

N° 401

SÉNAT

SESSION ORDINAIRE DE 2008-2009

Annexe au procès-verbal de la séance du 13 mai 2009

RAPPORT

FAIT

*au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) sur la proposition de résolution européenne présentée par M. Simon SUTOUR, au nom de la commission des Affaires européennes (2), en application de l'article 73 bis du Règlement, sur la proposition de décision-cadre relative à l'**utilisation de données des dossiers passagers (Passenger Name Record – PNR) à des fins répressives (E 3697),***

Par M. Yves DÉTRAIGNE,

Sénateur

(1) *Cette commission est composée de :* M. Jean-Jacques Hyst, *président* ; M. Nicolas Alfonsi, Mme Nicole Borvo Cohen-Seat, MM. Patrice Gélard, Jean-René Lecerf, Jean-Claude Peyronnet, Jean-Pierre Sueur, Mme Catherine Troendle, M. François Zocchetto, *vice-présidents* ; MM. Laurent Béteille, Christian Cointat, Charles Gautier, Jacques Mahéas, *secrétaires* ; M. Alain Anziani, Mmes Éliane Assassi, Nicole Bonnefoy, Alima Boumediene-Thiery, MM. Elie Brun, François-Noël Buffet, Pierre-Yves Collombat, Jean-Patrick Courtois, Mme Marie-Hélène Des Esgaulx, M. Yves Détraigne, Mme Anne-Marie Escoffier, MM. Pierre Fauchon, Louis-Constant Fleming, Gaston Flosse, Christophe-André Frassa, Bernard Frimat, René Garrec, Jean-Claude Gaudin, Mmes Jacqueline Gourault, Virginie Klès, MM. Antoine Lefèvre, Dominique de Legge, Mme Josiane Mathon-Poinat, MM. Jacques Mézard, Jean-Pierre Michel, François Pillet, Hugues Portelli, Roland Povinelli, Bernard Saugey, Simon Sutour, Richard Tuheiaiva, Alex Türk, Jean-Pierre Vial, Jean-Paul Virapoullé, Richard Yung.

(2) *Cette commission est composée de :* M. Hubert Haenel, *président* ; MM. Denis Badré, Michel Billout, Jean Bizet, Jacques Blanc, Jean François-Poncet, Aymeri de Montesquiou, Roland Ries, Simon Sutour, *vice-présidents* ; Mmes Bernadette Bourzai, Marie-Thérèse Hermange, *secrétaires* ; MM. Robert Badinter, Jean-Michel Baylet, Pierre Bernard-Reymond, Didier Boulaud, Mme Alima Boumediene-Thiery, MM. Gérard César, Christian Cointat, Pierre-Yves Collombat, Philippe Darniche, Mme Annie David, MM. Robert del Picchia, Pierre Fauchon, Bernard Frimat, Yann Gaillard, Mme Fabienne Keller, MM. Serge Lagache, Jean-René Lecerf, Mmes Colette Mélot, Monique Papon, MM. Jean-Claude Peyronnet, Hugues Portelli, Yves Pozzo di Borgo, Josselin de Rohan, Mme Catherine Tasca et M. Richard Yung.

Voir le(s) numéro(s) :

Sénat : 252 et 402 (2008-2009)

SOMMAIRE

	<u>Pages</u>
LES CONCLUSIONS DE LA COMMISSION DES LOIS	5
EXPOSÉ GÉNÉRAL	7
I. LA PROPOSITION DE DÉCISION-CADRE : DES NÉGOCIATIONS LOIN D'ÊTRE ACHEVÉES	8
A. LE CONTEXTE : UN DÉVELOPPEMENT ANARCHIQUE DE SYSTÈMES DE DONNÉES PNR À DES FINS RÉPRESSIVES	8
1. <i>Les données PNR : définition</i>	8
2. <i>Les expériences en dehors de l'Union européenne</i>	10
3. <i>Les expériences européennes</i>	11
4. <i>Le système PNR français</i>	12
B. LA PROPOSITION DE DÉCISION-CADRE : VERS UN PNR EUROPÉEN	14
C. UN TEXTE APPELÉ À ÉVOLUER	17
1. <i>Des avis extérieurs critiques</i>	17
2. <i>Les travaux de la présidence française de l'Union européenne</i>	18
3. <i>Un texte en panne ?</i>	20
II. LA PROPOSITION DE RÉOLUTION ET LA POSITION DE VOTRE COMMISSION	21
A. DEUX QUESTIONS FONDAMENTALES À TRANCHER : LES DONNÉES PNR SONT-ELLES RÉELLEMENT UTILES ET FAUT-IL UN « PNR EUROPÉEN » ?	21
1. <i>Des données utiles...</i>	21
2. <i>...à mettre en regard avec les risques pour le respect des droits fondamentaux</i>	23
3. <i>L'intérêt d'une harmonisation européenne</i>	24
B. LA DÉFINITION DU CHAMP DU PNR EUROPÉEN.....	24
1. <i>Des finalités à préciser</i>	24
2. <i>Quelles données collecter ?</i>	25
3. <i>L'exclusion des vols intracommunautaires</i>	26
C. LE FONCTIONNEMENT DU PNR EUROPÉEN	27
1. <i>Réduire la durée de conservation des données</i>	27
2. <i>Adopter la méthode « PUSH »</i>	27
3. <i>Préciser les destinataires des données</i>	28
4. <i>Renforcer le droit des personnes concernées</i>	28
5. <i>Limiter la transmission des données à des Etats tiers</i>	29
D. UNE TRANSPOSITION PAR LA LOI	30
PROPOSITION DE RÉOLUTION	31
EXAMEN EN COMMISSION MERCREDI 13 MAI 2009	33

ANNEXES	39
ANNEXE 1 LISTE DES PERSONNES ENTENDUES	41
ANNEXE 2 LISTE DES DONNÉES PNR QUI DEVRAIENT ÊTRE TRANSMISES EN APPLICATION DE LA PROPOSITION DE DÉCISION-CADRE	43
ANNEXE 3 ARTICLE 2 DE LA DÉCISION-CADRE DU 13 JUIN 2002 RELATIVE AU MANDAT D'ARRÊT EUROPÉEN (2002/584/JAI)	45
TABLEAU COMPARATIF	47

LES CONCLUSIONS DE LA COMMISSION DES LOIS

Réunie le mercredi 13 mai 2009, sous la présidence de M. Jean-Jacques Hyest, président, la commission des lois a examiné, sur le rapport de M. Yves Détraigne, **la proposition de résolution n° 252 (2008-2009) présentée par M. Simon Sutour au nom de la commission des affaires européennes sur la proposition de décision-cadre relative à l'utilisation des données des dossiers passagers (Passenger Name Record-PNR) à des fins répressives (E 3697).**

Après avoir présenté le contexte dans lequel des systèmes de collecte des données PNR à des fins répressives tendent à se développer à travers le monde ainsi que la proposition de décision-cadre, M. Yves Détraigne, rapporteur, a approuvé l'essentiel de la proposition de la résolution. Il a expliqué que celle-ci ne rejetait pas le principe d'un système PNR européen, mais qu'elle émettait des critiques fortes, le droit au respect de la vie privée et à la protection des données à caractère personnel n'étant pas garanti en l'état du texte.

Il a proposé d'aller encore plus loin sur plusieurs points en formulant des recommandations très précises.

La commission a décidé, sur son initiative et à l'unanimité :

- de préciser qu'au sein des services de sécurité autorisés à utiliser les données PNR, seuls des agents individuellement désignés et dûment habilités devraient pouvoir y accéder ;

- d'exclure de la liste des données PNR transmises la rubrique « 12) *Remarques générales* », qui est la seule où des données sensibles peuvent figurer ;

- de prévoir une durée de conservation de trois ans, à laquelle pourrait succéder une durée de conservation de trois ans des seules données PNR ayant montré un intérêt particulier au cours de la première période ;

- d'exiger que la transposition de la proposition de décision-cadre soit réalisée par la loi compte tenu des enjeux pour assurer un respect effectif des droits fondamentaux.

La commission a adopté la proposition de résolution ainsi rédigée.

Mesdames, Messieurs,

Le Sénat a été saisi, le 21 novembre 2007, au titre de l'article 88-4 de la Constitution, d'une proposition de décision-cadre relative à l'utilisation des données des dossiers passagers (Passenger Name Record-PNR) à des fins répressives¹. Ces données dites PNR sont recueillies par les compagnies aériennes et les agences de voyage auprès des passagers à l'occasion de la réservation du vol.

Cette proposition fait suite au Conseil européen des 25 et 26 mars 2004 qui avait invité la Commission européenne à soumettre une proposition « *en vue d'une approche commune de l'Union européenne dans l'utilisation des données passagers à des fins répressives* ». Cette invitation a d'ailleurs été réitérée dans le programme de La Haye en novembre 2004 qui fixe les objectifs pour la période 2004-2009 en matière de justice et d'affaires intérieures.

Présentée en novembre 2007, la proposition de décision-cadre a pour objectif « *d'harmoniser les dispositions des Etats membres relatives à l'obligation, pour les transporteurs aériens assurant des vols vers le territoire d'au moins un Etat membre ou à partir de celui-ci, de transmettre aux autorités compétentes les renseignements relatifs aux passagers aux fins de prévenir et de combattre les infractions terroristes et la criminalité organisée* ».

Cette proposition s'inscrit dans un contexte international de développement des systèmes de recueil des données PNR à des fins répressives depuis les attentats du 11 septembre 2001.

Elle est particulièrement symbolique puisqu'elle intervient après des négociations très difficiles entre les Etats-Unis et l'Union européenne sur les conditions du transfert aux Etats-Unis des données PNR recueillies par les compagnies assurant des vols entre ces deux territoires.

¹ Document COM (2007) 654 final.

Le Sénat, notamment par la voie de sa délégation pour l'Union européenne, avait émis de très fortes réserves sur ces accords. C'est donc en toute logique qu'il se doit d'exercer une même vigilance sur la présente proposition de décision-cadre.

Réunie le 3 mars 2009, la commission des affaires européennes a adopté une proposition de résolution présentée par notre collègue Simon Sutour dont votre commission des lois est désormais saisie.

Cette proposition de résolution européenne ne rejette pas le principe d'un système PNR européen. Elle exprime néanmoins des critiques fortes à l'encontre de la proposition de décision-cadre, le droit au respect de la vie privée et à la protection des données à caractère personnel n'étant pas garanti en l'état du texte.

I. LA PROPOSITION DE DÉCISION-CADRE : DES NÉGOCIATIONS LOIN D'ÊTRE ACHEVÉES

A. LE CONTEXTE : UN DÉVELOPPEMENT ANARCHIQUE DE SYSTÈMES DE DONNÉES PNR À DES FINS RÉPRESSIVES

1. Les données PNR : définition

Les compagnies aériennes et les agences de voyage collectent ces informations auprès des passagers dans le cadre des services de réservation. Stockées dans les bases de données des systèmes de réservation, elles sont échangées entre les entreprises intervenantes du moment de la réservation jusqu'à la réalisation des prestations demandées par les passagers. Les données présentes dans ces bases prennent la forme d'enregistrements d'informations standardisés au plan international dénommés « PNR » (Passenger Name Record).

Le PNR **peut** ainsi contenir, en fonction des prestations offertes par les compagnies et demandées par le client, des informations telles que :

- les nom et prénom du client ;
- les renseignements sur l'agence de voyage auprès de laquelle la réservation est effectuée ;
- l'itinéraire du déplacement qui peut comporter plusieurs étapes ;
- les indications des vols concernés (numéro des vols successifs, date, heures, classe économique, business...)
- le groupe de personnes pour lesquelles une même réservation est faite ;
- le contact à terre du passager (numéro de téléphone au domicile, professionnel...)

- les tarifs accordés, l'état du paiement effectué et ses modalités par carte bancaire ;
- les réservations d'hôtels ou de voitures à l'arrivée ;
- les services demandés à bord tels que le numéro de place affecté à l'avance, les repas et les services liés à la santé...

Le plus souvent, tous les champs ne sont pas remplis.

Votre rapporteur attire l'attention sur le fait que **ces données ne doivent pas être confondues avec les données dites « APIS »** (Advance Passenger Information System). Ces données sont celles collectées par les compagnies lors de la phase d'enregistrement des passagers sur un vol. Elles comportent le numéro et le type du document de voyage utilisé, la nationalité, le nom complet, la date de naissance, le point de passage frontalier utilisé pour entrer sur le territoire des États membres, le code de transport, les heures de départ et d'arrivée du transport, le nombre total des personnes transportées et le point d'embarquement initial.

Les données APIS sont moins nombreuses que les données PNR. Elles sont en revanche beaucoup plus fiables puisqu'elles sont vérifiées par le personnel des transporteurs au moment de l'enregistrement du vol. Les données PNR sont fournies par les voyageurs au stade de la réservation commerciale, laquelle peut d'ailleurs changer jusqu'à l'embarquement. Toutefois, des erreurs peuvent encore survenir lors de la transcription des noms des voyageurs par le personnel, car la lecture des documents de voyage n'est pas toujours automatisée.

Avant le 11 septembre 2001, les données PNR conservées à des fins commerciales par les opérateurs pouvaient être requises, comme toutes autres données, par l'autorité judiciaire pour les besoins d'une enquête ou d'une instruction.

Toutefois, aucun Etat n'avait mis en place de dispositifs spécifiques pour contraindre les transporteurs et les agences de voyage à transmettre ces données aux autorités compétentes à des fins de prévention et de répression d'infractions.

Les attentats du 11 septembre 2001 ont conduit les autorités américaines à accorder une attention particulière à ces données, compte tenu de l'enjeu pour la sécurité aérienne, de la vulnérabilité des terroristes lors du franchissement des frontières et de la richesse des informations susceptibles d'être contenues dans les dossiers passagers. Par un effet de contagion, d'autres Etats se sont organisés pour exploiter plus systématiquement ces données.

2. Les expériences en dehors de l'Union européenne

Trois pays se sont dotés d'un système de données PNR : les Etats-Unis, le Canada et l'Australie. La Corée du Sud a un projet en cours.

Ces trois systèmes, tous différents, ont donné lieu à la conclusion d'accords avec l'Union européenne pour régler les modalités de la transmission et de l'exploitation des données PNR issues de vols en provenance d'un Etat membre et à destination de l'un de ces trois pays.

Le système américain est le plus ancien et le plus abouti. Dans le cadre de la lutte contre le terrorisme et les actes criminels, les Etats-Unis ont adopté, le 19 novembre 2001, une législation sur la sécurité de l'aviation et du transport (the Aviation and Transportation Security Act) et le 5 mai 2002, une loi renforçant les conditions d'entrée sur le territoire américain (Enhanced Border Security and Visa Entry Reform Act). Ces mesures prévoyaient qu'à compter du 5 mars 2003, les compagnies aériennes devaient communiquer aux services des douanes et de sécurité américains des informations personnelles relatives à leurs passagers, sous peine de contrôles renforcés, d'amendes ou même de suspension du droit d'atterrir.

Toutefois, ces exigences américaines heurtant les règles européennes en matière de protection des données personnelles, la conclusion d'un accord entre l'Union européenne et les Etats-Unis était nécessaire afin que les compagnies aériennes ne soient pas placées en porte-à-faux entre les législations américaines et européennes. Sans revenir sur les péripéties ayant finalement abouti à la conclusion d'un accord le 19 octobre 2006 et entré en vigueur le 1^{er} août 2007, il faut retenir que :

- cet accord¹ a été conclu dans le cadre **du troisième pilier**² ;

- le ministère de l'intérieur américain (*Department of Homeland Security-DHS*) peut transférer les données PNR à d'autres autorités gouvernementales et qu'il a accès, dans des circonstances exceptionnelles, aux données sensibles, c'est-à-dire celle pouvant révéler l'origine raciale ou ethnique, les convictions religieuses, les opinions politiques ou un problème de santé ;

- les finalités du système sont très larges et évolutives ;

¹ La Cour de justice des communautés européennes a annulé le 30 mai 2006 le premier accord conclu le 28 mai 2004. Elle a jugé que la base juridique de cet accord était inappropriée puisque pris dans le cadre du premier pilier. Le traitement lié au transfert des données PNR aux autorités américaines ayant pour objet la sécurité publique, un nouvel accord devait être conclu dans le cadre du troisième pilier.

² Les champs de compétence de l'Union européenne sont répartis entre trois « piliers ». Le premier pilier regroupe schématiquement toutes les matières relatives au marché intérieur et à la libre circulation. Le deuxième pilier les questions de défense et de politique étrangère. Le troisième pilier, les questions de police et de justice.

Les règles d'adoption des textes européens diffèrent selon les piliers. Le premier pilier implique la majorité qualifiée, la codécision avec le Parlement européen et le contrôle de la Cour de justice. Le troisième pilier implique en revanche l'unanimité, l'avis simple du Parlement européen et l'absence de contrôle de la Cour de justice.

- les données sont conservées sept ans, puis huit ans supplémentaires en cas de besoin, soit un total de quinze années, sans que des garanties aient été apportées sur leur destruction passé ce délai.

Les accords avec l’Australie et le Canada sont en revanche plus équilibrés.

A propos de l’accord avec le Canada¹, plusieurs points sont notables :

- les finalités poursuivies sont exclusivement la lutte contre le terrorisme ;

- 25 rubriques de données PNR sont transmises aux autorités canadiennes contre 34 dans les accords avec les Etats-Unis ;

- les citoyens européens bénéficient du droit d’accès et de rectification de leurs données dans les mêmes conditions que les résidents canadiens ;

- la durée de conservation maximale est de trois ans et demi.

L’accord avec l’Australie est assez proche de l’accord canadien, même si les finalités du système sont aussi larges que celles de l’accord avec les Etats-Unis. Les données sensibles ne sont pas conservées.

3. Les expériences européennes

Comme le relève l’exposé des motifs de la proposition de résolution, au sein de l’Union européenne, le Royaume-Uni est le seul Etat membre à avoir un système PNR complet dans le cadre du programme e-borders.

Entré en vigueur en mars 2008, il couvre à la fois la collecte des données APIS et les données PNR. S’agissant de ces dernières, le Royaume-Uni procède à une collecte sélective concentrée sur certains itinéraires et destinations jugés plus risqués.

Les finalités sont très larges : terrorisme, grande criminalité, lutte contre l’immigration illégale et contrôles douaniers.

Le système ne fait pas de distinction a priori entre les vols en provenance d’un Etat membre de l’Union européenne ou d’un Etat tiers. Et il ne se limite pas au seul transport aérien.

La durée de conservation des données est de dix ans.

Le Danemark s’est également doté d’un cadre légal permettant la collecte des données PNR, mais uniquement à des fins de lutte antiterroriste. Toutefois, ces dispositions n’auraient pas encore été mises en œuvre.

En Belgique, les services de police peuvent dans le cadre d’une autorisation judiciaire demander aux compagnies aériennes un accès à leurs données PNR. Elles les utilisent notamment à des fins de profilage.

¹ Accord signé le 3 octobre 2005 et publié au Journal officiel de l’Union européenne le 21 mars 2006.

4. Le système PNR français

L'article 7 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme autorise la collecte et l'exploitation des données PNR et APIS.

Le ministre de l'intérieur est ainsi autorisé à créer des traitements automatisés des données à caractère personnel recueillies à l'occasion de déplacements internationaux en provenance ou à destination d'Etats n'appartenant pas à l'Union européenne. Les vols intracommunautaires sont exclus.

Trois catégories de données sont notamment concernées.

- les données directement collectées à partir de la **bande de lecture** optique (dite « MRZ ») des documents de voyage, de la carte nationale d'identité et des visas des passagers de transporteurs aériens, maritimes ou ferroviaires. Cette technique rend possible l'enregistrement systématique et rapide des données contenues dans la bande optique, même lorsque les agents aux frontières sont confrontés à l'arrivée simultanée et massive de plusieurs vols ;

Données enregistrées dans la bande MRZ

Le passeport	La carte nationale d'identité	Le visa
1. type de document	1. type de document	1. type de document
2. nom	2. nom	2. nom
3. prénoms	3. prénoms	3. prénoms
4. le numéro de passeport	4. le numéro de la CNI	4. numéro du visa
5. nationalité	5. nationalité	5. nationalité
6. date de naissance	6. date de naissance	6. date de naissance
7. sexe	7. sexe	7. sexe
8. date d'expiration du passeport		8. date de fin de validité du visa
		9. validité territoriale
		10. État émetteur
		11. nombre d'entrées
		12. durée du séjour
		13. début de validité

- les données « APIS » ;
- les données « PNR ».

La loi écarte expressément l'utilisation des données dites sensibles au sens de l'article 8 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Il s'agit de celles « *qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci* ». Les données concernant les types de repas à bord ou l'état de santé du voyageur ne peuvent pas faire l'objet d'une transmission.

Les finalités sont définies précisément :

- améliorer le contrôle aux frontières et la lutte contre l'immigration clandestine ;
- prévenir et réprimer les actes de terrorisme.

La loi précise également que les personnes ayant accès aux données collectées varient selon la finalité poursuivie. Ainsi, s'agissant de la prévention et de la répression du terrorisme, seuls les agents individuellement désignés et dûment habilités des services spécialisés peuvent accéder à ces traitements de données.

Ces traitements peuvent faire l'objet d'une interconnexion avec le fichier des personnes recherchées (FPR) et le système d'information Schengen (SIS).

La loi du 23 janvier 2006 est ainsi allée au-delà de la simple transposition de **la directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données APIS.**

Adoptée dans le cadre de **la lutte contre l'immigration clandestine et de l'amélioration des contrôles aux frontières (premier pilier)**, cette directive dispose que les États membres prennent les mesures nécessaires afin d'établir l'obligation, pour les transporteurs aériens, de transmettre, à la demande des autorités chargées du contrôle des personnes aux frontières extérieures, avant la fin de l'enregistrement, les données APIS des voyageurs entrant sur le territoire d'un État membre.

La loi ne précisait pas l'architecture technique du système, ni le nombre de traitements qui seraient mis en place.

La mise en œuvre de l'article 7 de la loi du 23 janvier 2006 s'est traduite par la création à titre expérimental du **Fichier des passagers aériens (FPA)** par un arrêté du 19 décembre 2006.

Le champ de cette expérimentation est très limité par rapport à ce que la loi autorise.

Elle ne concerne que les données APIS des passagers des vols directs en provenance et à destination de cinq pays (l'Afghanistan, le Pakistan, l'Iran, la Syrie et le Yémen). Au total, au cours des deux années de l'expérimentation, les données de 209.451 passagers ont été transmises.

Les données transmises sont conservées pendant cinq ans et peuvent être consultés par les services spécialisés à titre de source de renseignements. Toutefois, dans le cadre de la lutte contre l'immigration clandestine, ces données ne peuvent être consultées par les agents habilités que dans les 24 heures suivant leur transmission.

M. Jean-Yves Topin, directeur central de la police aux frontières, a indiqué que l'expérimentation avait été prolongée et qu'elle devrait être étendue à d'autres pays.

Deux dysfonctionnements sont apparus.

Tout d'abord, un manque de rigueur dans la transmission des données par certaines compagnies a été constaté. La mise en œuvre des sanctions prévues par la loi en cas de méconnaissance par les transporteurs de leurs obligations -50.000 euros pour chaque vol pour lequel les données n'ont pas été transmises- fait encore défaut.

Ensuite, de nombreuses erreurs sont imputables à des homonymies ou à des transcriptions inexactes des noms. Seule l'automatisation de la lecture des documents de voyage dans ces pays pourrait supprimer cette source d'erreur.

La France n'a donc pas mis en œuvre un traitement des données PNR à des fins répressives et de renseignements alors que la loi du 23 janvier 2006 l'y autorise.

Toutefois, la France n'est pas totalement dépourvue d'expérience.

En effet, **l'article 65 du code des douanes** permet depuis longtemps aux douanes d'exiger la communication des documents de toute nature relatifs aux opérations les intéressant, quel qu'en soit le support, et notamment ceux se trouvant dans les locaux des compagnies de navigation aérienne.

Ce texte permet aux douanes de requérir **ponctuellement** et expressément les données PNR de certains vols.

Selon M. Gérard Schoen, sous-directeur des affaires juridiques et du contentieux, du contrôle et de la lutte contre la fraude à la direction générale des douanes, alors même que la transmission des données PNR se fait au cas par cas et que certaines compagnies aériennes rechignent à transmettre l'intégralité des données dont elles disposent, l'efficacité des contrôles ciblés grâce à l'analyse des données PNR serait déterminante.

Ces diverses expériences **nationales, européennes et internationales** ont eu pour effet que les opérateurs du transport aérien et leurs intermédiaires ont acquis une grande expertise dans le domaine de la gestion des données de voyage. Il n'y a pas d'obstacle technique. La principale préoccupation des opérateurs a pour objet l'harmonisation des règles des divers systèmes PNR afin de diminuer le coût des transmissions.

B. LA PROPOSITION DE DÉCISION-CADRE : VERS UN PNR EUROPÉEN

Présentée en novembre 2007, la proposition de décision-cadre a pour objectif *« d'harmoniser les dispositions des Etats membres relatives à l'obligation, pour les transporteurs aériens assurant des vols vers le territoire d'au moins un Etat membre ou à partir de celui-ci, de transmettre aux*

autorités compétentes les renseignements relatifs aux passagers aux fins de prévenir et de combattre les infractions terroristes et la criminalité organisée ».

Les grandes lignes du système PNR européen seraient les suivantes.

Seuls les **vols internationaux** en provenance ou à destination d'un Etat tiers seraient concernés. En cas de transit du vol international concerné dans un Etat membre, les données seraient également collectées.

Les finalités seraient la lutte contre le terrorisme et la criminalité organisée. Les infractions terroristes seraient celles définies par la décision-cadre 2002/475/JAI du Conseil relative à la lutte contre le terrorisme. En revanche, la définition de la criminalité organisée et de ses limites demeurent plus incertaines.

Par ailleurs, le PNR européen serait un **système décentralisé** dans un double souci d'efficacité et de respect du principe de proportionnalité. Il ne serait donc pas constitué une base de données centralisée qui concentrerait l'ensemble des données PNR des vols à destination ou au départ de l'Union européenne. Chaque Etat membre se doterait d'une Unité d'information passagers (**UIP**)¹ chargée de collecter les données PNR relatives aux vols internationaux ayant pour point de départ ou d'arrivée le territoire de l'Etat membre. Toutefois, deux Etats membres ou plus pourraient instituer ou désigner la même UIP.

Les Etats membres pourraient échanger entre eux les données PNR collectées par l'intermédiaire des UIP, mais toujours en réponse à des besoins précis. Il s'agit notamment d'éviter la constitution d'une base unique des données PNR dans l'Union européenne.

La proposition de décision-cadre privilégie la **méthode « PUSH »** pour la transmission des données PNR aux UIP. Cette méthode laisse aux transporteurs le soin de transmettre les données PNR requises, par opposition à la méthode « PULL » par laquelle l'autorité requérante accède directement au système de réservation des transporteurs.

Les données PNR devant être collectées sont définies en annexe de la proposition de décision-cadre. **19 catégories de données** sont ainsi visées². L'annexe prévoit également la transmission de données complémentaires dans le cas où le passager serait un mineur non accompagné.

Il faut préciser que la proposition de la commission européenne n'impose **aucune obligation de collecte de données supplémentaires** aux transporteurs aériens, ni d'obligation de conservation de ces données. Elle ne leur impose qu'une obligation de transmission de ces données lorsqu'ils les détiennent pour les besoins de leurs activités commerciales.

¹ L'expression « Unité de renseignement passagers » est aussi utilisée indifféremment. Cette structure serait composée de membres des services clients comme les douanes, la police et la gendarmerie.

² Annexe n°2.

A titre d'exemple, alors que la liste des données PNR comporte le numéro du siège, la proposition de décision-cadre n'aurait pas pour effet de contraindre les compagnies à bas coût qui préfèrent le placement libre à attribuer un numéro de siège.

Toujours avec le même souci de ne pas faire peser sur les transporteurs des contraintes techniques et financières excessives, la méthode « PUSH » devrait être à terme la seule retenue. La transmission des données aurait lieu deux fois : 48 ou 24h avant le départ du vol puis à la clôture de celui-ci.

S'agissant des **données sensibles** qui pourraient figurer parmi les données PNR, c'est-à-dire celles susceptibles de révéler la race, la religion, l'état de santé ou l'orientation sexuelle d'une personne¹, le texte fait le choix de **proscrire leur utilisation** par les autorités compétentes. En conséquence, les UIP seraient dans l'obligation de les effacer immédiatement.

Les données PNR ainsi recueillies pourraient être **utilisées de quatre manières** :

- évaluer le risque présenté par certains passagers ;
- créer et actualiser les hypothèses et les indicateurs de risque en vue d'évaluer ces personnes ;
- fournir des renseignements aux services opérationnels sur les déplacements de certaines personnes, en dehors d'un cadre judiciaire ;
- dans le cadre d'une procédure judiciaire.

S'agissant de l'utilisation à des fins de profilage, chaque Etat membre conserverait la maîtrise de ses critères d'évaluation du risque. La seule limite fixée par la proposition est l'interdiction de décider d'une action coercitive sur la seule base de l'analyse des données PNR. Ainsi, il ne pourrait y avoir de « liste noire » à la différence du système américain. M. Jean-Yves Topin, directeur central de la police aux frontières, a confirmé qu'aucun passager ne se verrait interdire **d'embarquer**².

Enfin, le dernier aspect important est relatif à **la durée de conservation des données**. La Commission européenne propose une durée initiale de cinq ans. A l'expiration de cette période, les données seraient conservées pour une période supplémentaire de huit ans. Pendant cette seconde phase, les données ne seraient consultables que « *dans des circonstances exceptionnelles en réponse à une menace ou à un risque spécifique et réel* ».

¹ En pratique, les exemples fréquemment cités sont ceux des informations relatives au repas pris durant le vol (hallal, casher...) ou aux problèmes de santé d'un passager (handicap...).

² En revanche, si la consultation du fichier des personnes recherchées ou du SIS est positive, les autorités à la frontière pourront toujours refuser **l'entrée** sur le territoire français.

C. UN TEXTE APPELÉ À ÉVOLUER

Présentée par la Commission européenne le 6 novembre 2007, la proposition de décision-cadre a suscité depuis de nombreuses prises de position et a évolué à la suite des négociations au sein du Conseil.

1. Des avis extérieurs critiques

Le contrôleur européen pour la protection des données¹, l'agence européenne des droits fondamentaux² et le groupe de l'article 29 sur la protection des données³ ont tous émis des avis très réservés sur la proposition de décision-cadre.

Les critiques insistent en particulier sur l'insuffisance d'éléments d'information et de retours d'expérience démontrant l'utilité et la nécessité de la collecte des données PNR à des fins répressives. Cette absence de preuve de l'intérêt du dispositif serait d'autant plus rédhibitoire que la collecte indifférenciée des données PNR de tous les passagers à destination d'un Etat membre de l'Union européenne est susceptible de porter une atteinte grave au respect des droits individuels.

Le contrôleur européen pour la protection des données critique en particulier la technique du profilage qui consiste à bâtir des hypothèses de risque à partir de données personnelles ne caractérisant pas une infraction.

L'élaboration de modèles de déplacement et de comportement conduit à fonder des décisions à l'encontre d'individus qui auront ensuite le plus grand mal à se défendre de ces décisions.

Les autres critiques portent sur le système proposé par la Commission européenne. Le droit applicable en matière de protection des données (droit d'accès, de rectification, transferts des données vers des pays tiers...) est jugé très flou, voire inexistant. La durée de conservation des données serait excessive.

De manière générale, l'ensemble de la proposition serait trop imprécise et ne répondrait pas aux principes de finalité et de proportionnalité.

De son côté, le Parlement européen a adopté une résolution le 20 novembre 2008⁴. Si elle partage plusieurs de ces critiques, notamment sur l'imprécision du texte, elle porte un jugement plus nuancé sur l'utilité des données PNR pour les services en charge de la lutte contre le terrorisme et la grande criminalité. Le Parlement européen admet que ces données puissent être très utiles comme éléments de preuve dans une enquête. En revanche, il doute de sa pertinence à des fins de profilage préventif.

¹ Avis du 1^{er} mai 2008.

² Avis du 3 décembre 2008.

³ Avis du 5 décembre 2008.

⁴ Résolution n° 2008/0561. Cette résolution ne constitue pas son avis officiel sur la proposition de décision-cadre.

2. Les travaux de la présidence française de l'Union européenne

Compte tenu de la sensibilité de la proposition et des réactions suscitées, la présidence française de l'Union européenne a entrepris un travail particulier de concertation et d'analyse. Un groupe multidisciplinaire a été mis en place.

Conformément au mandat conféré à la présidence française par le Conseil le 25 juillet 2008, celle-ci a remis un rapport le 28 novembre 2008. Il apporte des réponses précises à plusieurs critiques. Il dégage aussi de nouvelles perspectives.

S'agissant des finalités du système, le rapport dessine un consensus autour de la prévention et de la répression du terrorisme, d'une part, ainsi que d'un ensemble d'infractions graves à **définir par référence à la liste d'infractions permettant la mise en œuvre de la décision-cadre relative au mandat d'arrêt européen**, d'autre part. Cette liste comporte 32 catégories de comportements criminels.

Le rapport préconise par ailleurs **une transmission systématique** des données PNR pour tous les vols entrant dans le champ de la décision-cadre, de préférence à une collecte sélective qui serait limitée à certaines liaisons jugées plus sensibles. Toutefois, après une phase d'expérimentation, le principe d'une collecte systématique pourrait être réévalué.

Tout en précisant le champ du PNR européen, le rapport souligne qu'il n'a pas pour effet d'interdire aux Etats membres de mettre en place des dispositifs nationaux complémentaires. Le PNR européen serait un minimum commun. Les Etats membres pourraient, d'une part, collecter aussi les données PNR des **vols intracommunautaires** ou d'autres modes de transport que l'avion et, d'autre part, élargir son utilisation à **d'autres finalités** comme la lutte contre l'immigration irrégulière¹.

S'agissant du fonctionnement du système PNR et de l'exploitation des données, la présidence française a également dégagé plusieurs pistes de travail.

Un consensus semble s'être dégagé sur **l'articulation entre l'Unité d'information passagers (UIP) et les services opérationnels** en charge des contrôles et des enquêtes dans chaque Etat membre. Il serait clair que dans chaque Etat membre, **seul l'UIP aurait accès aux données PNR brutes** transmises par les transporteurs aériens. Les services de contrôle et d'enquête seraient en liaison étroite avec cette plateforme pour définir leurs besoins, mais ils ne pourraient pas accéder directement aux données PNR. Cette centralisation dans une base sécurisée sous le contrôle de l'UIP doit garantir la traçabilité et la légalité de l'utilisation de ces données.

¹ Toutefois, on notera que la lutte contre les filières d'immigration clandestine relève bien de la criminalité organisée.

Ainsi, pour le profilage, il reviendrait à l'UIP d'évaluer en temps réel les données PNR, mais sur la base de critères définis par les services opérationnels (présélection des vols, nature du risque...). Et dans le cadre d'une enquête, ces services adresseraient une requête spécifique à l'UIP.

A propos du respect des droits fondamentaux, le rapport s'est également efforcé d'apporter des réponses directes aux avis précités du contrôleur européen à la protection des données, du G29 ou du Parlement européen.

Ainsi, le rapport propose d'abandonner les données relatives aux mineurs non accompagnés.

Le régime de protection des données applicable aux différentes étapes du système PNR est également clarifié :

- la directive n° 95-46 du 24 octobre 1995 s'appliquerait à la phase de transmission des données par les transporteurs aériens aux UIP désignées ;

- au niveau national, le droit commun serait applicable, celui-ci ne pouvant être inférieur aux standards fixés par la Convention du Conseil de l'Europe du 28 janvier 1981 relative à la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. En France, la CNIL serait donc compétente dans les conditions fixées par la loi « informatique et liberté » du 6 février 1978 modifiée ;

- les échanges de données PNR entre Etats membres entreraient dans le champ de la décision-cadre 2008/977/JAI du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.

Plusieurs points sont néanmoins restés en suspens.

S'agissant **des données sensibles** susceptibles de figurer parmi les données PNR transmises, le rapport ne repousse pas la solution retenue par la proposition de décision-cadre consistant à en interdire par principe l'utilisation. Toutefois, il remarque qu'*« il est traditionnellement jugé légitime d'en permettre une utilisation raisonnée dans le contexte d'une enquête criminelle si l'information qu'elles apportent peut soit contribuer à résoudre l'enquête, soit aider à laver la personne concernée de tout soupçon »*. Si l'utilisation des données sensibles à des fins de profilage demeure ainsi strictement exclue, en revanche leur exploitation dans le cadre d'une procédure judiciaire demeure une option ouverte à ce stade.

En outre, le rapport préconise que les données sensibles soient en tout état de cause transmises par les transporteurs aux UIP. Il reviendrait à celles-ci de les effacer ou de les verrouiller.

S'agissant de **la durée de conservation**, le rapport fait le constat de divergences importantes entre les Etats membres. Un accord pourrait cependant être trouvé autour d'une première phase de conservation obligatoire

de trois ans, suivie d'une phase supplémentaire comprise entre trois et sept ans.

Une nouvelle version de la proposition de décision-cadre a alors été présentée sur la base de ces orientations.

3. Un texte en panne ?

Compte tenu du nombre de dispositions faisant encore l'objet de discussion, il est peu probable que les négociations relatives à la proposition de décision-cadre progressent véritablement avant le premier semestre 2010.

Ce calendrier est d'autant plus probable que des incertitudes planent sur la base juridique d'un système de PNR européen.

Le service juridique du Conseil jugerait nécessaire l'adoption de deux textes distincts : une directive fixant les obligations des transporteurs aériens et une décision-cadre relative à l'utilisation policière et judiciaire de ces données.

Le rapport de la présidence française conforte cette analyse. Afin d'alléger les contraintes pesant sur les transporteurs et d'offrir des garanties fortes de protection des données personnelles, il estime que le régime de protection applicable à la transmission des données PNR par les compagnies aériennes devrait être uniforme. En droit positif, la transmission des données PNR à des fins commerciales est soumise à la directive n° 95-46 du 24 octobre 1995¹. En conséquence, la phase de transmission des données PNR à l'UIP de chaque Etat membre y serait également soumise. Or, la directive du 24 octobre 1995 relève du premier pilier.

Le Parlement européen s'est saisi de cette difficulté pour remettre en cause la base juridique de la proposition de décision-cadre. Compte tenu de la volonté affichée du Conseil d'associer le plus étroitement possible le Parlement européen aux négociations, bien qu'elles entrent dans le champ du troisième pilier à ce stade, on voit mal comment le Conseil pourrait passer outre.

L'entrée en vigueur du traité de Lisbonne au cours de la présidence espagnole aurait l'avantage d'épuiser cette question en faisant disparaître la division entre piliers.

¹ Directive n° 95-46 du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

II. LA PROPOSITION DE RÉOLUTION ET LA POSITION DE VOTRE COMMISSION

La proposition de résolution européenne adoptée par la commission des affaires européennes du Sénat ne rejette pas le principe d'un système PNR européen. Elle exprime néanmoins des critiques fortes à l'encontre de la proposition de décision-cadre, le droit au respect de la vie privée et à la protection des données à caractère personnel n'étant pas garanti en l'état du texte.

Cette vigilance est d'autant plus justifiée qu'à plusieurs reprises, la commission des affaires européennes a attiré l'attention sur les graves insuffisances des accords conclus entre les Etats-Unis et l'Union européenne pour le transfert des données PNR vers les Etats-Unis¹.

Les standards du PNR européen doivent être bien plus protecteurs des droits fondamentaux.

A. DEUX QUESTIONS FONDAMENTALES À TRANCHER : LES DONNÉES PNR SONT-ELLES RÉELLEMENT UTILES ET FAUT-IL UN « PNR EUROPÉEN » ?

1. Des données utiles...

L'utilité des données PNR demeure un sujet de controverse. Ainsi, le G29 ou le contrôleur européen de la protection des données remarquent l'absence d'éléments chiffrés démontrant l'utilité et la nécessité de ces données pour les services de sécurité. A l'opposé, les services en charge de la lutte contre le terrorisme et la criminalité organisée affirment que ces données sont une mine de renseignements extrêmement utiles et que leur exploitation n'est en aucune façon redondante avec d'autres dispositifs en vigueur comme les données APIS ou les visas biométriques.

Sans apporter de réponses définitives, les éléments précis et chiffrés manquant effectivement, votre rapporteur estime compte tenu des auditions et des premiers retours d'expérience que les données PNR ne sont pas redondantes avec d'autres dispositifs et sont une aide précieuse pour les services de sécurité.

Sur le premier point –une éventuelle redondance avec d'autres systèmes en vigueur (collecte des données APIS, consultation du Système d'information Schengen, mise en place d'un système européen de visa biométrique, obligation d'un passeport biométrique...)-, votre rapporteur attire l'attention sur le fait que ces systèmes sont particulièrement utiles pour identifier une personne avec certitude et déclencher des mesures (arrestation, refoulement, surveillance...) lorsque cette personne attire déjà l'attention des services de sécurité.

¹ Voir notamment le compte-rendu de la réunion de la commission des affaires européennes du Sénat du 19 septembre 2006.

Les données PNR sont d'une autre nature. Elles sont aussi utiles pour détecter des personnes non connues a priori des services de sécurité mais dont certains comportements peuvent être révélateurs d'un risque pour la sécurité. Poussant le raisonnement à l'extrême, M. Gérard Schoen de la direction générale des douanes a déclaré à votre rapporteur que la donnée PNR la moins intéressante était en définitive le nom du passager. Le profilage s'effectue à partir de l'analyse des autres données PNR, le nom permettant dans un second temps de relier cette analyse à un individu. Au demeurant, le nom est une des données les moins fiables du système PNR. Pour s'assurer de l'identité d'une personne, la consultation des données APIS et des documents de voyage est le moyen le plus pertinent.

Sur le second point, l'analyse des données PNR permet de bâtir des hypothèses de risque relativement fiables et de cibler en retour des contrôles ou la mise en place d'une surveillance.

En matière douanière, M. Gérard Schoen a révélé que le ciblage des contrôles à partir des données PNR était désormais un outil primordial et décisif pour l'efficacité de ses services. Entre 60 et 80 % des stupéfiants saisis par la douane dans les aéroports le sont à la suite d'un tel ciblage¹.

Des tests montrent que le taux de résultat des contrôles ciblés est huit fois supérieur à celui des contrôles aléatoires.

Ces résultats supposent une actualisation continue des hypothèses de risque, les stratégies des filières étant extrêmement fluctuantes. Pour y parvenir, les douanes testent des modèles de ciblage. Sont ainsi analysés les cas des personnes arrêtées aléatoirement pour tenter de discerner un critère objectif qui aurait permis de le détecter par la méthode de ciblage.

Efficaces pour lutter contre les trafics, les données PNR le sont également pour lutter contre le terrorisme, même s'il est plus difficile d'évaluer la plus-value.

M. Bernard Squarcini, directeur central du renseignement intérieur, a expliqué à votre rapporteur que le terrorisme international ne reposait plus sur un support étatique, mais s'appuyait sur des individus relativement isolés agissant en réseau. Cette évolution de la menace implique une détection précoce afin d'évaluer la dangerosité, cerner l'environnement et « *neutraliser judiciairement l'individu avant le passage à l'acte* ».

Dans ce contexte, les données PNR sont précieuses. Elles fournissent une multitude de petites informations qui, agrégées à d'autres, sont autant de signaux d'alarme. M. Bernard Squarcini a souligné qu'en matière de renseignement, il était très rare qu'une donnée soit décisive. Les données PNR ne dérogent pas à cette règle. Elles ne viennent que compléter une panoplie documentaire. C'est la raison pour laquelle il est très difficile d'évaluer la plus-value propre des données PNR dans la lutte antiterroriste comme le souhaiteraient de nombreux critiques du projet de PNR européen.

¹ Les douanes saisissent environ 75 % des stupéfiants en France.

Enfin, votre rapporteur estime que l'efficacité du système peut nécessiter de croiser les données PNR avec les données APIS et les fichiers SIS et FPR. C'est d'ailleurs ce que permet déjà la loi du 23 janvier 2006 relative à la lutte contre le terrorisme.

2. ...à mettre en regard avec les risques pour le respect des droits fondamentaux

L'argument de l'utilité des données PNR ne peut suffire à lui seul à justifier la mise en œuvre d'un système de collecte automatique de ces données à des fins répressives.

Le principe de proportionnalité requiert de mettre en balance les gains pour la sécurité et les sacrifices consentis au détriment du respect des droits fondamentaux.

Les systèmes PNR peuvent être comparés à des « filets dérivants » capturant de nombreuses données relatives à des citoyens ordinaires afin, d'une part, de détecter des activités terroristes ou criminelles et, d'autre part, de pouvoir réveiller ces données pendant plusieurs années en cas de besoin. Cette démarche est distincte de celle des fichiers de police traditionnels qui ont pour objet d'accumuler des données sur des personnes déjà connues des services.

Le principal reproche fait à ces collectes indifférenciées de données est de considérer chaque utilisateur comme un suspect a priori. Ses données personnelles sont conservées au cas où elles se révéleraient intéressantes **ultérieurement**.

Si ces critiques sont fondées, elles ne doivent pas faire oublier qu'une personne qui passe une frontière s'expose toujours à des contrôles exorbitants par rapport à ceux auxquels elle est exposée sur le territoire d'un Etat de droit. Le développement des systèmes PNR peut dès lors apparaître comme n'étant pas d'une nature si différente des contrôles applicables à ce jour aux voyageurs internationaux (questionnaires à l'entrée, contrôle d'identité, fouille des bagages...). Ils sont la traduction du principe de souveraineté.

La proposition de décision-cadre limite strictement son champ aux vols extracommunautaires. A cette condition, votre rapporteur estime que le principe de proportionnalité est respecté. Le principe d'un système PNR européen est acceptable.

Une fois le principe admis, la vigilance doit s'exercer sur les modalités de mise en œuvre de ce système.

3. L'intérêt d'une harmonisation européenne

Votre commission estime que le principe de subsidiarité est respecté.

Une harmonisation européenne présente de nombreux avantages.

Compte tenu de la libre circulation dans l'espace Schengen, l'intérêt d'un système PNR relativement homogène dans l'ensemble de cet espace est évident, car chaque Etat membre est responsable de sa frontière pour le compte de l'ensemble des autres Etats membres.

En outre, une harmonisation des solutions techniques retenues devrait réduire les contraintes et les coûts pour les opérateurs du transport aérien.

Compte tenu de l'expérience acquise et de l'existence de sociétés gérant les données PNR pour le compte des compagnies aériennes¹, le coût de la transmission des données aux autorités compétentes est évalué entre 10 et 20 centimes d'euro par passager. Plus l'harmonisation sera forte, plus ce coût sera faible. A cet égard, votre rapporteur est attaché à ce que la proposition de décision-cadre n'impose aucune obligation supplémentaire de collecte ou de conservation des données PNR.

Enfin, la mise en œuvre de solutions homogènes devrait renforcer la capacité de négociation de l'Union européenne vis-à-vis des Etats tiers qui disposent ou souhaiteraient se doter de systèmes similaires. Rappelons que lors de la négociation de l'accord entre les Etats-Unis et l'Union européenne, certains Etats-membres avaient été tentés de conclure des accords bilatéraux.

B. LA DÉFINITION DU CHAMP DU PNR EUROPÉEN

1. Des finalités à préciser

Votre commission rejoint parfaitement les préoccupations de la proposition de résolution relatives à une définition précise des finalités du système.

Si la lutte contre le terrorisme est définie de manière satisfaisante par référence à la décision-cadre 2002/475/JAI du Conseil relative à la lutte contre le terrorisme, il n'en est pas de même des autres infractions qui pourraient justifier l'utilisation des données PNR. Les références à des infractions graves ou à la criminalité organisée sont trop floues.

Les travaux du Conseil ont dégagé une piste intéressante. Les infractions graves seraient définies par référence à la liste d'infractions établie dans la décision-cadre 2002/584/JAI du 13 juin 2002 relative au mandat

¹ Ces sociétés sont dénommés « intermédiaires » par la proposition de décision-cadre. Deux sociétés se partagent l'essentiel de ce marché.

d'arrêt européen. Cette liste porte sur 32 catégories de comportements criminels¹ et est une référence importante reconnue par l'ensemble des Etats membres.

Cette solution serait satisfaisante. **Néanmoins, votre commission souligne que la référence à ces 32 catégories d'infractions n'exonère pas d'un examen de chaque catégorie afin de s'assurer de leur pertinence par rapport à l'exploitation des données PNR.**

Les raisons qui ont justifié l'inscription d'une infraction parmi la liste des infractions permettant le recours au mandat d'arrêt européen ne sont pas nécessairement valables lorsqu'on les applique au système PNR.

2. Quelles données collecter ?

Votre commission estime que la liste des données PNR qui devrait être transmise est pertinente et nécessaire dans sa quasi-totalité, les exemples cités par les services de sécurité démontrant l'utilité potentielle de chacune.

Une seule catégorie de données pose des difficultés : les données sensibles.

Ces données sensibles, c'est-à-dire celles « *révélant la race ou l'origine ethnique, les convictions religieuses, les opinions politiques, l'appartenance à un syndicat, la santé ou l'orientation sexuelle* » ne constituent pas à proprement parler une des catégories de données PNR.

Lorsque ces données figurent parmi les données PNR transmises, elles se trouvent en réalité dans la rubrique « 12) Remarques générales ». Cette rubrique est un champ libre dans lequel les compagnies aériennes peuvent inscrire des informations relatives au handicap d'une personne ou à ses préférences alimentaires par exemple.

La CNIL a souligné que de manière générale, il était de bonne pratique au regard de la protection des données à caractère personnel de proscrire les champs libres. Ces rubriques sont très difficiles à contrôler.

Les avis du G29, du contrôleur européen de la protection des données, du Parlement européen ainsi que les réactions de nombreuses organisations de protection des droits de l'homme sont unanimes pour critiquer l'utilisation, voire la simple transmission de ces données dans le cadre du PNR européen.

Pour sa part, la proposition de résolution demande que l'utilisation de ces données sensibles soit en principe exclue. Toutefois, si comme les travaux du Conseil l'envisagent, ces données étaient malgré tout utilisées, la proposition de résolution souhaite qu'elles ne soient utilisées que dans le cadre d'une enquête et non à des fins de profilage ou de simple renseignement.

¹ Voir l'annexe n° 3.

La question de l'utilisation des données sensibles pose également des problèmes techniques importants. Ces données figurant dans une rubrique « champ libre », comment faire pour les filtrer ? Ce filtrage doit-il revenir aux compagnies aériennes lors de la transmission ou aux UIP ?

Pour concilier ces équations contradictoires, **vo**tre **commission propose d'exclure purement et simplement de la liste des données PNR transmises la rubrique « 12) Remarques générales ».**

Cette solution présente plusieurs avantages.

La question du filtrage des données sensibles au sein de la rubrique « Remarques générales » ne se posera plus. En outre, elle répond à la fois aux critiques contre l'utilisation des données sensibles et aux réticences plus générales de la CNIL quant à l'utilisation des champs libres.

Mais surtout, cette solution permettra d'apaiser le débat sur le PNR européen sans que les capacités opérationnelles des services de sécurité ne soient véritablement affectées.

En effet, les auditions des responsables de ces services ont fait apparaître que cette rubrique était en définitive la moins utile. On notera enfin que la loi du 23 janvier 2006 relative à la lutte contre le terrorisme écarte expressément l'utilisation des données sensibles.

3. L'exclusion des vols intracommunautaires

La proposition de décision-cadre initiale exclut la collecte des données PNR des vols intracommunautaires, à l'exception des vols de transit.

Toutefois, les travaux du Conseil ont laissé ouverte la possibilité pour les Etats membres le désirant de collecter également ces données PNR. Le programme britannique e-borders le prévoit.

L'harmonisation des systèmes PNR européens serait donc une harmonisation minimale, les Etats membres pouvant se doter de dispositifs plus vastes.

Si chaque Etat membre demeure souverain, votre rapporteur estime que la France devrait s'interdire de mettre en œuvre un système national de collecte automatisé des données PNR **des vols nationaux, voire intracommunautaires**. A son sens, l'équilibre entre sécurité et liberté ne serait plus respecté.

C. LE FONCTIONNEMENT DU PNR EUROPÉEN

1. Réduire la durée de conservation des données

La proposition de décision-cadre initiale proposait une durée de conservation de 13 ans (5 ans suivis d'une période de 8 ans durant laquelle les données ne seraient consultables qu'en cas de circonstances exceptionnelles). Les travaux du Conseil semblent vouloir ramener cette durée entre 6 et 10 ans (3 ans suivis d'une période de 3 ou 7 ans).

La proposition de résolution européenne juge manifestement disproportionnée la durée de treize ans. Votre commission partage cette analyse. L'ensemble des responsables policiers ou douaniers entendus par votre rapporteur ont estimé qu'une durée de 5 ans était largement suffisante, les comportements des terroristes et des filières étant très mouvants.

La ligue des droits de l'homme a suggéré de distinguer une durée de conservation et une durée de préservation. Dans une première phase, toutes les données PNR seraient conservées. Dans une seconde phase, seules seraient préservées les données ayant déjà démontré un intérêt au cours de la première phase. Cette solution originale a pour principal mérite de réduire le volume des données conservées.

Votre commission préconise par conséquent **une première phase de conservation de trois ans à laquelle succéderait une phase de préservation de trois ans des seules données présentant un intérêt particulier**. A titre d'illustration, les critères pourraient être les suivants :

- les données ont déjà révélé un risque particulier ;
- les données se rattachent à une ligne particulièrement sensible ou à une agence de voyage ayant fréquemment attiré l'attention ;
- les données ont été consultées à des fins de renseignement ;
- une enquête est en cours.

Le fichier des données PNR se rapprocherait ainsi, au cours de cette seconde phase, du format habituel d'un fichier de police.

2. Adopter la méthode « PUSH »

La proposition de résolution européenne estime que seule la méthode dite « PUSH » offre les garanties nécessaires en laissant aux transporteurs aériens le contrôle de la qualité des données transmises et des conditions de transmission.

Votre commission partage absolument ce point de vue et juge qu'aucune phase transitoire ne devrait donner lieu à la mise en œuvre de la méthode inverse dite « PULL ». Les transporteurs aériens ont désormais acquis une véritable expérience des systèmes PNR et sont donc en mesure d'adopter la méthode « PUSH ».

3. Préciser les destinataires des données

La proposition de résolution attire l'attention sur la clarification des rôles entre les UIP et les services de sécurité qui pourront demander des données PNR.

Votre commission partage ce souci. Il ne devrait pas être possible aux services de sécurité d'accéder aux données PNR brutes, l'UIP devant demeurer un sas entre les données et les services utilisateurs.

De même, alors que la proposition de résolution juge nécessaire des précisions sur la qualité des services qui composeront les UIP et la liste des services de sécurité qui pourront utiliser les données, votre commission propose d'ajouter qu'au sein de ces services, seuls des agents individuellement désignés et spécialement formés pourront utiliser ces données.

En effet, le renvoi à une simple liste des services autorisés n'apparaît pas suffisant. Votre rapporteur observe que la loi du 23 janvier 2006 relative à la lutte contre le terrorisme dispose déjà que l'accès aux données PNR lorsqu'elles sont traitées aux fins de prévenir et de réprimer le terrorisme est limité aux « *agents individuellement désignés et dûment habilités* » des services compétents.

4. Renforcer le droit des personnes concernées

Les droits des personnes concernées étaient particulièrement incertains et flous dans la proposition de décision-cadre initiale.

Les travaux du Conseil ont permis des avancées indiscutables et la dernière version du texte apporte des réponses satisfaisantes à propos du droit à l'information, du droit d'accès aux données et de l'exercice des droits de rectification et d'effacement

Le régime légal applicable a été clarifié à chaque étape de la transmission et de l'utilisation des données PNR (voir le I.C.2)).

En outre, des garanties supplémentaires devraient figurer dans le texte de la décision-cadre qui définirait elle-même ses propres règles en matière de protection des données lors de la phase de traitement des données par les UIP.

Comme le relève le rapport d'information de la commission chargée des affaires européennes de l'Assemblée nationale sur la proposition de décision-cadre¹, il convient de noter que « *cet ensemble de droits applicable aux données traitées par les UIP, c'est-à-dire par des autorités publiques nationales, est inspiré des droits de la décision-cadre [2008/977/JAI du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale] dont les Etats membres n'avaient pas voulu qu'elle s'applique aux*

¹ Rapport d'information n° 1447-XIIIème législature de M. Guy Geoffroy.

*données traitées sur le plan interne mais **uniquement aux données échangées entre Etats membres**. La proposition de décision-cadre constituerait donc un pas en avant dans l'extension du champ de la protection des données réglementée au niveau européen dans le troisième pilier »¹.*

Ces avancées notables méritent d'être soulignées.

Mais elles ne conduisent pas votre commission à revenir sur les termes de la proposition de résolution. Sur ces questions essentielles, la vigilance doit demeurer en réaffirmant :

- la compétence des autorités indépendantes sur la protection des données –la CNIL en France- pour effectuer des contrôles au sein des UIP ;

- la nécessité de clarifier le dispositif, de façon à ce que les responsables des traitements soient immédiatement identifiables par les personnes souhaitant exercer leur droit d'accès ou de rectification ;

- l'intérêt de fixer dans le corps même de la proposition de décision-cadre les garanties nécessaires, en l'absence d'instrument juridique européen fixant des règles générales de protection de données en matière de police.

5. Limiter la transmission des données à des Etats tiers

La question de la transmission de données PNR à des Etats tiers a soulevé des inquiétudes importantes parmi les personnes entendues par votre rapporteur.

La proposition de décision-cadre initiale prévoyait peu de garde-fous. Elle disposait uniquement que les autorités du pays tiers devaient poursuivre des finalités identiques et que le pays tiers concerné ne pouvait transmettre ces données à un autre pays tiers sans l'accord explicite de l'Etat membre lui ayant transmis les données.

A la suite des travaux de la présidence française, les conditions de ces transferts ont été précisées. Il est désormais expressément prévu que :

- le pays tiers doit offrir un niveau de protection adéquat ;

- dans le cas où les données transmises par un Etat membre ont été obtenues par celui-ci auprès d'un autre Etat membre, le consentement de ce dernier a été recueilli.

Pour autant, votre commission estime que la vigilance doit rester de mise et approuve par conséquent les termes de la proposition de résolution sur ce sujet.

¹ Rappelons en effet que la directive n° 95-46 du 24 octobre 1995 relative à la protection des données à caractère personnel ne s'applique qu'aux matières relevant du premier pilier. Les questions de police en sont exclues.

En effet, plusieurs points importants n'ont pas été éclaircis dont celui du volume des données transférables.

La proposition de décision-cadre permettrait de procéder à des transferts de données PNR en masse vers des pays tiers. Cela n'est pas acceptable. Le principe doit être celui d'une transmission au cas par cas en réponse à des besoins spécifiques et motivés.

D. UNE TRANSPOSITION PAR LA LOI

Votre commission souhaite enfin marquer son souhait que la transposition de la décision-cadre, si ce texte est définitivement adopté, se fasse par la loi.

En effet, le gouvernement a le choix lorsqu'il crée un fichier de police entre le recours au pouvoir réglementaire et le passage par la loi. L'expérience de ces dernières années montre qu'il use de cette alternative en fonction des circonstances. Il faut d'ailleurs souligner que le passage par la loi est de plus en plus utilisé.

Compte tenu de l'enjeu de la création d'un PNR européen, il apparaît à votre commission que la transposition de la décision-cadre ne pourrait se faire raisonnablement que par la loi.

Cette solution se justifie d'autant plus que la proposition de décision-cadre devrait laisser aux Etats membres une latitude importante pour étoffer leur système PNR national ou préciser les conditions dans lesquelles les services de police accèdent aux données conservées par les UIP.

*

* *

Au bénéfice de l'ensemble de ces observations, votre commission a adopté une proposition de résolution, dont le texte est reproduit ci-après.

PROPOSITION DE RÉSOLUTION

(texte adopté par la commission des Lois en application de l'article 73 bis du règlement du Sénat)

Le Sénat :

Vu l'article 88-4 de la Constitution ;

Vu la proposition de décision-cadre relative à l'utilisation des données des dossiers passagers (Passenger Name Record – PNR) à des fins répressives (E 3697) ;

– prenant acte que cette proposition de décision-cadre tend à promouvoir une approche harmonisée au sein de l'Union européenne de l'utilisation des données des dossiers passagers à des fins répressives et que des discussions sont en cours au sein du Conseil ;

– considère qu'une telle approche doit retenir parmi ses priorités d'assurer un respect effectif des droits fondamentaux, en particulier le droit au respect de la vie privée et à la protection des données à caractère personnel ;

– souligne que les finalités de la proposition doivent être précisément délimitées et concerner exclusivement la prévention, la détection, l'instruction, la poursuite et la répression du terrorisme et d'un ensemble d'infractions graves, définies par référence à la liste d'infractions établie dans la décision-cadre relative au mandat d'arrêt européen, pour lesquelles l'utilisation de données des dossiers passagers s'avérerait pertinente ;

– estime que seule la méthode de transmission dite « PUSH » peut offrir les garanties nécessaires en permettant aux transporteurs aériens de garder le contrôle de la qualité des données transmises et des conditions de transmission ;

– juge nécessaire que des précisions et des garanties supplémentaires soient prévues sur la qualité des services qui seront chargés de l'unité de renseignements passagers et celle des autorités compétentes pour recevoir les données PNR et les traiter, ainsi que sur les conditions dans lesquelles des intermédiaires seraient susceptibles d'intervenir dans la collecte et la transmission des données ;

– estime qu'au sein de ces autorités, seuls des agents individuellement désignés et dûment habilités devraient pouvoir accéder aux données PNR ;

– demande que les autorités indépendantes sur la protection des données soient habilitées à effectuer des contrôles au sein de l'unité de renseignements passagers ;

– demande que la rubrique « 12) Remarques générales », qui est la seule où des données sensibles peuvent figurer, soit exclue de la liste des données PNR transmises ;

– juge manifestement disproportionnée la durée totale de treize ans prévue par la proposition pour la conservation des données ;

– propose une durée de conservation de trois ans, à laquelle pourrait succéder une durée de conservation de trois ans des seules données PNR ayant montré un intérêt particulier au cours de la première période ;

– estime que le régime de protection des données applicable doit être clarifié, en privilégiant un haut niveau de protection par référence aux standards du Conseil de l'Europe ;

– demande que des garanties supplémentaires soient prévues dans le texte même de la proposition sur les droits des personnes concernées, en particulier pour l'exercice du droit à l'information, du droit d'accès, de rectification et d'effacement des données et que le responsable du traitement chargé de donner suite à leurs demandes soit précisément identifié ;

– considère que les conditions dans lesquelles les données seraient susceptibles d'être transmises à des États tiers n'offrent pas les garanties suffisantes ; demande, en conséquence, qu'un tel transfert ne soit possible qu'au cas par cas et sous réserve que l'État tiers assure un niveau de protection adéquat des données et que des garanties soient prévues dans la mise en œuvre du principe de réciprocité ;

– considère que la transposition de la proposition de décision-cadre devra être réalisée par la loi compte tenu des enjeux pour assurer un respect effectif des droits fondamentaux.

EXAMEN EN COMMISSION MERCREDI 13 MAI 2009

La commission a tout d'abord procédé à l'examen du rapport de M. Yves Détraigne sur la proposition de résolution européenne n° 252 (2008-2009), en application de l'article 73 bis du Règlement, présentée par M. Simon Sutour au nom de la commission des affaires européennes, sur la proposition de décision-cadre relative à l'utilisation de données des dossiers passagers (Passenger Name Record) à des fins répressives (E 3697).

M. Yves Détraigne, rapporteur, a tout d'abord rappelé :

- que la proposition de décision-cadre, transmise au Sénat au titre de l'article 88-4 de la Constitution, avait pour objectif « d'harmoniser les dispositions des Etats membres relatives à l'obligation, pour les transporteurs aériens assurant des vols vers le territoire d'au moins un Etat membre ou à partir de celui-ci, de transmettre aux autorités compétentes les renseignements relatifs aux passagers aux fins de prévenir et de combattre les infractions terroristes et la criminalité organisée » ;

- que la commission des affaires européennes, réunie le 3 mars 2009, avait adopté une proposition de résolution, présentée par M. Simon Sutour, qui, tout en approuvant le principe d'un système PNR (Passenger Name Record) européen, avait considéré que la proposition de décision-cadre ne protégeait pas suffisamment la vie privée et les données à caractère personnel ;

- que les dossiers passagers, collectés et conservés par les compagnies aériennes et les agences de voyage, contenaient diverses informations telles que les renseignements sur l'agence de voyage auprès de laquelle la réservation est effectuée, l'itinéraire du déplacement, les indications des vols, le contact à terre du passager, les services demandés à bord... renseignements dont l'importance en matière de lutte contre le terrorisme avait conduit trois pays à se doter d'un système de traitement des données PNR : les Etats-Unis, le Canada et l'Australie -la Corée du Sud ayant un projet en cours. Ces systèmes, a-t-il précisé, ont donné lieu à la conclusion d'accords avec l'Union européenne pour régler les modalités de la transmission et de l'exploitation des données PNR issues de vols en provenance d'un Etat membre et à destination de l'un de ces trois pays.

Il a souligné que les expériences européennes étaient, elles, limitées, seul le Royaume-Uni ayant à ce jour décidé de se doter d'un système PNR complet, en vigueur depuis mars 2008. La France, quant à elle, n'a pas mis en œuvre un tel traitement, alors que la loi du 23 janvier 2006 relative à la lutte contre le terrorisme l'y autorise afin d'améliorer le contrôle aux frontières, la lutte contre l'immigration clandestine et le terrorisme, sous réserve de ne pas collecter des données dites sensibles au sens de la loi du 6 janvier 1978 « informatique et libertés ». La mise en œuvre de la loi de 2006 ne s'est en effet traduite que par la création, la même année, d'un fichier qui ne concerne que les données des

passagers des vols directs en provenance et à destination de cinq pays (l'Afghanistan, le Pakistan, l'Iran, la Syrie et le Yémen).

Présentant les grandes orientations du système PNR prévu par la proposition de décision-cadre, M. Yves Détraigne, rapporteur, a expliqué que :

- seuls les vols en provenance ou à destination d'un Etat tiers seraient concernés, y compris en cas de transit sur le territoire de l'Union européenne ;

- les finalités seraient la lutte contre le terrorisme et la criminalité organisée ;

- le PNR européen serait un système décentralisé : chaque Etat membre se doterait d'une Unité d'information passagers (UIP) chargée de collecter les données PNR relatives aux vols ayant pour point de départ ou d'arrivée son territoire. Les Etats membres pourraient échanger entre eux les données PNR collectées par l'intermédiaire des UIP, mais toujours en réponse à des besoins précis ;

- les UIP seraient tenues d'effacer immédiatement les données sensibles qui pourraient figurer parmi les données PNR, c'est-à-dire celles susceptibles de révéler l'origine ethno- raciale, la religion, l'état de santé ou l'orientation sexuelle d'une personne ;

- s'agissant de l'utilisation à des fins de profilage, chaque Etat membre conserverait la maîtrise de ses critères d'évaluation du risque, la seule limite fixée par la proposition étant l'interdiction de décider d'une action coercitive sur la seule base de l'analyse des données PNR ;

- enfin, les données seraient conservées pendant treize ans mais ne seraient consultables, après cinq ans, que « dans des circonstances exceptionnelles en réponse à une menace ou à un risque spécifique et réel ».

M. Yves Détraigne, rapporteur, a ensuite souligné que la proposition de décision-cadre, critiquée par certains comme trop imprécise et contraire aux principes de finalité et de proportionnalité, avait fait l'objet d'un rapport présenté le 28 novembre 2008 sous la présidence française de l'Union européenne, dont il a exposé les grandes lignes :

- s'agissant des finalités du système, le rapport dessine un consensus autour, d'une part, de la lutte contre le terrorisme, d'autre part, de la répression d'un ensemble d'infractions graves à définir par référence à la liste d'infractions permettant la mise en œuvre de la décision-cadre relative au mandat d'arrêt européen ;

- le rapport souligne que le PNR européen n'aurait pas pour effet d'interdire aux Etats membres de mettre en place des dispositifs nationaux complémentaires destinés, par exemple, à collecter également les données PNR des vols intracommunautaires ou à élargir son utilisation à d'autres finalités comme la lutte contre l'immigration irrégulière ;

- pour respecter le principe de proportionnalité, le rapport propose, par exemple, d'abandonner les données relatives aux mineurs non accompagnés ;

- au niveau national, le droit commun serait applicable, ce qui impliquerait notamment la compétence des autorités de protection des données, telles que la CNIL ;

- les échanges de données PNR entre Etats membres entreraient dans le champ de la décision-cadre 2008/977/JAI du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.

M. Yves Détraigne, rapporteur, a toutefois souligné que le rapport laissait deux points majeurs en suspens.

D'une part, le rapport note, s'agissant des données sensibles, qu'il est « traditionnellement jugé légitime d'en permettre une utilisation raisonnée dans le contexte d'une enquête criminelle » alors que la proposition de décision-cadre prohibe par principe la conservation de telles données.

D'autre part, le rapport fait le constat de divergences importantes entre les Etats membres concernant la durée de conservation des données.

Le rapporteur a ensuite souligné que le système PNR, tel qu'envisagé par la proposition de décision-cadre, lui paraissait :

- nécessaire pour assurer la sécurité en Europe car susceptible, d'une part, de fournir une multitude d'informations en apparence de faible importance mais qui, croisées avec d'autres, sont autant de signaux d'alarme, d'autre part, d'aboutir à une harmonisation européenne, rendue indispensable par la libre circulation des personnes au sein de l'espace Schengen ;

- conforme au principe de proportionnalité dès lors que le texte limite strictement le champ du PNR aux vols extracommunautaires.

Examinant la proposition de résolution adoptée par la commission des affaires européennes, M. Yves Détraigne, rapporteur :

- a déclaré partager son souhait de définir précisément les finalités du système PNR, soulignant que, si la lutte contre le terrorisme était définie de manière satisfaisante par référence à la décision-cadre 2002/475/JAI du Conseil relative à la lutte contre le terrorisme, les références à des infractions graves ou à la criminalité organisée pouvaient, dans un souci de clarification, renvoyer à la liste d'infractions établie dans le cadre du mandat d'arrêt européen, comme préconisé par le rapport précité du 28 novembre 2008 ;

- a relevé que la proposition de résolution européenne avait demandé que l'utilisation des données sensibles soit en principe exclue, que leur filtrage soit assuré directement par les transporteurs aériens et que, si leur conservation était envisagée en vue de l'éventuelle utilisation dans le cadre d'une enquête, des garanties spécifiques soient apportées. Il a souligné que cette solution, outre qu'elle posait des problèmes techniques tenant aux modalités de filtrage, présentait un risque d'atteinte à la vie privée. Il a en conséquence proposé d'exclure purement et simplement de la liste des données PNR transmises la

rubrique « Remarques générales », champ libre seul susceptible de recueillir les données sensibles ;

- s'est félicité que la proposition de décision-cadre exclue la collecte des données PNR des vols intracommunautaires et a souhaité que la France ne mette pas en œuvre un système complémentaire national de collecte automatisée des données PNR des vols nationaux, voire intracommunautaires ;

- s'est réjoui que la proposition de résolution européenne ait jugé manifestement disproportionnée la durée totale de treize ans prévue par la proposition de décision-cadre pour la conservation des données, et, en conséquence, a préconisé une première phase de conservation de trois ans à laquelle succéderait une phase de préservation de trois ans des seules données présentant un intérêt particulier ;

- a partagé la volonté de la commission des affaires européennes d'attirer l'attention sur la clarification des rôles entre les UIP et les services de sécurité qui pourraient demander l'accès aux données PNR ;

- a souhaité compléter la proposition de résolution, qui juge nécessaires des précisions sur la qualité des services qui composeront les UIP et la liste des services de sécurité qui pourront utiliser les données, afin d'ajouter qu'au sein de ces services seuls des agents individuellement désignés et spécialement formés pourront requérir des données ;

- a appelé de ses vœux, comme la proposition de résolution, le renforcement des droits des personnes, soulignant que si les travaux du Conseil avaient d'ores et déjà permis des avancées indiscutables notamment en prévoyant un droit à l'information ainsi qu'à l'accès et la rectification des données, des garanties supplémentaires devraient figurer dans le texte de la décision-cadre, parmi lesquelles la compétence des autorités indépendantes sur la protection des données pour effectuer des contrôles au sein des UIP ainsi que la nécessaire clarification du dispositif de façon à ce que les responsables des traitements soient immédiatement identifiables par les personnes souhaitant exercer leur droit d'accès ou de rectification ;

- a approuvé les termes de la proposition de résolution concernant la limitation de la transmission des données à des Etats tiers. Après avoir souligné que la proposition de décision-cadre permettrait de procéder à des transferts de données PNR en masse vers des pays tiers, il a marqué sa préférence pour une transmission au cas par cas en réponse à des besoins spécifiques et motivés ;

- enfin, a jugé nécessaire que le législateur soit saisi en cas de transposition de la décision-cadre.

M. Simon Sutour a salué la qualité du travail du rapporteur et s'est réjoui en particulier que ses propositions marquent clairement la compétence du législateur pour transposer la décision-cadre et préconisent une durée totale de conservation des données de six ans au lieu des treize envisagés par la proposition de décision-cadre.

Toutefois, il a précisé que, à la différence du rapporteur qui semblait approuver le principe d'un PNR européen, la proposition de résolution se bornait à en prendre acte.

Il a souhaité que le Sénat adopte une résolution ambitieuse, conscient que le processus européen de négociation à vingt-sept conduirait nécessairement à certains compromis.

Notant que certaines commissions nommaient rapporteur un sénateur qui avait déjà rapporté le même texte, au nom de la commission des affaires européennes, alors que d'autres privilégiaient un examen par un autre sénateur, il a appelé de ses vœux une harmonisation des pratiques sur ce point.

M. Jean-Jacques Hyst, président, a souligné l'intérêt de désigner, comme le pratique la commission des lois pour les propositions de résolution européenne comme pour les propositions de loi, un rapporteur différent de l'auteur afin d'apporter un double regard à l'examen de ces textes. Toutefois, il a jugé que cette bonne pratique ne devrait pas être érigée en règle et qu'il était préférable de ménager une souplesse.

M. François Zocchetto a approuvé le projet de PNR européen, susceptible selon lui de renforcer la lutte contre le terrorisme tout en apportant des garanties pour les personnes au regard des pratiques actuelles. Il s'est également félicité que le rapporteur ait, d'une part, proposé d'exclure les données sensibles de la liste des données PNR transmises, d'autre part, affirmé la compétence du législateur en matière de transposition de la décision-cadre.

Il a demandé si la proposition de décision-cadre ne visait que la transmission des données PNR des vols internationaux.

M. Yves Détraigne, rapporteur, a confirmé que la proposition initiale proscrit l'utilisation des données PNR des vols intracommunautaires.

Approuvant les conclusions du rapport, en particulier celles concernant la compétence législative, M. Jean-René Lecerf a souhaité que les gouvernements entendent davantage la voix des parlements sur les enjeux de sécurité et de libertés publiques, regrettant, à titre d'exemple, l'absence de consultation parlementaire sur la mise en place du système PNR américain et espérant la plus grande prise en compte de la résolution du Sénat sur le PNR européen.

Toutefois, il a souligné le décalage entre les précautions prises au niveau européen et les conditions très défavorables dans lesquelles les Etats-Unis collectent et conservent pour de longues durées des données relatives aux passagers à destination de ce pays.

M. François Pillet a jugé complexe la proposition du rapporteur concernant la durée de conservation des données et a marqué sa préférence pour une durée unique de dix ans, alignée sur le délai de prescription en matière criminelle.

En réponse à M. François Zocchetto qui demandait comment s'assurer de la complète destruction des données à l'expiration du délai de leur conservation, M. Yves Détraigne, rapporteur, a noté, d'une part, que l'accès réduit à ces données limitait le risque de copie, d'autre part, qu'il appartenait aux autorités de contrôle des données, telles que la Commission nationale de l'informatique et des libertés (CNIL) en France, de contrôler leur suppression effective et irréversible, ajoutant que les contrevenants s'exposaient à de lourdes sanctions pénales.

M. Jean-Jacques Hyest, président, a mis en avant le coût de la conservation des données.

M. Jean-Pierre Vial s'est étonné que la proposition de décision-cadre encadre strictement la consultation des données passagers alors que, par ailleurs, de nombreuses informations relatives aux vols des avions particuliers sont aisément accessibles sur le site de l'aviation civile. Il a indiqué qu'en matière de renseignement économique, ces informations étaient redoutables.

Au bénéfice de l'ensemble de ces observations, la commission a adopté la proposition de résolution rédigée dans les termes proposés par le rapporteur.

ANNEXES

ANNEXE 1
LISTE DES PERSONNES ENTENDUES

S.G.A.E.

M. Laurent Pic, secrétaire général adjoint

CNIL

M. Georges de La Loyère, commissaire

M. Laurent Lim, chargé de mission au service des affaires juridiques

Police aux frontières

M. Jean-Yves Topin, directeur central

Direction générale des douanes

M. Gérard Schoen, sous-directeur des affaires juridiques et du contentieux,
du contrôle et de la lutte contre la fraude

Mme Laurence Jaclard, chargée des relations avec les institutions

Direction centrale du renseignement intérieur

M. Bernard Squarcini, directeur

M. Michel Pagès, sous-directeur des technologies du renseignement

M. Pascal Rousseu, chef de la division sur l'analyse des données
opérationnelles

Conseil National des Barreaux

Me Nicolas Perrault

Barreau de Paris

Me Vincent Nioré

Conférence des Bâtonniers

M. Alain Guilloux, bâtonnier

Ligue des Droits de l'Homme

M. Jean-Claude Vitran, responsable du groupe de travail « Libertés et
technologies de l'information et de la communication »

M. Jean-Sébastien Marriez

Remarque : la Commission nationale consultative des droits de l'homme a
adressé à votre rapporteur une contribution écrite.

ANNEXE 2
LISTE DES DONNÉES PNR QUI DEVRAIENT ÊTRE TRANSMISES
EN APPLICATION DE LA PROPOSITION DE DÉCISION-CADRE

Données pour tous les passagers

- (1) Code du dossier passager (PNR)
- (2) Date de réservation/d'émission du billet
- (3) Date(s) prévue(s) du voyage
- (4) Nom(s)
- (5) Adresse et contact (numéro de téléphone, adresse électronique)
- (6) Moyens de paiement, y compris l'adresse de facturation
- (7) Itinéraire complet pour le PNR concerné
- (8) Profil de client fidèle
- (9) Agence de voyage/agent de voyage
- (10) Statut du voyageur (confirmations, enregistrement, non-présentation ou passager de dernière minute sans réservation)
- (11) PNR scindé/divisé
- (12) Remarques générales (à l'exclusion de toute information sensible)
- (13) Etablissement des billets (numéro du billet, date d'émission, billets aller simple, champs des billets informatisés)
- (14) Numéro du siège et autres informations concernant le siège
- (15) Passage de codes
- (16) Bagages
- (17) Nombre et autres noms de voyageurs figurant dans le PNR
- (18) Informations API éventuellement collectées
- (19) Historique complet des modifications des PNR énumérées aux points 1 à 18

ANNEXE 3
ARTICLE 2 DE LA DÉCISION-CADRE DU 13 JUIN 2002
RELATIVE AU MANDAT D'ARRÊT EUROPÉEN (2002/584/JAI)

Article 2

Champ d'application du mandat d'arrêt européen

1. Un mandat d'arrêt européen peut être émis pour des faits punis par la loi de l'État membre d'émission d'une peine ou d'une mesure de sûreté privatives de liberté d'un maximum d'au moins douze mois ou, lorsqu'une condamnation à une peine est intervenue ou qu'une mesure de sûreté a été infligée, pour des condamnations prononcées d'une durée d'au moins quatre mois.

2. Les infractions suivantes, si elles sont punies dans l'État membre d'émission d'une peine ou d'une mesure de sûreté privatives de liberté d'un maximum d'au moins trois ans telles qu'elles sont définies par le droit de l'État membre d'émission, donnent lieu à remise sur la base d'un mandat d'arrêt européen, aux conditions de la présente décision-cadre et sans contrôle de la double incrimination du fait :

- participation à une organisation criminelle,
- terrorisme,
- traite des êtres humains,
- exploitation sexuelle des enfants et pédopornographie,
- trafic illicite de stupéfiants et de substances psychotropes,
- trafic illicite d'armes, de munitions et d'explosifs,
- corruption,
- fraude, y compris la fraude portant atteinte aux intérêts financiers des Communautés européennes au sens de la convention du 26 juillet 1995 relative à la protection des intérêts financiers des Communautés européennes,
- blanchiment du produit du crime,
- faux monnayage, y compris la contrefaçon de l'euro,
- cybercriminalité,
- crimes contre l'environnement, y compris le trafic illicite d'espèces animales menacées et le trafic illicite d'espèces et d'essences végétales menacées,
- aide à l'entrée et au séjour irréguliers,
- homicide volontaire, coups et blessures graves,
- trafic illicite d'organes et de tissus humains,
- enlèvement, séquestration et prise d'otage,

- racisme et xénophobie,
- vols organisés ou avec arme,
- trafic illicite de biens culturels, y compris antiquités et œuvres d'art,
- escroquerie,
- racket et extorsion de fonds,
- contrefaçon et piratage de produits,
- falsification de documents administratifs et trafic de faux,
- falsification de moyens de paiement,
- trafic illicite de substances hormonales et autres facteurs de croissance,
- trafic illicite de matières nucléaires et radioactives,
- trafic de véhicules volés,
- viol,
- incendie volontaire,
- crimes relevant de la juridiction de la Cour pénale internationale,
- détournement d'avion/navire,
- sabotage.

3. Le Conseil peut décider à tout moment, statuant à l'unanimité et après consultation du Parlement européen dans les conditions prévues à l'article 39, paragraphe 1, du traité sur l'Union européenne, d'ajouter d'autres catégories d'infractions à la liste contenue au paragraphe 2 du présent article. Le Conseil examine, à la lumière du rapport soumis par la Commission au titre de l'article 34, paragraphe 3, s'il y a lieu d'étendre ou de modifier cette liste.

4. Pour les infractions autres que celles visées au paragraphe 2, la remise peut être subordonnée à la condition que les faits pour lesquels le mandat d'arrêt européen a été émis constituent une infraction au regard du droit de l'État membre d'exécution, quels que soient les éléments constitutifs ou la qualification de celle-ci.

TABLEAU COMPARATIF

Texte de la proposition de résolution	Proposition de la commission
Le Sénat,	<i>(Alinéa sans modification).</i>
Vu l'article 88-4 de la Constitution ;	<i>(Alinéa sans modification).</i>
Vu la proposition de décision-cadre relative à l'utilisation des données des dossiers passagers (Passenger Name Record - PNR) à des fins répressives (E 3697) ;	<i>(Alinéa sans modification).</i>
- prenant acte que cette proposition de décision-cadre tend à promouvoir une approche harmonisée au sein de l'Union européenne de l'utilisation des données des dossiers passagers à des fins répressives et que des discussions sont en cours au sein du Conseil ;	<i>(Alinéa sans modification).</i>
- considère qu'une telle approche doit retenir parmi ses priorités d'assurer un respect effectif des droits fondamentaux, en particulier le droit au respect de la vie privée et à la protection des données à caractère personnel ;	<i>(Alinéa sans modification).</i>
- souligne que les finalités de la proposition doivent être précisément délimitées et concerner exclusivement la prévention, la détection, l'instruction, la poursuite et la répression du terrorisme et d'un ensemble d'infractions graves pour lesquelles l'utilisation de données des dossiers passagers s'avérerait pertinente ;	- souligne... ...graves, définies par référence à la liste d'infractions établie dans la décision-cadre relative au mandat d'arrêt européen, pour...
- estime que seule la méthode de transmission dite « PUSH » peut offrir les garanties nécessaires en permettant aux transporteurs aériens de garder le contrôle de la qualité des données transmises et des conditions de transmission ;	...pertinente ; <i>(Alinéa sans modification).</i>
- juge nécessaire que des précisions et des garanties supplémentaires soient prévues sur la qualité des services qui seront chargés de l'unité de renseignements passagers et celle des autorités compétentes pour recevoir les données PNR et les traiter, ainsi que sur les conditions dans lesquelles des intermédiaires seraient susceptibles d'intervenir dans la collecte et la transmission des données ;	<i>(Alinéa sans modification).</i>
- demande que les autorités indépendantes sur la protection des données soient habilitées à effectuer des contrôles au sein de l'unité de renseignements passagers ;	- estime qu'au sein de ces autorités, seuls des agents individuellement désignés et dûment habilités devraient pouvoir accéder aux données PNR ; <i>(Alinéa sans modification).</i>
	- demande que la rubrique « 12) Remarques générales », qui est la seule où des données sensibles peuvent figurer, soit exclue de la liste des données PNR transmises ;

Texte de la proposition de résolution

- considère que la liste des données devant être transmises devrait faire l'objet d'un examen supplémentaire afin que l'utilité de leur collecte soit avérée au regard des finalités poursuivies ;

- demande que l'utilisation de données sensibles révélant la race ou l'origine ethnique, les convictions religieuses, les opinions politiques, l'appartenance à un syndicat, la santé ou l'orientation sexuelle d'une personne soit en principe exclue, que leur filtrage soit assuré directement par les transporteurs aériens et que, si leur conservation était envisagée aux seules fins de leur possible utilisation dans le cadre d'une enquête criminelle, des garanties spécifiques soient prévues ;

- juge manifestement disproportionnée la durée totale de treize ans prévue par la proposition pour la conservation des données et demande, en conséquence, que cette durée soit réduite à un délai raisonnable ;

- estime que le régime de protection des données applicable doit être clarifié, en privilégiant un haut niveau de protection par référence aux standards du Conseil de l'Europe ;

- demande que des garanties supplémentaires soient prévues dans le texte même de la proposition sur les droits des personnes concernées, en particulier pour l'exercice du droit à l'information, du droit d'accès, de rectification et d'effacement des données et que le responsable du traitement chargé de donner suite à leurs demandes soit précisément identifié ;

- considère que les conditions dans lesquelles les données seraient susceptibles d'être transmises à des États tiers n'offrent pas les garanties suffisantes ; demande, en conséquence, qu'un tel transfert ne soit possible qu'au cas par cas et sous réserve que l'État tiers assure un niveau de protection adéquat des données et que des garanties soient prévues dans la mise en oeuvre du principe de réciprocité.

Proposition de la commission

Alinéa supprimé.

Alinéa supprimé.

- juge...

...données ;

- propose une durée de conservation de trois ans, à laquelle pourrait succéder une durée de conservation de trois ans des seules données PNR ayant montré un intérêt particulier au cours de la première période ;

(Alinéa sans modification).

(Alinéa sans modification).

(Alinéa sans modification).

- considère que la transposition de la proposition de décision-cadre devra être réalisée par la loi compte tenu des enjeux pour assurer un respect effectif des droits fondamentaux.