préalable**, conférant ainsi à la CNCTR le même pouvoir de communication directe dont elle dispose par principe en vertu des règles de droit commun [(1)].

Le rapporteur pour avis estime cette modification bienvenue. Il juge toutefois nécessaire de modifier le champ des éléments susceptibles d'être communiqués en le limitant aux seuls renseignements collectés et effectivement conservés, pendant leur période de conservation, ainsi qu'aux transcriptions et extractions réalisées.

En effet, prévoir un accès de la CNCTR à l'ensemble des renseignements collectés serait, d'une part, inutile pour la conduite du contrôle et, d'autre part, coûteux dès lors que :

– ceux qui ne présentent aucun intérêt opérationnel ne sont pas conservés mais sont détruits après leur recueil ;

– et que leur éventuelle conservation entraînerait des coûts d'investissement et de fonctionnement non négligeables.

(1) Article L. 833-2 du code de la sécurité intérieure.

Pour la conduite de ce contrôle, la CNCTR aurait accès aux dispositifs de conservation des services. Aucun dispositif de stockage supplémentaire spécifique ne serait mis en œuvre, qui s'ajouterait à ceux utilisés par les services pour conserver les renseignements collectés.

Enfin, il est prévu que la CNCTR puisse adresser au Premier ministre et à la Délégation parlementaire au renseignement (DPR) toute recommandation et observation qu'elle jugerait nécessaire au titre de son contrôle **(alinéa 15)**. Pour ce qui concerne la DPR, une telle disposition nécessite une mesure de coordination, prévue à l'article 8 *bis* nouveau du projet de loi.

L'alinéa 16 procède quant à lui à une coordination dans le code de la sécurité intérieure en supprimant, dans une disposition relative aux possibilités de réquisition des opérateurs et prestataires de services, une référence à l'article L. 811-5 du même code censuré par le Conseil constitutionnel.

c. La clarification du champ d'application des mesures de captation des données informatiques émises ou reçues par des périphériques

L'article L. 853-2 du code de la sécurité intérieure permet, entre autres, aux services habilités de recourir à des dispositifs techniques leur permettant d'accéder à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles sont reçues ou émises par des périphériques audiovisuels (captation sur écran).

Il s'agit de mesures subsidiaires, qui ne peuvent être mises en œuvre que dans l'hypothèse où les renseignements relatifs aux finalités de l'article L. 811-3 du même code ne peuvent être recueillis par un autre moyen légalement autorisé.

L'alinéa 6 de l'article 8 supprime la référence au caractère « audiovisuel » des périphériques actuellement concernés par ces dispositions. Ce faisant, il permet d'adapter le régime en vigueur aux évolutions technologiques en étendant l'application de cette technique de renseignement à la captation de données informatiques échangées grâce à des protocoles sans fil [(1)], employés de plus en plus fréquemment dans le cadre de l'utilisation d'objets connectés notamment.

S'agissant de techniques particulièrement intrusives, l'autorisation délivrée pour les mettre en œuvre est de deux mois renouvelable, contre une durée de quatre mois renouvelable dans le cas général prévu en application de l'article L. 821-4 du même code.

(1) Le plus répandu étant sans doute le wifi.

3. Mesure de coordination relative aux relations entre la CNCTR et la DPR (article 8 *bis*)

Introduit par amendement à l'initiative du rapporteur pour avis de la commission des Affaires étrangères, de la défense et des forces armées du Sénat, M. Michel Boutant, **l'article 8 *bis*** est un article de coordination modifiant l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires.

Il en complète l'article 6 *nonies* afin de préciser que la DPR sera destinataire des observations que la CNCTR lui adressera en application du contrôle exercé sur la mise en œuvre du nouveau régime de l' « exception hertzienne ».

4. La possibilité de mettre en œuvre des mesures de surveillance de l'hertzien « ouvert » pour certains services et unités du ministère des Armées (article 9)

● Par la création d'un article L. 2371-1 dans le code de la défense, **les alinéas 1 à 4 de l'article 9 permettront aux unités des armées chargées de la défense militaire de continuer mettre en œuvre des mesures de surveillance de l'hertzien « ouvert », dans le cadre du nouveau régime de « l'exception hertzienne », et pour le seul exercice de leurs missions**. Si elles n'appartiennent pas aux services expressément habilités à mettre en œuvre des techniques de renseignement sur le territoire national, certaines unités doivent pouvoir recourir à la surveillance des communications hertziennes « ouvertes » notamment à des fins de veille stratégique ou de soutien aux opérations.

Ces missions de défense militaire ont trait à la dissuasion nucléaire, à la défense opérationnelle, à la défense maritime du territoire et à la défense aérienne (posture permanente de sauvegarde maritime et posture permanente de sûreté aérienne). Elles s'exercent également pour la mise en œuvre de l'action de l'État en mer. D'après l'étude d'impact, les mesures de surveillance pratiquées dans le domaine hertzien, dans le cadre exclusif de ces missions, permettent « *d'identifier, en temps réel, la présence d'intrus ou d'éléments faisant pesant une menace sur ou à proximité du territoire national, afin d'intervenir pour empêcher un acte hostile* ». On peut citer, à titre d'exemple, la présence d'embarcations qui chercheraient à pister un sous-marin nucléaire lanceur d'engins sortant de la base de l'Île-Longue et communiquant entre elles à cet effet.

L'alinéa 4 de l'article 9 précise que la CNCTR sera informée du champ et de la nature des mesures de surveillance qui seront mises en œuvre par ces unités dans le cadre de leurs missions.

Il s'agit de **modalités de contrôle encore allégées** par rapport au régime prévu pour les mesures de surveillance des communications hertziennes « ouvertes » mises en œuvre dans le cadre d'actions de renseignement. **Un tel allégement est légitime dès lors que, d'une part, de telles mesures ne sont pas**

attentatoires aux libertés publiques s'agissant de communications non privatives et que, d'autre part, les unités concernées ne les mettront pas en œuvre dans le cadre d'actions de renseignement *stricto sensu* (mesures de surveillance administrative). Ces unités ne pourront d'ailleurs recourir qu'à cette seule technique, à l'exclusion des autres techniques prévues par le code de la sécurité intérieure.

Par renvoi aux nouvelles dispositions du code de la sécurité intérieure, et en dehors des dispositions spécifiques relatives au contrôle de la CNCTR, les mesures mises en œuvre par les unités chargées de la défense militaire seront soumises au **régime général de la nouvelle « exception hertzienne » quant à la procédure** (absence d'autorisation préalable) **et quant aux règles encadrant la conservation des données, leur transcription, leur extraction et leur destruction.**

● **Les alinéas 5 et 6 de l'article 9** créent un article L. 2371-2 nouveau dans le code de la défense sur la base duquel **la direction générale de l'armement** pourra également procéder à la mise en œuvre des mesures de surveillance de communications dans le domaine hertzien « ouvert ». Une telle **possibilité** sera toutefois **doublement limitée** :

– quant à la **nature des mesures** : la DGA ne pourra effectuer que des **mesures d'interception,** l'exploitation des renseignements recueillis étant expressément prohibée ;

– quant à la **finalité des mesures** : la DGA ne pourra y recourir qu'à la seule fin de mener les **campagnes d'essai des matériels utilisés par les forces armées et permettant la mise en œuvre de mesures de surveillance**. Mentionnés au 1° de l'article 226-3 du code pénal, il s'agit des appareils et dispositifs techniques dont la liste est établie par arrêté du Premier ministre [(1)] et qui permettent la réalisation de tout type d'interception [(2)].

(1) Arrêté du 4 juillet 2012 fixant la liste d'appareils et de dispositifs techniques prévue par l'article 226-3 du code pénal.
(2) Idem, annexes I et II.

TRAVAUX DE LA COMMISSION

La commission examine pour avis, sur le rapport de M. Guillaume Gouffier-Cha, le projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme (n° 104), au cours de sa réunion du mardi 12 septembre 2017.

M. Guillaume Gouffier-Cha, rapporteur pour avis. Monsieur le président, chers collègues, je suis honoré d'inaugurer cette rentrée parlementaire en rapportant le premier texte dont notre commission s'est saisie pour avis sous cette nouvelle législature. Cette saisine concerne deux domaines qui intéressent la défense : les systèmes de traitement des données *Advanced Passenger Information* (API) et *Passenger Name record* (PNR), qui font l'objet des articles 5 à 7 du projet de loi, et les techniques de renseignement, traités dans les articles 8 à 9.

Je présenterai successivement les principales dispositions prévues dans ces matières, en m'efforçant d'être le plus clair possible malgré la technicité de ces sujets.

Les articles 5 et 6 concernent le système « API-PNR aérien ». Ils visent, d'une part, à pérenniser le système expérimental en vigueur qui arrive à échéance à la fin de l'année 2017, d'autre part, à mettre en conformité le droit national avec le droit communautaire à la suite de l'adoption définitive de la « directive PNR ».

J'anticipe nos débats sur les amendements de suppression de ces deux articles en rappelant dès à présent que la transposition d'une directive constitue une obligation communautaire en vertu des traités européens, ainsi qu'une exigence constitutionnelle.

Les données PNR sont l'ensemble des informations fournies par une personne physique ou par un opérateur lors de la réservation d'un voyage auprès d'un transporteur aérien. Ce sont des informations déclaratives. On dénombre dix-neuf catégories PNR, parmi lesquelles : la date de réservation et d'émission du billet, la ou les dates du voyage, les noms, prénoms, et dates de naissance des voyageurs, ou encore les informations relatives aux éventuels programmes de fidélité.

Afin de relativiser certaines craintes concernant ces données PNR, je rappelle qu'elles existent depuis plusieurs dizaines d'années, et qu'elles sont recueillies et exploitées à des fins commerciales par les opérateurs privés du secteur aérien dans l'indifférence générale des citoyens-passagers. Il peut paraître surprenant que leur utilisation devienne suspecte dès lors qu'elle est le fait de la puissance publique afin de prévenir les crimes les plus graves et d'appuyer les enquêtes.

Les données API sont des données d'enregistrement et d'embarquement collectées, comme leur nom l'indique, lors de ces phases. Il existe seize catégories de données API parmi lesquelles le numéro d'identification du passager, le numéro et le type du document de voyage utilisé, ou encore le nombre, le poids et l'identification des bagages.

Ce système permet aux différents services de sécurité et de renseignement spécialement habilités d'interroger, de manière indirecte, une base de données dans le cadre de finalités limitativement énumérées. En substance, il s'agit de prévenir et de détecter les formes les plus graves de criminalité – actes terroristes, traite d'êtres humains, trafic d'armes par exemple –, mais aussi d'appuyer les enquêtes menées dans ces domaines. Prenons l'exemple imaginaire d'un M. X mis en cause par la justice pour participation à un réseau de trafic de drogue. Le système permettra de confirmer qu'il était présent sur plusieurs vols entre l'Amérique du Sud et la France, en ayant toujours acheté ses billets à la dernière minute sans réservation, sachant que des saisies de drogue d'origine sud-américaine avaient été opérées à l'arrivée de chacun de ces vols.

La France a créé, sur le fondement de l'article 17 de la loi de programmation militaire pour la période 2014-2019, un système expérimental dans le domaine aérien. À l'époque, elle s'était fortement inspirée des dispositions du projet de directive PNR. De fait, la transposition de la directive PNR « finale » n'appelle que des ajustements marginaux de notre système.

La procédure du système français comprend trois étapes.

Les opérateurs concernés transmettent d'abord à un service spécifique, l'Unité Information Passagers (UIP), les données pour l'ensemble des vols à destination et en provenance du territoire national, à l'exception des déplacements reliant deux points de la France métropolitaine. Sont donc concernés les vols internationaux, les vols intra-européens, ainsi que les vols en provenance et à destination des collectivités et territoires ultramarins.

Les différents services habilités peuvent ensuite adresser des requêtes à l'UIP, dans le cadre des finalités limitativement prévues que j'ai brièvement rappelées. Ces services ne disposent donc pas d'un accès direct au système de traitement. Les agents de l'UIP, individuellement désignés et spécialement habilités, traitent la requête après en avoir vérifié la conformité. Ils exploitent les données selon deux méthodes en procédant soit par criblage des individus et des objets, soit par ciblage.

Le criblage consiste à croiser les informations API-PNR avec certains fichiers relatifs à des personnes ou des objets recherchés ou surveillés, comme le fichier des personnes recherchées, ou le système d'information Schengen.

Le ciblage se traduit par l'application de grilles d'analyse des risques qui comprennent différents critères et leur pondération. On détectera, par exemple, l'existence de trajets atypiques avec le cas de passagers se présentant

régulièrement à l'embarquement sans avoir réservé ou, au contraire, ne s'y présentant pas après avoir réservé.

Enfin, l'UIP transmet le résultat de la requête au service demandeur.

Que prévoit la directive 2016/681, dont les articles 5 et 6 assurent la transposition ? Elle a trois objets principaux. Elle oblige les transporteurs aériens à transmettre les données PNR de leurs passagers aux UIP de tous les États membres concernés par les vols extra-Union européenne. Elle permet aux États membres d'étendre cette obligation à tout ou partie des vols intra-Union européenne, sous réserve de le notifier à la Commission européenne. Enfin, elle oblige les États membres à mettre en œuvre des traitements de données alimentés par les informations PNR, aux seules fins de prévenir et détecter les infractions terroristes et les formes graves de criminalité, et de permettre les enquêtes et les poursuites en la matière.

Les modifications à apporter au droit national sont de deux ordres.

Elles concernent les finalités du système. Au-delà des actes terroristes, prévus par la directive comme par notre droit actuel, la liste des « formes graves de criminalité » diffère entre les normes européenne et nationale. La directive retient un champ légèrement plus réduit, prévu à son annexe II. Logiquement, l'article 6 du projet de loi renvoie à cette même annexe afin d'harmoniser le droit français avec le droit européen. Le projet de loi maintient par ailleurs un troisième type de finalité : les atteintes aux intérêts fondamentaux de la Nation, notion inscrite à l'article 410-1 du code pénal. Cette finalité n'est pas prévue par la directive car une telle matière ne relève pas de la compétence de l'Union européenne, mais de celle de chaque État membre, de manière souveraine. Son maintien dans le droit national est donc conforme à la directive.

Les modifications concernent aussi les opérateurs soumis à l'obligation de transmission des données. En l'état du droit en vigueur, les transporteurs aériens ont l'obligation légale de transmettre les données à l'UIP. Les opérateurs de voyage ou de séjour affrétant un aéronef peuvent également y être soumis. Comme la directive le permet, l'article 6 complète la liste des opérateurs concernés, en y ajoutant les agences de voyages.

Pour conclure sur ce sujet je précise que, comme tous les États membres, la France est tenue de transposer la directive 2016/681 avant le 25 mars 2018.

J'en viens à l'article 7 qui concerne le système « PNR maritime ».

La loi du 20 juin 2016 pour l'économie bleue avait prévu un système « PNR maritime » expérimental jusqu'au 31 décembre 2017. L'article 7 pérennise l'autorisation de collecte des données pour les passagers du secteur maritime au-delà de cette date. Il autorise la création d'un système automatisé de traitement de ces données distinct de celui instauré dans le secteur aérien.

Je pense qu'il faut rendre permanent ce système préventif à l'embarquement. La menace terroriste reste malheureusement encore vive, et le secteur maritime présente des vulnérabilités auxquelles il est nécessaire de remédier. Des mesures ont toutefois déjà été prises, comme, dans le domaine de la sécurité portuaire, le renforcement des pelotons de sûreté maritime et portuaire (PSMP), et, dans le domaine de la sûreté des navires en mer, la mise en place, depuis le 1er août 2016, d'équipes de protection des navires à passagers (EPNAP).

Je rappelle l'importance de l'activité des navires à passagers pour la France en termes de flux : elle concerne 32,5 millions de passagers par an. Le trafic transmanche est le plus important, avec 17 millions de passagers environ, suivi par les liaisons entre la Corse et le continent avec quatre millions de passagers. Les outre-mer sont également concernées : l'activité de croisière représente par exemple 1,6 million de passagers aux Antilles.

En substance, les finalités du système « PNR maritime » seront les mêmes que celles prévues pour le système aérien : la prévention et la constatation des actes de terrorisme, des atteintes aux intérêts fondamentaux de la Nation, et d'un certain nombre d'infractions parmi les formes les plus graves de criminalité.

L'obligation de transmission des données s'appliquera aux exploitants de navires pour les passagers à destination ou en provenance du territoire national, quel que soit le pavillon arboré. Les agences de voyage et les opérateurs de voyage ou de séjour affrétant tout ou partie d'un navire pourront également y être soumis.

Quelles seront les modalités d'accès au fichier par les services habilités ? Souhaitant écarter toute possibilité d'accès direct, le Sénat a précisé, en première lecture, que les services devraient interroger une unité spéciale, sorte d'UIP du secteur maritime. S'il s'agit d'une idée intéressante qui enrichit le débat et qu'il ne faut pas exclure de mettre en œuvre dans les années qui viennent, ce dispositif pose aujourd'hui davantage de questions qu'il n'en résout.

Je relève que le système « PNR maritime » sera alimenté par des données qui présentent un degré de sensibilité moindre que le système « API-PNR aérien » – la seule information potentiellement sensible étant la communication des moyens de paiement et de l'adresse de facturation. Dès lors, cela ne justifie pas la mise en œuvre des mêmes modalités de connexion au fichier, telle que l'interdiction d'accès direct par les services.

Par ailleurs, je souhaite insister sur un aspect très pratique. Si une unité de gestion devait être créée, les délais incompressibles pour son installation auraient pour conséquence de priver notre pays des possibilités offertes par le système durant cette période. En effet le système expérimental deviendrait caduc dès la promulgation de la loi, alors que le système pérennisé ne pourrait pas fonctionner avant la mise en place, relativement longue et coûteuse, d'une « UIP maritime ». Il s'agit d'une question complexe que nous allons devoir trancher au cours des

débats et nous échangerons sur ce sujet avec l'exécutif. Un dispositif spécifique devra sans doute être envisagé d'ici à la séance publique.

J'en viens aux dispositions relatives aux techniques de renseignement. Les articles 8 à 9 du projet de loi redéfinissent le régime légal de surveillance des communications hertziennes afin de mettre le droit en conformité avec une récente censure du Conseil constitutionnel.

Je rappelle brièvement les principes qui encadrent l'utilisation des techniques de surveillance, avant de souligner en quoi et pourquoi le régime applicable au domaine hertzien en diffère.

Le régime juridique applicable aux activités et techniques de renseignement a été défini par deux lois de juillet et novembre 2015. Deux types de services peuvent mettre en œuvre ces techniques. Il s'agit, d'une part, des « services spécialisés de renseignement » qui disposent d'une habilitation générale à mettre en œuvre l'ensemble des techniques de surveillance pour l'exercice de leurs missions respectives, et pour l'ensemble des finalités limitativement prévues par la loi. Ces six services constituent le « premier cercle » de la communauté française du renseignement. On y trouve trois services relevant du ministère des Armées : la direction générale de la sécurité extérieure (DGSE), la direction du renseignement militaire (DRM) et la direction du renseignement et de la sécurité de la défense (DRSD). D'autre part, certains services, dits du « second cercle », peuvent être autorisés à recourir à ces techniques, mais uniquement pour certaines finalités et pour une liste définie de techniques.

Qu'en est-il de la procédure ? Par principe, toute demande d'utilisation d'une technique de renseignement destinée à surveiller le territoire national fait l'objet d'une procédure d'autorisation préalable. Elle est délivrée par le Premier ministre, après avis préalable obligatoire, mais simple, de la Commission nationale de contrôle des techniques de renseignement (CNCTR), qui dispose par ailleurs d'un certain nombre de pouvoirs de contrôle.

La surveillance des communications électroniques internationales, reçues ou émises de l'étranger, est soumise à une procédure d'autorisation différente : si elle reste délivrée par le Premier ministre, l'avis de la CNCTR n'est pas légalement requis.

Le régime spécifique au domaine hertzien est appelé « exception hertzienne ». En 1991, le législateur avait choisi d'exclure de la procédure d'autorisation préalable et de contrôle les mesures de surveillance des communications empruntant la voie hertzienne. Ce régime dérogatoire avait été confirmé par la loi de juillet 2015. Ce choix se justifiait par le fait que les mesures mises en œuvre dans le domaine hertzien ne visent pas des communications individualisables, et que, par conséquent, elles ne portent pas atteinte à la vie privée ou au secret des correspondances. En effet, techniquement, ces communications se propagent dans l'espace public sans support filaire. Elles

peuvent donc être librement captées par quiconque dispose d'un récepteur branché sur la bonne fréquence et se trouve dans leur périmètre d'émission. Ce type de communication s'apparente au cas d'un individu qui utiliserait un mégaphone dans la rue : dès lors que vous disposez d'un récepteur, vos oreilles, et que celui-ci est situé dans le périmètre d'émission du message, vous le captez. Son auteur ne peut dès lors prétendre que vous portez alors atteinte à sa vie privée et au secret de ses correspondances, puisqu'il a choisi de le diffuser dans le domaine public.

Le problème réside dans le fait que toutes les communications opérées par la voie hertzienne ne revêtent pas ce caractère intégralement « public ». C'est notamment ce qu'a relevé le Conseil constitutionnel. Saisi d'une question prioritaire de constitutionnalité en 2016, il a jugé que le régime de « l'exception hertzienne » était contraire à la Constitution. Le principal grief étant que ce régime n'excluait pas l'interception de communications ou le recueil de données individualisables. Le Conseil a par ailleurs relevé que la mise en œuvre du régime ne faisait l'objet d'aucune procédure d'autorisation ni d'aucune garantie en termes de contrôle, notamment. Afin de permettre au législateur de tirer les conséquences de cette censure, le Conseil constitutionnel a reporté les effets de sa décision au 31 décembre 2017.

L'objet des articles 8 à 9 du projet de loi consiste donc à redéfinir une « exception hertzienne » conforme aux droits et libertés garantis par la Constitution.

Le maintien de techniques de surveillance dans le domaine hertzien est une nécessité opérationnelle dans trois domaines. Dans le domaine militaire, les interceptions de communications radio longues et très longues distances permettent aux forces armées de disposer d'informations précieuses, y compris lorsqu'elles sont menées depuis le territoire national. Je rappelle à cet égard que notre territoire ne se limite pas à la France métropolitaine. Ces interceptions peuvent par exemple permettre de détecter des mouvements de troupes, de navires ou d'aéronefs étrangers. Dans le domaine de la contre-ingérence, les services peuvent intercepter des communications entre les puissances étrangères et leurs agents. Enfin, en matière de lutte contre le terrorisme, les communications radio peuvent être utilisées par les organisations terroristes et les groupes djihadistes.

Avant de présenter ce que le texte prévoit, ce qu'il est, je tiens d'abord à dire ce qu'il n'est pas : il ne témoigne pas d'une volonté de surveillance généralisée, et ne permettra pas aux services d'écouter plus qu'avant. Il leur permettra d'écouter et de surveiller autant, mais dans un cadre juridique renouvelé, conforme aux droits et libertés garantis par notre Constitution. Il sera plus protecteur des libertés publiques, du respect de la vie privée et du secret des correspondances, car il sera entouré de garanties inédites dans le domaine de l'hertzien « public ».

L'article 8 du projet de loi limite donc « l'exception hertzienne » au strict nécessaire. Il crée à cet effet un dispositif à double entrée, qui en restreint le champ.

L'hertzien « privé » concernera les communications qui empruntent exclusivement la voie hertzienne, sans intervention d'un opérateur, mais qui revêtent malgré tout un caractère privé. Les demandes de surveillance dans ce domaine seront dorénavant soumises au droit commun, avec autorisation préalable du Premier ministre et contrôle de la CNCTR.

L'hertzien « public » concernera les communications qui empruntent exclusivement la voie hertzienne, sans intervention d'un opérateur, mais qui ne relèvent d'aucun réseau privatif. Leur surveillance restera logiquement soumise à un régime allégé sans autorisation préalable, comme c'est le cas actuellement, mais des modalités inédites de contrôle *a posteriori* par la CNCTR seront prévues – nous y reviendrons.

Comment faire la distinction entre hertzien « privé » et hertzien « public » ? L'hertzien « privé » regroupera les communications échangées au sein d'un réseau réservé à l'usage d'un groupe fermé d'utilisateurs. C'est le recours à certains modes de communication qui permettra de le déterminer. Le principal équipement concerné serait le talkie-walkie numérique ou PMR (*Private Mobile Radio*), qui se caractérise, d'une part, par sa portée limitée, d'autre part, par l'intégration dans l'appareil de mécanismes d'authentification et de partage de clés de chiffrement. De fait, son utilisation révèle bien l'intention des utilisateurs de conférer un caractère privé à leurs échanges, quand bien même ceux-ci empruntent le domaine public que constitue l'hertzien.

La nouvelle « exception hertzienne » sera dorénavant expressément et légalement limitée au seul hertzien « public », conformément aux prescriptions du Conseil constitutionnel. Son nouveau champ sera résiduel, car limité aux communications qui ne relèvent d'aucun réseau privatif, et qui ne peuvent être interceptées sur le fondement d'aucune des autres techniques de renseignement.

Au total, la grande majorité des interceptions hertziennes sera soumise au droit commun, ce qui constitue un progrès considérable en termes de respect des droits et libertés. Concrètement, le nouveau champ couvrira uniquement la CB, les radioamateurs, les talkies-walkies analogiques ainsi que les communications radio des gammes VLF et HF et les moyens radio militaires tactiques. Bref, l'« exception hertzienne » et le régime dérogatoire qui y est attaché deviendront réellement « exceptionnels ».

Je vous proposerai deux amendements dans ce domaine. Le premier précisera le point de départ des délais de conservation des informations collectées. Le second aura trait aux modalités de contrôle de la CNCTR : il s'agit de lui donner accès non pas à l'ensemble des renseignements collectés, puisque ceux qui

s'avèrent inutiles sont détruits par les services, mais aux seuls renseignements effectivement conservés et exploités par ces derniers.

Enfin, l'article 9 permettra aux unités des armées chargées de la défense militaire de continuer à mettre en œuvre des mesures de surveillance hertzienne, dans le cadre du seul hertzien « public », et uniquement pour l'exercice de leurs missions. Ces missions ont trait à la dissuasion nucléaire, à la défense opérationnelle, à la défense maritime du territoire et à la défense aérienne ; elles s'exercent également dans le cadre de l'action de l'État en mer. De telles mesures pourraient, par exemple, permettre de détecter la présence d'embarcations communiquant entre elles sur l'hertzien « ouvert », et qui chercheraient à pister un sous-marin nucléaire lanceur d'engins sortant de la base de l'Île-Longue, au large de Brest.

Les modalités de contrôle par la CNCTR seront allégées par rapport au régime prévu pour les mesures de surveillance de l'hertzien « ouvert », dans le cadre d'actions de renseignement. Un tel allégement est légitime : d'une part, puisqu'il s'agit de communications non privatives, les mesures prises par les unités militaires ne sont pas attentatoires aux libertés publiques ; d'autre part, ces mesures, qui ne constituent pas des actions de renseignement au sens de la surveillance administrative, ont une visée purement opérationnelle.

Le même article permet également à la Direction générale de l'armement (DGA) d'effectuer des interceptions sous le régime de « l'exception hertzienne », mais à une fin unique et précise : la conduite des campagnes d'essai des matériels utilisés par les forces armées et permettant la mise en œuvre de mesures de surveillance. Toutes les données collectées dans le cadre des tests des matériels sont, bien entendu, immédiatement détruites par la DGA.

Mes chers collègues, je vous prie de m'excuser d'avoir été un peu long, mais il s'agit de sujets relativement complexes, et j'espère avoir été suffisamment clair pour que chacun des membres de notre commission puisse prendre la mesure des enjeux des articles qu'il nous revient d'examiner pour avis.

M. le président. Les dispositions qui figurent dans ce projet de loi visant à compléter notre dispositif de lutte contre le terrorisme sont effectivement très techniques. Avant de passer à l'examen des seize amendements que j'ai reçus sur ce texte, certains de nos collègues souhaitent vous poser quelques questions, Monsieur le rapporteur pour avis.

M. Jean-François Eliaou. J'aimerais savoir s'il y aura des liaisons et des interactions possibles entre le PNR aérien et le PNR maritime : ce point est important car, à défaut de pouvoir croiser les données, il me semble que nous perdrions un peu en efficacité.

Par ailleurs, y aura-t-il des connexions entre le PNR maritime français et ceux d'autres pays européens, et la Corse sera-t-elle incluse dans le PNR français ?

J'ai entendu dire qu'il était question de créer deux PNR maritimes français, l'un pour la côte méditerranéenne, l'autre pour l'Atlantique. Si cela devait être le cas, les données de ces deux PNR pourraient-elles être croisées ?

Enfin, je n'ai pas très bien compris si vous étiez favorable ou non à la création d'une UIP maritime : pourriez-vous nous préciser les enjeux de cette question ainsi que votre position ?

M. Christophe Lejeune. J'ai compris que les fichiers ne concerneraient que les personnes suspectées d'actes liés au terrorisme, et que nos services secrets ne disposeraient pas d'un accès direct à ces fichiers, mais devraient passer par l'intermédiaire d'UIP. Pouvez-vous nous préciser qui nommera les personnes constituant les UIP et qui aura autorité sur elles ?

M. Bastien Lachaud. Plutôt que de poser une question, j'aimerais faire une intervention à caractère général sur le texte de loi, en commençant par rappeler que notre pays s'est doté de six lois antiterroristes depuis 2012, et que c'est donc la septième loi de ce genre qui nous est soumise aujourd'hui. Le fait de revenir aussi régulièrement sur le même sujet montre, à mon sens, que l'on n'aborde jamais les vrais problèmes, ou que l'on n'y apporte pas les bonnes solutions. Cela me semble être malheureusement encore le cas avec ce texte, qui tient surtout de l'affichage, avec la pérennisation dans l'État de droit des mesures d'exception de l'état d'urgence.

En procédant de la sorte, nous ne posons pas les questions qui seraient pertinentes pour lutter contre la commission d'actes terroristes, notamment celle des moyens financiers et humains accordés aux services de renseignement, celle de la traque de l'argent servant au financement du terrorisme – en particulier dans le cadre des paradis fiscaux –, celle des alliances stratégiques nouées par la France avec des États qui encouragent la commission d'actes terroristes, ou encore celle de la participation de la France à la déstabilisation de régions entières du fait de décisions prises par des présidents de la République sans contrôle du Parlement, contrairement à ce que prévoit l'article 35 de la Constitution.

Par ailleurs, les mesures d'exception de l'état d'urgence vont perdre en efficacité en même temps qu'elles vont perdre leur caractère d'exception, car les personnes souhaitant commettre des actes terroristes vont pouvoir contourner plus facilement des dispositions qu'ils connaissent bien.

Un bilan des mesures d'exception passées dans le droit commun, notamment aux États-Unis à la suite des attentats du 11 septembre 2001, montre que les facilités accordées à l'exécutif se sont révélées inefficaces, voire contre-productives. En effet, le fait de revenir sur notre État de droit constitue une victoire morale pour nos adversaires, et les mesures intégrées au droit commun sont dévoyées pour entraver l'action syndicale ou la défense de l'environnement, voire d'autres formes de mobilisation nécessaires à la vie démocratique. Nous portons donc atteinte à l'État de droit en permettant de faire subir indûment des

atteintes à la vie privée, des mesures vexatoires ou simplement arbitraires à nos concitoyens qui, de ce fait, ne trouvent plus dans la République la sûreté qu'ils sont en droit d'en attendre.

La logique générale de ce texte est celle d'un approfondissement de ce que certains appellent déjà une « démocrature » à propos de pays que nous jugeons d'habitude avec sévérité. Parallèlement au coup d'État social que représentent les ordonnances relatives à la réforme du code du travail qui, si nous ne les empêchons pas, feront vivre les salariés dans la crainte de l'arbitraire d'un licenciement abusif jamais véritablement puni, ce texte constitue une autre façon de saper l'État de droit, qui est justement ce que nos ennemis cherchent à abattre.

Je voudrais conclure en vous rappelant l'avertissement lancé par un penseur insoupçonnable à vos yeux, le libéral Benjamin Constant, qui, il y a deux cents ans, disait déjà : « Lorsque l'arbitraire frappe sans scrupule les hommes qui lui sont suspects, ce n'est pas seulement un individu qu'il persécute, c'est la nation entière qu'il indigne d'abord et qu'il dégrade ensuite (…) L'arbitraire est dangereux pour un gouvernement considéré sous le rapport de son action ; car, bien qu'en précipitant sa marche, il lui donne quelquefois l'air de la force, il ôte néanmoins toujours à son action la régularité et la durée ».

M. Joaquim Pueyo. Je suis très favorable à une mise en œuvre rapide et concrète du PNR européen qui, je le rappelle, correspond à une recommandation que nous avions formulée en juillet 2016 dans le cadre du rapport que la mission d'information sur les moyens de Daech et adoptée à l'unanimité.

La problématique du retour de ceux que l'on appelle les « combattants étrangers », à savoir les Français qui se sont rendus dans la zone irako-syrienne pour y rejoindre des organisations terroristes, nous oblige à renforcer les contrôles des déplacements de ces individus afin de pouvoir les intercepter à leur retour, notamment quand ils évitent le transport aérien au profit du transport maritime – une pratique qui justifie à elle seule la création d'un PNR maritime.

La lutte contre les faux passeports renforcera l'utilité et l'efficacité du PNR si l'on fait en sorte d'imposer la biométrie à l'ensemble des passeports au sein de l'Union européenne. Pour ce qui est du PNR maritime, nous sommes favorables au texte.

Si le rôle de la CNCTR, réintroduite à plusieurs reprises par le Sénat, me paraît fondamental, il est permis de se demander si elle disposera de moyens suffisants pour exercer la mission de contrôle qui lui sera confiée – une mission extrêmement importante, car le contrôle est indissociable de l'État de droit.

J'apprécie que la délégation parlementaire au renseignement (DPR) puisse se faire communiquer les observations de la CNCTR, ce qui permettra au Parlement d'exercer pleinement sa mission de contrôle.

Les dispositions les plus délicates de ce texte sont sans doute celles relatives à la surveillance hertzienne. Cependant, les observations formulées par le Conseil constitutionnel ont été prises en compte, ce qui constitue à mes yeux une garantie importante et me permettra de voter en faveur de ces dispositions, comme je le ferai pour le reste du texte.

M. le rapporteur pour avis. À l'heure actuelle, il n'existe pas de lien entre le PNR aérien et le PNR maritime, et le véritable enjeu réside dans la possibilité de coordonner le PNR aérien français à ceux des autres États de l'Union européenne. Je répète que le PNR aérien et le PNR maritime sont appelés à contenir des données différentes en nature et en nombre – seize à dix-neuf catégories de données pour le PNR aérien, une dizaine pour le PNR maritime.

Pour ce qui est du PNR maritime, il concerne tous les ports français, y compris ceux de la Corse et ceux situés outre-mer.

Avant la mise en place de l'Unité Information Passagers, les données du PNR aérien étaient déjà collectées par les compagnies privées ; la création de l'UIP est donc la bienvenue en ce qu'elle confère aussi cette compétence à la puissance publique. Pour ce qui est du PNR maritime, c'est aujourd'hui la gendarmerie maritime qui est destinataire des données adressées par les compagnies maritimes. Une réflexion sera à mener, au cours des années à venir, sur la constitution, d'ores et déjà envisagée, d'une ou deux unités de gestion chargées de la collecte des données auprès des transporteurs maritimes. À titre personnel, je suis favorable à ce qu'il ne soit créé qu'une seule unité – à l'instar de ce qui se fait dans le domaine aérien, avec l'unité basée à Roissy – plutôt qu'une unité pour la façade atlantique et une autre pour la Méditerranée. Cela dit, si l'exigence de la création d'une UIP dédiée au secteur maritime subsiste dans le texte, le PNR maritime ne pourra pas fonctionner au 1er janvier 2018.

Pour répondre à M. Lejeune, je précise que les agents de l'UIP sont nommés par décret. L'UIP est une unité interministérielle basée à Roissy et rattachée au ministère chargé des douanes, mais qui exerce aussi ses missions pour le compte des ministères des Armées, de l'Intérieur et des Transports.

M. Lachaud a développé des considérations à caractère politique, auxquelles je répondrai par des éléments d'ordre technique. Premièrement, ce texte est nécessaire, car il faut bien sortir de l'état d'urgence, qui n'a pas vocation à devenir un état permanent. Deuxièmement, ce texte est responsable, puisque nous sommes en train d'atteindre l'équilibre recherché. Il porte enfin la marque d'un certain courage, une qualité nécessaire pour mettre fin à la prorogation permanente de l'état d'urgence.

Je rappelle par ailleurs que les cinq articles que nous examinons ne sont pas issus de dispositifs se rattachant à l'état d'urgence, mais qui existent déjà, et qu'il nous appartient de mettre en conformité avec le droit. Ainsi, l'exception hertzienne remonte à 1991, et c'est le Conseil constitutionnel qui nous a demandé

de mettre ce dispositif en conformité avec la Constitution – c'est l'objet des articles 8 et 9 du projet de loi, qui vont dans le sens d'un renforcement de la protection de nos libertés publiques.

M. Pueyo soulève une vraie question, celle des moyens de la CNCTR et du rôle du Parlement. Sur ce point, nous devons saluer le travail accompli par nos collègues sénateurs. À l'origine, le texte prévoyait, pour l'hertzien « public », un filtre sous la forme d'une autorisation préalable du Premier ministre, que le Sénat a supprimé et que le Gouvernement ne semble pas désireux de réintroduire : nous devrions donc en rester à un contrôle direct de la CNCTR.

Les sénateurs ont, par ailleurs, introduit un article 8 *bis* qui me semble aller dans le bon sens, puisqu'il introduit la DPR. Désormais, la CNCTR devra rendre compte devant la DPR des observations qu'elle aura à formuler au sujet des interceptions hertziennes.

La commission en vient à l'examen des articles dont elle s'est saisie pour avis.

Article 5 (art. 17 de la 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) : *Pérennisation du traitement des données relatives aux passagers aériens, dit « système API-PNR France »*

La commission est saisie de l'amendement DN6 de M. Bastien Lachaud.

M. Bastien Lachaud. L'article 5 propose de pérenniser une mesure qui ne devait rester en vigueur que jusqu'au 31 décembre 2017 : le législateur précédent entendait en effet donner un caractère temporaire au fichier de traitement automatisé qu'est l'API-PNR, une intention sur laquelle nous devrions pour le moins nous interroger. Ne s'agissait-il pas de se donner le temps de vérifier l'utilité de cette mesure et les risques d'atteinte à l'État de droit qu'elle comporte ? Alors que la Commission nationale de l'informatique et des libertés (CNIL) affirmait, en août 2016, que ce fichier créé à titre expérimental devrait faire l'objet d'une évaluation avant d'envisager ou non son maintien, aucune étude n'a jamais prouvé l'utilité de conserver ces données personnelles pour une durée maximale de cinq ans.

Estimant que vous avez l'intention de faire entrer dans le droit commun une disposition dont personne ne peut garantir aujourd'hui le bien-fondé, nous proposons pour notre part de supprimer l'article 5, afin d'éviter de pérenniser un traitement de données que nous estimons attentatoire au droit à la vie privée.

M. le rapporteur pour avis. Je suis un peu déçu de constater que mon exposé liminaire ne semble pas avoir convaincu tous nos collègues. Je suis défavorable à cet amendement, comme je le serai à l'amendement DN7 visant à supprimer l'article 6, et pour les mêmes raisons.

Sur le plan juridique, la France est tenue de transposer la directive PNR : il s'agit à la fois d'une obligation en vertu des traités ratifiés par notre pays et d'une exigence constitutionnelle. Pour ce faire, les articles 5 et 6 doivent être adoptés. Dans le cas contraire, nous manquerions à nos engagements européens et à nos règles constitutionnelles.

Sur le fond, comme je l'ai dit, le système API-PNR – dont on nous a confirmé l'efficacité au cours de plusieurs auditions, en dépit de ce que vous affirmez – n'est pas seulement un outil de prévention – et pas uniquement du terrorisme –, c'est également un outil précieux d'appui aux enquêtes, qui permet de confondre les individus mis en cause par la justice pour la commission des infractions les plus graves.

Nous avons des divergences de fond en la matière, qui auront plutôt vocation à se confronter dans l'hémicycle. Si cela peut vous donner un peu d'espoir, sachez qu'un réexamen de tous les éléments de la directive PNR est prévu d'ici à 2020. Vous pourrez donc, le moment venu, mobiliser vos représentants au Parlement européen pour faire valoir à nouveau vos arguments. En attendant, notre pays se conformera à ses obligations.

M. Jean-Christophe Lagarde. En quoi la directive européenne exige-t-elle que les dispositifs deviennent permanents ?

M. le rapporteur pour avis. La directive européenne oblige à mettre en place une UIP dans chaque État-membre et à créer des traitements de données alimentés par les informations API-PNR.

M. Jean-Christophe Lagarde. À mon sens, elle demande à ce que soit mis en place un fichier PNR, mais n'exige pas que ce fichier soit pérenne. La souveraineté de la France n'est pas en cause, puisque l'Europe ne nous contraint pas à rendre le fichier permanent. Ce qui avait été adopté sous la législature précédente suffisait à répondre à l'exigence européenne, en prévoyant un réexamen périodique effectué dans le cadre du contrôle parlementaire. Il serait donc vain de prétendre que c'est l'Europe qui nous interdit de prendre la décision de revoir nos procédures – ce qui ne saurait se faire que d'un commun accord avec les autres pays, dans la mesure où le PNR est un fichier partagé.

M. le rapporteur pour avis. Je le répète, une révision sera possible d'ici 2020.

*La commission **rejette** l'amendement.*

La commission examine l'amendement DN2 de M. Stéphane Trompille.

M. Stéphane Trompille. Après avoir échangé avec le rapporteur pour avis, je retire mon amendement.

M. le rapporteur pour avis. La disposition prévue créerait en effet une trop lourde charge et du reste l'amendement est mal placé.

L'amendement est ***retiré.***

La commission émet un avis ***favorable*** *à l'adoption de l'article 5* ***sans modification****.*

Article 6 (art. L. 232-1 et L. 232-7 du code de la sécurité intérieure) : *Transposition de la directive « PNR »*

La commission examine l'amendement DN7 de M. Alexis Corbière.

M. Alexis Corbière. L'amendement DN7 vise à supprimer l'article. Je remercie le rapporteur pour avis d'avoir eu la franchise de nous indiquer que les dispositifs que nous examinons ne sont pas la transposition de l'état d'urgence mais que la majorité entend saisir l'occasion qui lui est ici offerte pour légiférer sur toute une série de sujets, profitant d'une sorte d'effet d'aubaine, si je puis m'exprimer ainsi.

Disons clairement aux Français que si le PNR avait été en vigueur, il n'aurait eu aucune efficacité pour empêcher les attentats qui ont frappé la France : aucun des criminels impliqués n'a pris l'avion. Aussi la généralisation envisagée des contrôles nous engage-t-elle dans une spirale sécuritaire consistant, notre collègue Lachaud y a fait allusion, à donner une forme de victoire à nos adversaires.

En outre, nous créerions des outils potentiellement très dangereux puisque les fichiers en question doivent être partagés au niveau européen et qu'ils sont donc susceptibles de tomber on ne sait entre quelles mains ; or, il convient d'éviter toute remise en cause possible des libertés fondamentales.

Je vous propose donc de supprimer cet article, j'y insiste, inopportun, inefficace, problématique sur le fond.

M. le rapporteur pour avis. Avis défavorable pour les mêmes raisons que celles invoquées pour rejeter l'amendement DN6.

M. Fabien Gouttefarde. Je reviens sur le procès en inefficacité fait au PNR. Je rappelle l'existence d'un rapport d'information du 16 novembre 2011, remis par notre ancien collègue Guy Geoffroy, qui concluait, à propos du PNR, que l'Union européenne et les États-Unis s'accordent « sur le grand intérêt de ces données dans la lutte contre le terrorisme et la criminalité grave ». Les données PNR ont en effet fait la preuve de leur efficacité dans cette lutte. Aussi, je vous invite à lire une partie du rapport en particulier, celle portant sur « l'intérêt des données PNR d'après les expériences menées dans les autres États membres ».

Je prends au hasard l'exemple du programme britannique « *e-borders* » qui comprend des données PNR. Au moment de la remise du rapport Geoffroy,

330 millions de mouvements de passagers avaient été analysés et il avait été procédé à 89 000 arrestations dont celles de terroristes et de trafiquants. C'est pourquoi, dès lors que l'on tient compte de l'avis des services du renseignement et de celui des professionnels de la sécurité, il n'y a pas lieu, dans cette enceinte, de douter de l'efficacité du dispositif proposé.

M. Stéphane Trompille. Comment M. Corbière peut-il affirmer qu'aucune des personnes impliquées dans les actes terroristes qui ont frappé la France n'a pris l'avion ?

M. Patrice Verchère. On imagine ce qu'aurait permis le PNR s'il avait existé bien plus tôt, quand on se rappelle que Mehdi Nemmouche a atterri le 18 mars 2014 à Francfort, de retour de Syrie, deux mois avant l'attaque – dont il est l'auteur présumé – du Musée juif de Belgique, à Bruxelles, qui a provoqué la mort de quatre personnes. Hayat Boumeddiene, quant à elle, a pu s'envoler vers la Turquie, depuis Madrid, une semaine avant que son compagnon, M. Coulibaly, ne tue neuf personnes au cours de la prise d'otages de l'Hyper-Cacher de la Porte de Vincennes.

S'il est vrai que le PNR n'est sans doute pas un dispositif suffisant – malgré tout son intérêt –, il nous apparaît toutefois nécessaire. Aussi soutenons-nous cet article et sommes-nous défavorables au présent amendement de suppression.

M. Alexis Corbière. Le PNR ne permettra pas aux autorités de savoir si un individu qui aura pris l'avion une fois est dangereux.

Vous évoquiez le rapport de M. Geoffroy, mon cher collègue, mais je vous rappelle que le G29, le Groupe européen des autorités de protection des données, a constaté en 2010, dans le cadre du PNR nord-américain, « qu'il n'a jamais été prouvé de façon concluante que la quantité considérable de données passagers collectée est véritablement nécessaire à la lutte contre le terrorisme et la grande criminalité ». N'essayez-vous pas plutôt, dès lors, de compenser, par le biais du PNR, le manque de moyens dont disposent nos services de renseignement ?

Le recueil et l'exploitation des métadonnées ne résoudront pas le problème : c'est le renseignement humain qui permettra de lutter efficacement contre le terrorisme. C'est une des difficultés que nous sommes en train de mettre en évidence.

Je maintiens donc mon amendement de suppression.

M. Jean-Christophe Lagarde. Il faut en revenir à certaines réalités. Il est évident que quand on collecte des informations sur des centaines de millions de déplacements, aucun service de renseignement ne les analysera individuellement. Le seul intérêt, en réalité, pour les services de renseignement et les services de police, est de pouvoir retracer les parcours de personnes soupçonnées d'être

dangereuses ou bien jugées telles. Il s'agit donc d'établir quelles peuvent être les correspondances entre ces parcours.

Affirmer que le PNR est en mesure d'empêcher les attentats est tout aussi péremptoire qu'affirmer qu'il ne servirait à rien dans le combat contre le terrorisme est hasardeux – pour rester gentil.

On a évoqué précédemment les circuits de financement – et je suis d'accord pour considérer qu'il devrait s'agir d'une priorité – ; eh bien, ces derniers impliquent des déplacements qu'on peut recroiser avec les déplacements de ceux qui ont commis des attentats. C'est exactement la même chose que lorsqu'il s'agit de surveillance électronique. C'est d'ailleurs ainsi que l'on constate, quitte à surprendre, peut-être, le commun des mortels, qu'après la commission d'un acte ou sa tentative, après une interpellation, après une opération de police fortuite – je pense ici aux découvertes récentes à Villejuif –, en recoupant les données électroniques, les informations sur les déplacements, on finit par reconstituer des réseaux. Voilà à quoi sert le PNR.

En revanche – et j'explique ici mon vote de tout à l'heure –, si le PNR est une contrepartie nécessaire à la guerre menée contre nous ainsi qu'à la facilitation, ces dernières années, de la liberté de circulation, nous devrions veiller à ce que le débat sur ce dispositif ne soit pas clos. En effet, malgré tout, le recueil et l'exploitation de ces métadonnées sont susceptibles, à un moment ou à un autre, de porter atteinte à certaines libertés fondamentales. C'est pourquoi l'article 5 devrait prévoir une limite dans le temps, au terme de laquelle nous serions amenés à nous prononcer sur l'éventuelle prorogation du dispositif. Or ne pas fixer cette limite, interdire tout débat parlementaire, toute discussion avec les experts, me paraît une erreur : ces fichiers sont nécessaires parce que nous vivons une situation particulière : la lutte contre le terrorisme dont nous savons qu'elle va durer plusieurs années mais dont nous pouvons espérer un jour la fin.

Mme Sereine Mauborgne. Dans ce cas, Monsieur Lagarde – question de béotienne –, pourquoi n'avez-vous pas déposé d'amendement à cet effet ?

M. Jean-Christophe Lagarde. Madame le député, chère collègue, je ne suis pas sûr que vous ayez à juger mon travail – et je ne me permettrais pas de juger le vôtre. Mais on verra.

M. le président. Restons-en là pour le moment.

M. le rapporteur pour avis. Il est toujours possible de débattre en séance publique.

Je précise qu'il y a un fichier PNR pour chaque État – il n'y a pas, aujourd'hui, de fichier européen. Aussi l'une des grandes tâches à mener dans les années à venir est-elle l'amélioration de la coordination de nos différents systèmes.

*La commission **rejette** l'amendement.*

*Puis elle émet un avis **favorable** à l'adoption de l'article 6 **sans modification**.*

Article 7 (art. L. 232-4, L. 232-7 et L. 232-7-1 [nouveau] du code de la sécurité intérieure) : *Création d'un fichier « PNR maritime »*

La commission examine l'amendement DN8 de M. Bastien Lachaud.

M. Bastien Lachaud. Je réserve mon argumentation sur le fond pour le débat en séance publique. Je me borne en attendant à indiquer qu'elle est la même, pour cet amendement de suppression de l'article, que pour les précédents.

M. le rapporteur pour avis. Je l'ai rappelé tout à l'heure, le secteur maritime présente des vulnérabilités alors qu'il représente des flux considérables. Je considère qu'on ne peut pas faire comme si la menace s'arrêtait aux quais de nos ports. Il est normal qu'un contrôle préalable à l'embarquement puisse être effectué. Mais, là encore, nous en débattrons en séance publique.

Avis défavorable.

*La commission **rejette** l'amendement.*

*Puis elle émet un avis **favorable** à l'adoption de l'article 7 **sans modification**.*

Après l'article 7

La commission examine l'amendement DN3 de Mme Frédérique Lardet.

Mme Frédérique Lardet. Le présent amendement concerne le renforcement des moyens mis à disposition des forces de polices et des forces armées dans le cadre de leurs missions de surveillance des périmètres de protection. Mais, après discussion avec le rapporteur pour avis, il semble préférable d'en faire un amendement portant article additionnel après l'article 1er qui sera examiné en commission des Lois. C'est pourquoi je retire mon amendement.

*L'amendement est **retiré**.*

Chapitre II

Techniques de renseignement

Article 8 (art. L. 822-2, L. 852-2 [nouveau], L. 853-2, L. 854-9-1 à L. 854-9-3 [nouveaux] et L. 871-1 du code de la sécurité intérieure) : *Encadrement de la faculté de procéder à des écoutes hertziennes*

La commission examine l'amendement DN9 de M. Alexis Corbière.

M. Alexis Corbière. Franchement, je n'ai pas compris en quoi le texte levait les réserves faites par le Conseil constitutionnel en 2016. Nous créerions ici un gigantesque aspirateur de données hertziennes dont certaines touchant à la vie privée. Cela concernera aussi bien le wifi que le *bluetooth* ou encore la téléphonie 3G… J'insiste : les réserves formulées par le Conseil constitutionnel ne sont pas du tout obsolètes. Cet article nous paraissant liberticide en ce qu'il ne garantit pas le respect des correspondances privées notamment, il serait sage de le supprimer.

M. le rapporteur pour avis. Notre point de vue, ici aussi, diverge.

Tout d'abord, le Conseil constitutionnel n'a pas censuré le principe même de la surveillance de l'hertzien privatif, comme vous semblez l'indiquer dans l'exposé sommaire de votre amendement. Il a censuré les conditions dans lesquelles elle s'opérait jusqu'alors. Le projet de loi répond aux exigences du Conseil constitutionnel en créant le système de double entrée que j'évoquais tout à l'heure et en prévoyant des garanties inédites dans le domaine hertzien.

Vous dites également qu'il s'agit d'une nouvelle collecte de données. Or, je le répète : c'est faux. Les services ne surveilleront pas davantage qu'avant : ils surveilleront autant, mais dans un cadre plus protecteur des droits et des libertés, conformément à la décision du Conseil constitutionnel.

Je le redis : le présent projet de loi fait entrer le hertzien privé – dont le seul mode de communication visé est le talkie-walkie numérique – dans le droit commun, avec toutes les garanties légales y afférant.

Vous notez que sont notamment cités des exemples hors de France. C'est parce qu'une action menée depuis le territoire national peut aussi permettre d'intercepter des communications à l'étranger, compte tenu des fréquences et des longueurs d'onde utilisées – dans le cadre, en particulier, de nos opérations de défense.

L'article 8 répondant aux objections du Conseil constitutionnel, je suis défavorable à cet amendement.

*La commission **rejette** l'amendement.*

Puis elle examine les amendements DN5 et DN16 de Mme Frédérique Lardet.

Mme Frédérique Lardet. À la suite des explications apportées par le rapporteur pour avis, je retire ces deux amendements.

*Les amendements DN5 et DN16 sont **retirés.***

La commission examine ensuite, en discussion commune, les amendements DN17, de M. le rapporteur pour avis, et DN4 de Mme Frédérique Lardet.

M. le rapporteur pour avis. L'amendement DN17, d'ordre technique, vise à préciser le point de départ des délais de conservation des données en prévoyant qu'ils courent à compter de leur recueil pour les renseignements non chiffrés – soit six ans –, et à compter de leur déchiffrement pour les renseignements chiffrés – à savoir huit ans.

Mme Frédérique Lardet. Je retire l'amendement DN4 au profit de celui du rapporteur pour avis.

L'amendement DN4 est ***retiré.***

M. Jean-Christophe Lagarde. Le rapporteur pour avis a qualifié son amendement de technique. Il l'est relativement… Pourquoi le délai de conservation des données chiffrées est-il deux ans plus long que le délai de conservation des données non chiffrées ? C'est, me semble-t-il, supposer que, pendant les deux premières années, on peut, le cas échéant, déchiffrer les renseignements et qu'ensuite on ne les déchiffrera pas et qu'on ira les rechercher la septième et la huitième année, au cas où… Bref, je comprends votre intention mais moins le mécanisme consistant à prévoir deux délais différents alors que seul le déchiffrement compte.

M. le rapporteur pour avis. C'est le droit commun applicable aux communications électroniques internationales. En outre, les données chiffrées sont par définition plus complexes à traiter, ce qui explique que les délais soient un peu plus longs que pour les données non chiffrées, souvent traitées immédiatement par nos services.

M. Thibault Bazin. Qu'en est-il de la coopération des services de sécurité et de justice des États européens ? Nous collectons des données mais les différents pays les partagent-ils ? Le texte ne l'évoque pas du tout. On sait que des progrès ont été accomplis depuis vingt ans mais le niveau de partage des données *via* le *hub* d'information Europol semble *a priori* encore insuffisant malgré la recrudescence d'attentats depuis deux ans et demi. Qu'avez-vous à nous dire sur la question, monsieur le rapporteur pour avis ?

M. le rapporteur pour avis. Je l'ai précisé moi-même tout à l'heure : ce sera l'une de nos tâches, dans les années à venir, que d'améliorer la coopération entre nos services de renseignement au niveau européen, mais qui ne me semble pas l'objet du présent texte – à dimension nationale.

M. Thibault Bazin. Il n'y a donc rien de prévu à l'échelle internationale…

M. le rapporteur pour avis. Les discussions ont lieu au cas par cas, en fonction des affaires. Reste que les États ont conscience de la nécessité d'améliorer notre système de coopération. Nous reviendrons par conséquent régulièrement sur ces questions dans les mois et les années qui viennent puisque, hélas, elles se posent à chaque fois qu'un attentat est commis. On doit néanmoins

noter des améliorations, comme on a pu le constater lors du terrible attentat de Barcelone, à la suite duquel les services français et espagnols ont très rapidement coopéré.

M. Thibault Bazin. De même qu'après l'attentat de Berlin.

M. le rapporteur pour avis. En effet.

La commission ***adopte*** *l'amendement DN17.*

Puis elle en vient à l'amendement DN18 du rapporteur pour avis.

M. le rapporteur pour avis. Le présent amendement concerne le champ des renseignements auxquels la CNCTR aura accès. Parmi les données que collectent nos forces de renseignement, il y a des données brutes qu'elles détruisent immédiatement, d'autres qu'elles conservent sans pour autant les traiter, enfin les données qu'elles conservent et traitent. Il s'agit par conséquent de préciser que le contrôle de la CNCTR portera non pas sur toutes les données interceptées mais sur les données collectées conservées et les données collectées conservées et traitées.

Cette précision vise là encore à ne pas mettre nos services en difficulté. Il est entendu que, dans la majeure partie des cas, nous évoquons des contrôles faits lors d'une opération de défense et non dans le cadre d'une opération de lutte contre le terrorisme sur le territoire national. Si, dès lors, les données ayant vocation à être immédiatement détruites devaient être conservées, il conviendrait de procéder à de nouveaux investissements pour améliorer nos dispositifs de stockage.

M. Jean-Christophe Lagarde. Je vais voter contre l'amendement du rapporteur. S'il était prévu que les données collectées et immédiatement jetées ne pourraient plus faire l'objet du contrôle de la CNCTR, j'aurais déjà un doute. Or, l'amendement précise que ladite commission ne peut plus contrôler ce qui a été collecté et jeté entre le moment de la collecte et celui du contrôle. Le contrôle, disons les choses clairement, n'est pas réalisé à chaque minute, au jour le jour, mais il est périodique. Cela signifie qu'entre le moment où les services de renseignement ont collecté les données et celui où ils les ont jetées, il peut s'être passé plein de choses. Et il faut être naïf pour penser que les services de renseignement ne peuvent pas extraire un renseignement, le conserver et le traiter ailleurs… On peut même avoir décidé d'une écoute, même relevant du domaine de la défense, écoute sur la légitimité de laquelle la CNCTR devrait pouvoir s'interroger, et ne pas avoir trace de cette collecte à un moment où à un autre.

Dès lors que les données en question sont conservées un ou plusieurs jours, la commission doit savoir qu'une interception a eu lieu. Le traitement d'une donnée peut en effet parfaitement ne pas être déclaré puisqu'on va vous expliquer ensuite qu'on ne l'a jamais interceptée… Je ne suis pas soupçonneux vis-à-vis des services de renseignement mais je pense qu'il faut les protéger d'eux-mêmes. En

effet, le besoin opérationnel pousse parfois à utiliser de façon excessive un droit qui serait insuffisamment contrôlé.

Mme Natalia Pouzyreff. En matière de collecte de données de type hertzien effectuée par nos forces de défense, il n'y a pas de déclaration ni de tri *a priori* puisque l'écoute est réalisée sur une large bande de fréquence.

M. le rapporteur pour avis. Dès lors qu'une donnée est conservée ne serait-ce que quelques jours, il en reste une trace, donc la CNCTR pourra la contrôler. J'ajoute que la CNCTR réalise un travail assez considérable et rend des avis – dont le nombre reste confidentiel. C'est une partie du « brut », le « bruit » qui, en fait, est immédiatement jeté.

M. Jean-Christophe Lagarde. Votre amendement prévoit d'ajouter les mots : « conservés à la date de sa demande » ; autrement dit, si je traduis bien, à la date de la demande effectuée par la CNCTR. Vous estimez par conséquent qu'il ne sert à rien de contrôler des données qui n'ont pas du tout été traitées. Je demande qu'on réfléchisse, d'ici à l'examen du texte en séance, sur la question de savoir ce qui peut se passer entre deux contrôles.

M. le rapporteur pour avis. J'ai du mal à saisir votre propos, Monsieur Lagarde. Les données qui sont conservées peuvent faire l'objet d'un contrôle. Celles qui ne sont que du « bruit » n'ont pas à faire l'objet d'un contrôle.

M. Stéphane Trompille. N'est-il pas possible d'ajouter le terme « surplus » ou celui de « bruit » ?

M. le rapporteur pour avis. Non.

La commission ***adopte*** *l'amendement.*

Puis elle émet un avis ***favorable*** *à l'adoption de l'article 8 ainsi* ***modifié.***

Article 8 ***bis*** **(art. 6** ***nonies*** **de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires) :** *Communication à la délégation parlementaire au renseignement des observations de la CNCTR sur les écoutes hertziennes*

La commission émet un avis ***favorable*** *à l'adoption de l'article 8 bis* ***sans modification.***

Article 9 (art. L. 2371-1 et L. 2371-2 [nouveaux] du code de la défense) : *Possibilité pour les forces armées de procéder à des écoutes hertziennes pour le seul exercice de leur mission de défense*

La commission examine l'amendement DN10 de M. Bastien Lachaud.

M. Bastien Lachaud. Je rappelle que les ondes wifi sont des ondes hertziennes et qu'elles ne passent donc pas par un opérateur privé entre la *box* et

un ordinateur. Dès lors, toutes les communications internet ciblées pourraient être enregistrées. Je veux bien qu'on me prouve le contraire et je serais ravi de l'entendre ; en attendant, il paraît sage de ne pas permettre d'interceptions dans ce cas précis.

M. le rapporteur pour avis. Avis défavorable à cet amendement de suppression.

Je tiendrai à votre disposition un tableau avec les différentes techniques de renseignement et les différents dispositifs concernés.

À partir du moment où il y a un opérateur, nous sommes dans le droit commun.

M. Bastien Lachaud. Mais en l'occurrence il n'y a pas d'opérateur !

M. le rapporteur pour avis. Si, car dès lors qu'il y a une *box* il y a un opérateur ! Vous constaterez en lisant le tableau que je viens d'évoquer que le wifi non connecté n'est pas concerné.

M. Bastien Lachaud. Entre la *box* et l'ordinateur, je le répète, il n'y a pas d'opérateur.

M. le rapporteur pour avis. Si, et le cas que vous mentionnez est soumis au droit commun, l'autorisation préalable du Premier ministre et l'avis obligatoire de la CNCTR étant requis. Il ne peut en être autrement.

En ce qui concerne le wifi, je mentionnerai, point technique assez obscur, le wifi non connecté qu'on utilise quand on écoute de la musique, par exemple, avec une enceinte d'une marque quelconque. À l'exception de ce dernier cas, d'une manière générale le wifi ne peut pas bénéficier de l'exception hertzienne et, en cas d'interception, si les autorisations préalables faisaient défaut, des sanctions seraient prononcées.

M. Jean-François Eliaou. Votre démonstration m'a semblé claire, Monsieur le rapporteur pour avis. Vous avez exclu tout ce qui était privé résultant d'une déconnexion entre deux appareils. Pour le wifi, il s'agit obligatoirement d'une clef de connexion entre le récepteur et l'émetteur. Il semble donc, à partir de votre démonstration, que nous retombons dans le hertzien privé qui n'est pas dans le champ de la loi.

M. le président. Et en plus, ici, il y a un opérateur.

*La commission **rejette** l'amendement.*

*Puis elle émet un avis **favorable** à l'adoption de l'article 8 bis **modifié.***

Après l'article 9

La commission examine l'amendement DN11 de M. Alexis Corbière.

M. Alexis Corbière. Le présent amendement prévoit que « l'autorisation préalable d'exportation mentionnée au I [du code de la défense] ne peut concerner un État engagé dans une intervention militaire extérieure sans mandat de l'Organisation des nations unies. » Il prévoit en outre, après l'alinéa 1 de l'article L. 2335-4 dudit code, d'insérer un deuxième alinéa ainsi rédigé : « L'autorité administrative mentionnée à l'alinéa précédent doit suspendre, modifier, abroger ou retirer les licences d'exportation qu'elle a délivrées et qui concernent un État engagé dans une intervention militaire extérieure sans mandat de l'Organisation des nations unies. »

En effet, la France participe à de nombreux conflits directement ou indirectement à travers les licences qu'elle donne et qui permettent la diffusion des armes. On ne peut donc sérieusement lutter contre le terrorisme si on laisse se propager ce type de conflit.

Nous voulons, de plus, être cohérents avec le traité sur le commerce des armes, qui vise à empêcher leur trafic là où leur utilisation risque de favoriser la perpétration de violations graves des droits humains, du droit international humanitaire – en particulier en cas de répression interne. L'article 6, alinéa 3, du traité précise qu'un État signataire « *ne doit autoriser aucun transfert d'armes classiques (…) s'il a connaissance, lors de l'autorisation, que ces armes ou ces biens pourraient servir à commettre un génocide, des crimes contre l'humanité, des violations graves des conventions de Genève de 1949, des attaques dirigées contre des civils ou des biens de caractère civil et protégés comme tels, ou d'autres crimes de guerre tels que définis par des accords internationaux auxquels il est partie.* » Je pourrais citer des conflits comme celui qui a lieu au Yémen et où de l'armement français est utilisé.

Il apparaît donc cohérent, dans un texte de loi portant sur la lutte contre le terrorisme, que, pour le dire simplement, la France n'arme pas, fût-ce de manière indirecte, ceux qui pourraient par la suite la frapper.

M. le rapporteur pour avis. Cet amendement semble constituer un cavalier législatif mais il revient sur un sujet politique dont nous continuerons de débattre en séance.

Je rappelle en attendant que la France applique strictement les dispositions de la position commune 2008/944/PESC, qui détermine les critères à l'aune desquels de telles exportations peuvent être réalisées. Or ces critères sont particulièrement rigoureux.

La France applique en outre tous les régimes de sanctions ainsi que les mesures restrictives imposées par l'ONU, l'Organisation pour la sécurité et la coopération en Europe (OSCE) et l'Union européenne. Elle participe aux

instruments internationaux relatifs au désarmement, à la maîtrise des armements et à la non-prolifération. Notre pays a d'ailleurs joué un rôle moteur pour l'adoption du traité sur le commerce des armes.

Plus concrètement, comme son nom l'indique, la commission interministérielle pour l'étude des exportations de matériels de guerre (CIEEMG) est un organe interministériel. Participent à ses travaux, notamment, des représentants du ministère des Affaires étrangères.

Au total, notre régime de contrôle est l'un des plus complets, des plus robustes, et des plus rigoureux.

Une remarque enfin : nous sommes tous, je le crois, attachés à l'existence d'un système de règlement pacifique des conflits, en particulier *via* l'ONU ; mais nous sommes tous également conscients des limites du système onusien, comme nous avons encore pu le constater à plusieurs reprises ces derniers mois.

Il peut arriver qu'une intervention militaire soit nécessaire et doive être conduite de manière urgente, par exemple pour protéger des populations civiles et empêcher la commission de massacres. Or, pour des raisons politiques, un ou plusieurs membres permanents du Conseil de sécurité pourraient bloquer toute résolution visant à délivrer un mandat, pourtant nécessaire, de l'ONU. Je rappelle le précédent du Kosovo : les opérations ont été menées pour faire face à ce qui s'annonçait comme une catastrophe humanitaire et elles l'ont été dans le cadre de l'Organisation du traité de l'Atlantique nord (OTAN), la Russie et la Chine menaçant d'opposer leur veto à une résolution de l'ONU.

Devrions-nous nous lier les mains face au risque, avéré, d'instrumentalisation du fonctionnement de l'ONU ? Je ne le crois pas. C'est pourquoi j'émets un avis défavorable.

La commission ***rejette*** *l'amendement.*

M. le président. Je précise que j'avais volontairement appelé l'amendement DN12 avant le DN11 car les amendements sont examinés, en commission comme dans l'hémicycle, en allant du plus général à celui qui l'est le moins.

La commission en vient à l'amendement DN12 de M. Bastien Lachaud.

M. Bastien Lachaud. J'avoue avoir un peu de mal avec les arguments que le rapporteur pour avis a développés pour s'opposer à l'amendement DN11. Nous débattrons en séance publique de sa conception du rôle de l'ONU.

L'amendement DN12 vise à accroître le rôle du Parlement lors de la délivrance d'autorisations préalables d'exportations d'armes, ainsi qu'en matière de décisions de suspension, modification, abrogation ou retrait de ces

autorisations, autant de sujets qui restent aujourd'hui du ressort exclusif de l'exécutif.

La commission permanente de chaque assemblée en charge des affaires de défense pourrait émettre un avis sur ces décisions. Il serait pris de manière transparente et ouverte, et la collégialité du Parlement permettrait de limiter les conflits d'intérêts. Un contrôle parlementaire doit pouvoir exister avant la vente d'armes à des États étrangers. C'est une disposition de bon sens.

M. le rapporteur pour avis. Avis défavorable. Monsieur le député, selon l'exposé sommaire de votre amendement, « le rôle accru du Parlement dans un domaine aussi fondamental pour la République que l'exportation d'armes à des États tiers découle nécessairement de l'article 34 de la Constitution car il dispose, en particulier, que la loi fixe les règles concernant l'organisation générale de la Défense nationale ».

Je ne suis certain ni de la pertinence de cette analyse ni de celle de votre interprétation de l'article 34 de la Constitution sur le rôle du Parlement en matière de défense. Une exportation d'armement est avant tout un acte politique et diplomatique au service des partenariats stratégiques que notre pays noue avec des puissances étrangères. Par nature, il s'agit bien d'un domaine relevant de l'exécutif.

Au-delà de cette question de principe, sur le fond, votre amendement ne pourrait être mis en œuvre compte tenu du nombre de demandes adressées à la CIEEMG. Les commissions parlementaires ne pourraient matériellement pas traiter l'ensemble des dossiers. Elles ne disposeraient pas des ressources matérielles et techniques suffisantes pour mener à bien ce travail. En 2016, 11 218 licences d'exportation et autres autorisations ont été délivrées, ce qui représente en moyenne 935 autorisations par mois, soit plus de 30 par jour, et autant d'avis éventuels à rendre pour les commissions parlementaires !

Vous abordez toutefois un sujet important. Lors de la précédente législature, notre commission avait d'ailleurs consacré un rapport d'information au dispositif de soutien aux exportations d'armement. Nous pouvons débattre de cette question, mais, d'une part, le dispositif proposé ne me paraît ni adapté ni opérant, d'autre part, ce projet de loi ne me semble pas constituer le véhicule idoine pour les mesures que vous proposez. De la même manière, les amendements DN13 et DN14 qui prévoient le dépôt de rapports d'information par le gouvernement me semblent être des cavaliers législatifs.

M. Jean-Christophe Lagarde. Cet amendement pose une question relative à la nature même de V^{e} République, marquée, depuis ses débuts, par une quasi-absence de culture parlementaire.

Je fais d'abord remarquer à notre rapporteur pour avis que, dès lors que 900 autorisations sont délivrées tous les mois, elles ne peuvent pas faire l'objet d'un réel contrôle politique par le ministre compétent : l'administration est donc

seule aux manettes. Je lui signale ensuite qu'en matière de ventes d'armes à l'étranger, le contrôle parlementaire existe aux États-Unis, pays qui exporte sans doute davantage d'armes que la France. Non seulement nous avons un manque de culture parlementaire, mais nous n'avons jamais appris à faire travailler un petit nombre d'élus astreints au secret. Un commissaire de chaque groupe politique pourrait participer à un tel groupe. Il paraît que nous sommes dans un nouveau monde : nous pouvons espérer que des changements adviennent.

Dans les faits, le commerce des armes vient en complément d'accords de défense dont les parlementaires n'ont pas à connaître. En revanche un contrôle parlementaire devrait s'exercer en opportunité. Dans une démocratie, le Parlement doit être associé aux décisions. Évidemment, il ne s'agit pas que tous les parlementaires soient impliqués : seule une délégation de parlementaires serait concernée. Au plus fort de la Guerre froide, les parlementaires américains disposaient d'une capacité totale de contrôle sur l'activité de l'administration en matière de vente d'armes, y compris lorsqu'il s'agissait des services de renseignements. Un président des États-Unis est obligé de s'interroger avant de prendre une décision en la matière, et de la partager avec sa représentation parlementaire.

Dans la nécessité de résilience qui s'impose à nous pour les dix ou vingt prochaines années, et dans le combat qui nous est imposé, j'estime que mieux intégrer le Parlement sans pour autant paralyser l'exécutif permettra de renforcer ce dernier et de nous donner des armes contre ceux qui veulent abattre notre système. Nous devrions nous poser cette question, même si nous ne le faisons pas aujourd'hui – car notre rapporteur pour avis a raison, ce n'est pas l'objet du projet de loi que nous examinons.

Disons clairement que tout cela dépend aussi du seul président de la République. Si ce dernier ferme la porte et campe sur ses pouvoirs propres et ceux de l'exécutif, nous n'y pourrons rien. Cependant, puisqu'une majorité a été élue à l'Assemblée nationale qui affirme vouloir changer un certain nombre de pratiques anciennes, en voilà une qui mériterait d'évoluer vers ce que font un certain nombre de grandes démocraties. D'autres approches existent, aussi bien dans un régime présidentiel, comme celui des États-Unis, que dans un régime parlementaire, comme au Royaume-Uni.

M. Bastien Lachaud. Je ne reviens pas sur l'impossibilité technique évoquée par le rapporteur pour avis : M. Jean-Christophe Lagarde a parfaitement répondu à cet argument.

Le rapporteur pour avis considère également que ce projet de loi ne constitue pas le bon véhicule pour la disposition que nous proposons. Nous examinons pourtant un projet de loi « renforçant la sécurité intérieure et la lutte contre le terrorisme ». J'ose espérer que votre ambition ne se limite pas à empêcher la commission d'actes terroristes en France, mais qu'elle concerne aussi ceux qui pourraient advenir dans autres pays ! Nous savons bien qu'à l'étranger,

en particulier en Afrique et au Moyen-Orient, des actes terroristes sont commis au moyen d'armes potentiellement exportées par la France. Je ne vois en conséquence pas en quoi la question du contrôle parlementaire du commerce des armes ne serait pas directement liée à la lutte contre les actes terroristes, en particulier ceux qui ont lieu à l'étranger.

M. le président. Mon cher collègue, il ne s'agissait que d'une petite pique de la part de notre rapporteur pour avis.

La commission ***rejette*** *l'amendement.*

La commission est saisie de l'amendement DN14 de M. Bastien Lachaud.

M. Bastien Lachaud. Je l'ai dit précédemment, nous devons avoir la volonté de lutter efficacement contre les actes terroristes en France, mais aussi à l'échelle internationale. Dans cet objectif, nous proposons que le Gouvernement remette au Parlement, dans un délai de trois mois à compter de la promulgation de la présente loi, un rapport d'information faisant un état des lieux très précis de l'utilisation des armes qui ont été exportées de France durant les dix dernières années, afin de déterminer si certaines de ces armes ont été détournées de leur utilisation première pour être éventuellement utilisées dans le cadre de crimes contre l'humanité, de crimes de guerre, ou d'attaques dirigées contre des populations civiles.

En effet, si nous ne remettons pas en question le fait que la France puisse être une grande puissance exportatrice d'armes dont la grande qualité est reconnue, nous estimons que cette spécificité implique un contrôle rigoureux exercé par le Parlement et, à travers lui, par nos concitoyens, sur l'utilisation qui est faite des armes vendues par la France. Tel est l'objet de notre amendement DN14.

M. le rapporteur pour avis. J'ai indiqué les règles, légitimement contraignantes, qui encadrent nos exportations d'armement et, sans y revenir, je veux rappeler un exemple précis qui démontre la rigueur de nos procédures en la matière : en 2014, notre pays a refusé d'exporter les bâtiments de projection et de commandement (BPC) à la Russie, du fait de la politique de déstabilisation menée par ce pays.

Par ailleurs, compte tenu de la structure de l'offre française, les matériels exportés par la France ne sont pas les plus susceptibles de faire l'objet d'un détournement, mais plutôt des matériels « rustiques » – je pense par exemple aux armes automatiques et à leurs munitions, non produites en France.

Quand on suggère la remise d'un rapport, il convient de s'interroger sur le caractère effectivement réalisable de cette démarche, notamment en termes de délais. En l'occurrence, le champ du rapport que vous demandez est tellement vaste – il couvrirait les exportations effectuées au cours des dix dernières années –

qu'aucune administration ne serait en mesure de mener ce travail dans un délai de trois mois !

Enfin, il existe déjà un rapport annuel sur les exportations, transmis chaque année au Parlement par le ministère de la défense – la remise de ce document donnant lieu à un débat devant notre Commission et à l'audition du ministre de la défense.

Je suis donc défavorable à l'amendement DN14 – comme je le serai, pour les mêmes raisons, à l'amendement DN13.

M. Bastien Lachaud. Il est un peu inquiétant de s'entendre dire que l'administration est incapable de nous indiquer ce que sont devenues les armes vendues par la France au cours des dix dernières années. Cela tend à démontrer que, lorsqu'on accorde une licence à un pays pour l'utilisation des armes qu'on lui vend, on ne vérifie même pas l'usage qu'il a fait des armes achetées précédemment – car si cette vérification était faite, on en retrouverait facilement les traces dans nos archives.

Les arguments que vous avez exposés ne nous ayant pas convaincus, nous maintenons notre demande de rapport, Monsieur le rapporteur.

Mme Natalia Pouzyreff. S'il est vrai que la lutte contre le terrorisme ne doit pas se limiter au territoire national, force est de constater que les terroristes emploient le plus souvent des produits bas de gamme, à vocation civile, pour effectuer leurs attaques, et non les matériels de guerre relevant de la haute technologie qui font l'objet de cet amendement.

*La commission **rejette** l'amendement.*

Elle examine l'amendement DN13 de M. Alexis Corbière.

M. Alexis Corbière. Lutter efficacement contre les actes terroristes en France et à l'échelle internationale implique que nous portions une attention particulière aux régions du monde qui en sont le foyer, et que nous nous interrogions sur leur situation ainsi que sur le rôle que nous y jouons.

Nous proposons donc que le Gouvernement remette au Parlement un rapport d'information sur l'utilisation des armes exportées par la France vers l'Arabie saoudite et dont l'État français a autorisé l'exportation au titre de l'article L. 2335-3 du code de la défense, afin d'évaluer précisément si ces armes ont été détournées de leur utilisation première prévue par l'autorisation préalable d'exportation pour être utilisées dans des opérations ayant mené ou ayant pu mener à des crimes pouvant être qualifiés de crimes contre l'humanité, de crimes de guerre, et à des attaques dirigées contre des populations civiles ; l'examen de ce rapport permettra également de vérifier si la France a méconnu ou non ses obligations relatives au Traité sur le commerce des armes, entré en vigueur le 24 décembre 2014.

En mars 2017, un panel d'experts de l'ONU, mais aussi de nombreux acteurs de la société civile et certains États, ont dénoncé l'utilisation faite par l'Arabie saoudite d'armes qui lui avaient été fournies par la France, pour conduire des bombardements aériens contre des cibles civiles au Yémen – notamment des écoles, des fêtes de mariage, des hôpitaux et des marchés –, et ainsi potentiellement commettre des crimes contre l'humanité, des crimes de guerre ainsi que des attaques dirigées contre des civils.

Selon un rapport de *Control Arms* paru en février 2016, la France a autorisé 16 milliards d'euros de ventes d'armes à l'Arabie saoudite en 2015, loin devant les États-Unis, dont l'autorisation était limitée à 5,2 milliards d'euros, et le Royaume-Uni – 3,5 milliards d'euros.

Par cette demande de rapport, nous souhaitons que le Parlement puisse disposer d'une information clarifiée quant à la réalité de ces graves accusations concernant un État avec qui la France a, sous les précédents gouvernements, noué des liens diplomatiques, militaires, économiques et commerciaux particulièrement étroits, que l'actuel gouvernement semble vouloir pérenniser.

M. le rapporteur pour avis. Pour les mêmes raisons que celles exposées précédemment, j'émets un avis défavorable à l'amendement DN13. Plus largement, il me semble que, sur les sujets complexes qui sont ici évoqués, il pourrait être utile d'organiser une audition des responsables de la CIEEMG.

*La commission **rejette** l'amendement.*

M. le président. Mes chers collègues, nous avons terminé l'examen des amendements portant sur les articles dont notre commission s'était saisie.

ANNEXE

LISTE DES PERSONNES AUDITIONNÉES PAR LE RAPPORTEUR POUR AVIS

(Par ordre chronologique)

➢ **M. Francis Delon,** président de la commission nationale de contrôle des techniques de renseignement et **M. Marc Antoine**, conseiller auprès du président.

➢ **Mme Camille Faure**, adjointe à la directrice des affaires juridiques du ministère des Armées, **M. Mathieu Rhée**, chef du bureau des données personnelles – direction des affaires juridiques, **M. le lieutenant-colonel Christophe Junqua**, cabinet militaire de la ministre des Armées, **Mme Animya N'Tchandy**, conseillère parlementaire au cabinet de la ministre, ainsi que des **représentants de la direction générale de la sécurité extérieure et de la direction du renseignement militaire**.

➢ **M. Vincent Bouvier**, Secrétaire général de la Mer et **M. le colonel Pascal Cheylan**, chargé de mission sûreté.

➢ **M. Olivier Bardin**, directeur de l'Unité Information Passagers chargée du traitement automatisé de données à caractère personnel « API-PNR France ».