N° 3961

# ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

TREIZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 16 novembre 2011.

# RAPPORT D'INFORMATION

DÉPOSÉ

PAR LA COMMISSION DES AFFAIRES EUROPÉENNES[1]

*sur* **la proposition de directive relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière,**

ET PRÉSENTÉ

PAR M. Guy GEOFFROY,

Député

[1] *La composition de cette Commission figure au verso de la présente page.*

*La Commission des affaires européennes est composée de :* M. Pierre Lequiller, *président* ; MM. Michel Herbillon, Jérôme Lambert, Didier Quentin, Gérard Voisin *vice-présidents* ; M. Jacques Desallangre, M^me^ Marietta Karamanli, MM. Francis Vercamer *secrétaires ;* M. Alfred Almont, M^me^ Monique Boulestin, MM. Pierre Bourguignon, Yves Bur, Patrice Calméjane, Christophe Caresche, Philippe Cochet, Jean-Yves Cousin, Bernard Deflesselles, Lucien Degauchy, Michel Diefenbacher, Jean Dionis du Séjour, Marc Dolez, Daniel Fasquelle, Pierre Forgues, M^me^ Marie-Louise Fort, MM. Jean-Claude Fruteau, Jean Gaubert, Hervé Gaymard, Guy Geoffroy, M^mes^ Annick Girardin, Anne Grommerch, Pascale Gruny, Elisabeth Guigou, Danièle Hoffman-Rispal, MM. Régis Juanico, Robert Lecou, Michel Lefait, Lionnel Luca, Philippe Armand Martin, Jean-Claude Mignon, Pierre-Alain Muet, Jacques Myard, Michel Piron, M^mes^ Chantal Robin-Rodrigo, Valérie Rosso-Debord, Odile Saugues, MM. André Schneider, Philippe Tourtelier.

## SOMMAIRE

—

Pages

**RÉSUMÉ DU RAPPORT**

Les premiers systèmes d'exploitation de grande ampleur des données des dossiers passagers (Passenger Name Record, dites PNR), qui sont celles recueillies et par les transporteurs au stade de la réservation commerciale, ont vu le jour à la suite des attentats du 11 septembre 2001. Ainsi les Etats-Unis ont-ils exigé de disposer des données relatives aux passagers décollant ou atterrissant sur leur territoire. La négociation d'accords PNR avec les Etats-Unis a été et demeure complexe car, si l'Union européenne et les Etats-Unis s'accordent sur le grand intérêt de ces données dans la lutte contre le terrorisme et la criminalité grave, des divergences importantes existent sur la protection à garantir s'agissant de données personnelles.

Le rapporteur estime que les données PNR ont fait la preuve de leur efficacité dans la lutte contre le terrorisme et contre la criminalité grave, notamment parce qu'elles sont disponibles en amont des déplacements et parce qu'elles permettent de dégager des critères tendant à permettre de définir le niveau de risque représenté par un passager. Elles sont également utilisées dans le cadre d'enquêtes et de poursuites pénales. Au sein de l'Union, le Royaume-Uni a mis en oeuvre le système de collecte et d'exploitation le plus abouti. Mais plusieurs autres Etats membres utilisent d'ores et déjà les données PNR s'agissant du trafic aérien et un certain nombre d'Etats se sont dotés d'un cadre juridique permettant leur exploitation.

Ainsi, à moyen terme, de nombreux systèmes de collecte et de traitement risquent de cohabiter dans l'Union, sans harmonisation, ce qui serait coûteux, peu efficace et peu satisfaisant en matière de protection des données.

Le programme de Stockholm « *une Europe ouverte et sûre qui protège les citoyens* », adopté le 2 décembre 2009, qui pose les priorités de l'action de l'Union dans l'espace de liberté, de sécurité et de justice, demande à la Commission européenne de présenter une proposition concernant l'utilisation des données PNR aux fins de la

prévention et de la détection des infractions terroristes et des infractions graves, ainsi que des enquêtes et des poursuites en la matière.

Après la présentation d'une première proposition de décision-cadre pour la mise en oeuvre d'un système PNR européen le 6 novembre 2007, sur laquelle les négociations n'avaient pas abouti, la Commission européenne a donc présenté le 2 février 2011 une nouvelle proposition de directive, dans le cadre institutionnel découlant du traité de Lisbonne.

Le présent rapport examine la proposition de directive, qui a été nettement améliorée par rapport à la proposition de décision-cadre de 2007. Ainsi, qu'il s'agisse de la durée de conservation, du transfert des données vers des Etats tiers ou de l'interdiction de l'utilisation des données sensibles, points sur lesquels l'Assemblée nationale avait émis des réserves dès 2009, les progrès doivent être soulignés.

Toutefois, dans la recherche d'un juste équilibre entre la lutte contre le terrorisme et la criminalité grave et la préservation des droits fondamentaux, il conviendra de veiller à ne pas adopter de règles si strictes qu'elles pourraient considérablement réduire l'intérêt même du dispositif.

Le rapport s'attachera également à demander la reprise de certains éléments du projet, encore inaboutis.

Mesdames, Messieurs,

Le présent rapport étudie la proposition de directive tendant à permettre le traitement des données des dossiers passagers (*passenger name record* ou PNR) à des fins répressives. Les données PNR sont les données collectées par les transporteurs internationaux au stade de la réservation commerciale.

Ce projet européen tend à encadrer la collecte et le traitement des données PNR par les autorités publiques nationales à des fins de lutte contre le terrorisme et les formes graves de criminalité. Il fait suite aux discussions engagées en 2007 sur la proposition de décision-cadre relative à l'utilisation des données PNR[(2)] qui n'avait pas pu être adoptée avant l'entrée en vigueur du traité de Lisbonne. Cette proposition avait fait l'objet d'un rapport présenté le 11 février 2009 par le rapporteur devant la commission des affaires européennes. La proposition de résolution adoptée par la commission des affaires européennes avait ensuite été confirmée par la commission des lois puis est devenue définitive le 18 octobre 2009[(3)].

Les données PNR ont plusieurs utilités : collectées en amont du décollage, elles peuvent permettre d'établir des critères d'évaluation du risque que représente un passager ; traitées en temps réel, les données PNR peuvent permettre de prévenir une infraction ou d'arrêter des personnes ayant commis ou commettant une infraction ; enfin, ces données peuvent être utilisées dans le cadre d'enquêtes et de poursuites et ont déjà fait leurs preuves dans le cadre de plusieurs démantèlements de réseaux de trafiquants.

---

[(2)] *Proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record -PNR) à des fins répressives du 6 novembre 2007, COM(2007) 654 final.*

[(3)] *Rapport d'information n° 1447 présenté par M. Guy Geoffroy le 11 février 2009 au nom de la commission chargée des affaires européennes* sur la proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record, PNR) à des fins répressives (COM [2007] 654 final/n° E 3697) *puis rapport n° 1948 du 30 septembre 2009 fait au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République* sur la proposition de résolution de M. Guy Geoffroy, rapporteur de la commission chargée des affaires européennes, sur la proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passager Name record, PNR) à des fins répressives (COM [2007] 654 final/n° E 3697), *par M. Guy Geoffroy. Résolution adoptée n° 352 du 18 octobre 2009 sur la proposition de décision cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name record, PNR) à des fins répressives.*

La collecte et le traitement des données concerneraient l'ensemble des passagers de vols en provenance ou à destination de pays tiers, chaque Etat membre de l'Union étant destinataire des données relatives aux vols au départ ou à l'arrivée sur son territoire.

La masse des données en cause ainsi que le fait qu'elles concernent la plupart du temps des personnes qui ne sont suspectées de rien et n'ont rien à se reprocher nécessitent que le projet soit précisément justifié et proportionné. Les impératifs de lutte contre la criminalité grave et le terrorisme ne sont pas seuls en jeu et un équilibre doit être trouvé avec le respect dû à la vie privée et la protection des données personnelles.

La question des données sensibles, de la durée de conservation ou du partage des données avec des Etats tiers retiendront notamment toute l'attention du rapporteur.

Une telle mesure serait nécessairement coûteuse mais il n'est malheureusement pas possible de fournir une estimation précise.

Dès ses travaux menés en 2007, le rapporteur a été convaincu de la grande utilité des données PNR et des potentialités uniques de cet instrument ainsi que de la nécessité d'avancer unis au sein de l'Union sur ces questions. En effet, jusqu'ici, l'Union s'est principalement positionnée en réaction aux exigences des Etats tiers avec lesquels des accords PNR ont été négociés. Les données PNR des passagers européens et étrangers sont non seulement utilisées dans plusieurs Etats tiers (Etats-Unis, Canada et Australie), mais aussi par plusieurs Etats membres, dans le cadre de leurs législations nationales respectives.

Il est désormais temps que l'Union fixe un cadre dans lequel les données pourraient être traitées en son sein, parce qu'elles sont nécessaires à la lutte contre la criminalité grave et le terrorisme, parce qu'un cadre harmonisé devrait être défini avant que vingt-sept systèmes nationaux différents ne soient mis en place et parce qu'une Union dotée d'une doctrine établie en la matière pourrait peser de tout son poids face aux demandes parfois excessives des Etats tiers.

## I. DES DONNÉES DÉJÀ UTILISÉES A DES FINS REPRESSIVES EN APPLICATION DE LÉGISLATIONS NATIONALES

Deux types de données collectées par les transporteurs aériens doivent en premier lieu être distingués : les données PNR et les données API.

Les données des dossiers passagers dites « PNR » (*Passenger Name Record*) sont celles collectées par les compagnies aériennes auprès de leurs passagers au stade de la réservation commerciale. Les informations sont nombreuses et concernent notamment l'identification du passager (nom, prénom, adresse, coordonnées), les dates de son voyage, l'agence de voyage utilisée, son itinéraire complet, sa place dans l'avion, ses bagages (poids), le contact dans le pays d'arrivée, le tarif accordé, le moyen de paiement, le nombre et le nom des personnes l'accompagnant. Une rubrique « remarques générales » permet de noter des demandes particulières du passager relatives aux repas ou en relation avec son état de santé.

Les données dites « API » (*Advance passenger information system*) sont les données biographiques (nom, prénom, date de naissance, sexe, nationalité) et les informations relatives au document de voyage utilisé (carte nationale d'identité, passeport, visa) recueillies lors de l'enregistrement à partir du document de voyage.

Les données API et les données PNR sont donc différentes. Les données API recueillies lors de l'enregistrement sont officielles et vérifiées par le personnel des transporteurs alors que les données PNR, recueillies en amont au stade de la réservation commerciale, ont un caractère aléatoire. Même lorsque les données de PNR sont transférées à la clôture de l'enregistrement (une fois les dernières modifications de réservation opérées), elles ne constituent pas une base fiable à 100 %.

En France, le contrôle des déplacements des passagers du transport aérien génère trois types de collecte : les données figurant sur les documents d'identité alimentent le fichier national transfrontière, les données collectées lors de l'enregistrement (données API) sont destinées au fichier des passagers aériens et, enfin, le cadre juridique permettant la collecte des données PNR a été créé en 2006.

**A. En France : le fichier national transfrontière et le fichier des passagers aériens**

*1. Le fichier national transfrontière (FNT)*

Le fichier national transfrontière a été créé par arrêté du ministre de l'intérieur en date du 29 août 1991 mais est resté quasi inutilisé car il était alimenté et exploité manuellement à partir des données figurant sur les cartes d'embarquement et de débarquement lors des contrôles frontaliers.

L'article 7 de la loi du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers (loi n° 2006-64) a prévu d'automatiser son alimentation par les données figurant sur les bandes à lecture optique (bandes MRZ) des documents de voyage (carte nationale d'identité, visa ou passeport) et les données figurant sur les cartes d'embarquement et de débarquement.

Les données de la bande MRZ des documents d'identité sont les suivantes :

**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. Etat émetteur |
| | | 11. nombre d'entrées |
| | | 12. durée du séjour |
| | | 13. début de validité |

L'utilisation du fichier national transfrontière est ciblée. Seuls les vols à destination ou en provenance d'un nombre limité de pays ont été concernés par l'automatisation du fichier.

Les données sont conservées pendant une durée de trois ans et il n'y a pas d'interconnexion avec le fichier des personnes recherchées ou le système d'information Schengen (SIS) (ces bases de données étant de toute façon interrogées lors des contrôles frontaliers pour les ressortissants de pays tiers).

*2. Le fichier des passagers aériens (FPA)*

La directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers a imposé aux Etats de mettre en oeuvre un régime de transfert des données API des compagnies aériennes vers les autorités répressives sur demande de ces dernières. Elle vise principalement à lutter contre l'immigration clandestine et à améliorer les contrôles aux frontières (article premier). Néanmoins, l'article 6 de la directive dispose que les Etats membres peuvent utiliser les données à des fins répressives.

Les données sont transférées sur demande des Etats.

La France a prévu de pouvoir étendre cette obligation aux transports ferroviaire et maritime et a élargi la finalité de cette transmission, outre les contrôles aux frontières et la lutte contre l'immigration clandestine (I de l'article 7 de la loi du 23 janvier 2006), à la lutte contre le terrorisme (II de l'article 7).

Le fichier des passagers aériens, qui regroupe les données API, a été créé par l'article 7 de la loi du 23 janvier 2006. Les vols intra européens ne sont pas concernés. Le traitement des données est soumis aux dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Lorsque les données sont traitées aux fins de prévenir et de réprimer des actes de terrorisme (II de l'article 7), l'accès aux traitements est limité aux agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales spécialement chargés de ces missions, et des services de police et de gendarmerie nationales ainsi que des douanes chargés de la sûreté des transports internationaux. Il est possible de réaliser un croisement avec le fichier des personnes recherchées et le système d'information Schengen (III de l'article 7).

Pour une entreprise de transport, le fait de méconnaître ses obligations est puni d'une amende d'un montant maximum de 50 000 euros pour chaque voyage.

Ce fichier peut théoriquement concerner l'ensemble des destinations mais se concentrait à l'origine sur cinq pays. 31 destinations sont aujourd'hui surveillées.

Si la mention « connu » ressort du croisement avec le fichier des personnes recherchées ou le système d'information Schengen, les services intéressés en sont avertis.

Ce résultat n'est conservé que 24 heures (conformément à la demande de la CNIL dans sa délibération 2006-198) et le reste des données l'est pendant cinq années (article 4 de l'arrêté du 19 décembre 2006 pris pour l'application de l'article 7 de la loi n° 2006-64 du 23 janvier 2006). Dans le cadre de la lutte contre l'immigration clandestine, ces données ne peuvent être consultées que dans les 24 heures qui suivent leur transmission.

A l'heure actuelle, les résultats liés à l'exploitation apparaissent modestes, notamment du fait d'un taux de fausses concordances assez élevé (la saisie des noms est une source d'erreurs importante), du caractère limité des données API, ce qui démontre *a contrario* tout l'intérêt des données PNR, du fait que le croisement avec le FPR ne permet pas un ciblage des personnes réellement dangereuses et du fait que les sanctions prévues à l'encontre des compagnies aériennes ne sont pas systématiquement mises en œuvre.

Le FPA doit être prochainement profondément rénové, d'une manière qui permette de le rendre plus efficace et modulable avec les données PNR.

*2. Le cadre juridique établi en France pour permettre la collecte des données PNR*

Les données API fournissent trop peu de résultats. La direction générale de la police nationale et la direction centrale du renseignement intérieur, entendues par le rapporteur, jugent que l'exploitation des données PNR constituera un saut majeur dans la lutte contre le terrorisme et la grande criminalité.

La France n'a pas mis en œuvre de régime de collecte des données des dossiers passagers. Les négociations européennes engagées depuis 2007 ont reporté la mise en œuvre concrète du dispositif législatif existant depuis 2006.

L'article 7 de la loi du 23 janvier 2006 précitée a en effet prévu que les données PNR puissent être collectées et traitées afin d'améliorer le contrôle aux frontières, de lutter contre l'immigration clandestine et de lutter contre le terrorisme selon les modalités suivantes :

– « *afin d'améliorer le contrôle aux frontières et de lutter contre l'immigration clandestine, le ministre de l'intérieur est autorisé à procéder à la mise en oeuvre de traitements automatisés de 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, à l'exclusion des données relevant du I de l'article 8 de la loi n° 78-17du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés* » (I de l'article 7 de la loi du 23 janvier 2006) ;

– les données PNR sont celles « *relatives aux passagers et enregistrées dans les systèmes de réservation* […] *lorsqu'elles sont détenues par les transporteurs aériens, maritimes ou ferroviaires* » ;

– les traitements mentionnés au premier alinéa sont soumis aux dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

– lorsque les données sont traitées aux fins de prévenir et de réprimer des actes de terrorisme (II de l'article 7), l'accès aux traitements « *est alors limité aux agents individuellement désignés et dûment habilités : des services de police et de gendarmerie nationales spécialement chargés de ces missions ; des services de police et de gendarmerie nationales ainsi que des douanes, chargés de la sûreté des transports internationaux* » ;

– le traitement peut faire l'objet d'une interconnexion avec le fichier des personnes recherchées et le système d'information Schengen (III de l'article 7) ;

– pour une entreprise de transport, le fait de méconnaître ses obligations est puni d'une amende d'un montant maximum de 50 000 euros pour chaque voyage.

Le préfet Marc Cabane a récemment été chargé de définir une plateforme permettant de collecter et de traiter les données PNR.

Les douanes françaises, s'appuyant sur l'article 65 du code des douanes, peuvent demander aux compagnies aériennes leur transmettre des données PNR. N'utilisant cette faculté qu'avec certaines compagnies aériennes et bien que l'utilisation demeure ciblée, l'intérêt de l'outil est clairement démontré. Ainsi, à l'aéroport de Roissy Charles De Gaulle, 80 % des saisies de cocaïne ont été réalisées grâce à l'utilisation des données PNR par la cellule de ciblage de Roissy. Le taux de réussite des constatations obtenues grâce à un ciblage par les données PNR est 7 fois supérieur à celui obtenu par les autres méthodes d'analyse. L'expérience montre que le nombre de contrôles est réduit mais que la qualité des contrôles est bien supérieure. Toutefois, M. Gérard Schoen, sous-directeur des affaires juridiques, du contentieux, du contrôle et de la lutte contre la fraude à la direction générale des douanes, entendu par le rapporteur, a estimé que le ciblage serait efficace si les agents ayant la charge du ciblage sont également confrontés aux réalités de ce contrôle.

L'examen des systèmes existants dans plusieurs Etats membres, seul le Royaume-Uni ayant mis en œuvre un fichier de données PNR, permet de donner une idée des avantages attendus d'un PNR européen.

### B. L'intérêt des données PNR d'après les expériences menées dans les autres Etats membres

Le Royaume-Uni a mis en oeuvre dès 2004 un projet pilote dit « Sémaphore » qui visait à mettre en place un système intégré de gestion des contrôles aux frontières grâce notamment à l'utilisation des données API et PNR. Le programme e-borders, prenant le relais du projet pilote, vise le transport aérien, maritime et ferroviaire. Les données des passagers sont recueillies et analysées avant le voyage (données PNR) puis, à la frontière, les données biométriques des passeports et des visas sont également exploitées et, enfin, un régime de facilitation des contrôles pour les passagers volontaires, reposant sur l'utilisation de la biométrie, a été créé.

Le programme ayant connu une montée en charge progressive, l'objectif est que le système soit totalement achevé pour 2014. Il convient de noter que les finalités du programme e-borders visent, outre le contrôle aux frontières, la lutte antiterroriste et le crime organisé, la lutte contre l'immigration illégale et la fraude fiscale. Les données API sont recueillies et traitées pour tous les modes de transport et tous les trajets mais les données PNR ne sont recueillies que pour certaines destinations, précisément ciblées.

75 % des flux de données concernent le transport aérien. Les données sont conservées pendant dix ans, dont cinq années sur une base active puis cinq années avec une possibilité d'accès au cas par cas. Selon les informations transmises au rapporteur, le budget du programme depuis sa mise en place pourrait atteindre 1,2 milliard de livres. Ce montant très élevé est lié au caractère extensif du programme (finalités larges, tous modes de transport, déplacements internationaux, européens et nationaux) ainsi qu'aux difficultés rencontrées lors de la mise en œuvre initiale. Un certain nombre de surcoûts liés au caractère novateur du programme ont été enregistrés.

Selon les dernières informations transmises au rapporteur, 330 millions de mouvements de passagers ont été analysés dans le cadre du e-borders (analyse des données API et PNR) et il a été procédé à 89 000 arrestations. La part des données PNR collectées est minoritaire dans ce système, avec quatorze millions de données collectées chaque année. Toutefois, leur usage est jugé très positif par les autorités, avec une très nette amélioration des contrôles positifs grâce au ciblage sur la base de critères prédéfinis par rapport à une exploitation manuelle. Plusieurs exemples d'arrestations de terroristes et de trafiquants d'êtres humains grâce aux données PNR ont été fournis par les autorités britanniques.

Le troisième rapport de la Chambre des Communes britannique relatif au programme e-borders, publié le 15 décembre 2009, fait état de doutes sur la possibilité d'appliquer le programme e-borders aux déplacements intra européens (s'agissant notamment de l'exigence de fournir des données en avance comme condition du voyage). Le rapport émet des réserves sur le fait de savoir si les possibles obstacles à la liberté de circulation au sein de l'Union peuvent être considérés comme étant justifiés par les finalités du programme, au regard du droit européen.

D'autres Etats membres utilisent les données PNR dans un cadre significativement moins large que celui du Royaume-Uni.

Les autorités de police judiciaire belges peuvent, dans le cadre d'une autorisation judiciaire donnée par le parquet, demander aux compagnies aériennes d'obtenir un accès à leurs données PNR. L'usage des données PNR peut être proactif ou réactif.

En Suède, les données PNR sont notamment utilisées dans le domaine du renseignement et de la lutte contre le terrorisme. Les douanes utilisent également les données PNR.

Le Danemark dispose d'un cadre juridique pour l'exploitation des données PNR.

La Commission européenne indique dans sa proposition de directive que l'expérience acquise dans les Etats membres utilisant les données PNR démontre une progression sensible des résultats dans la lutte contre la drogue, la traite des êtres humains et le terrorisme. Les données PNR traitées permettent de mieux comprendre la composition et le fonctionnement des réseaux criminels et terroristes. La Belgique a ainsi signalé que 95 % de l'ensemble des saisies de drogue effectuées en 2009 résultaient exclusivement ou essentiellement du traitement de données PNR. La Suède a déclaré que 65 à 75 % de l'ensemble des saisies de drogue effectuée en 2009 sur son territoire résultaient exclusivement ou essentiellement du traitement des données PNR. Le Royaume-Uni a indiqué qu'au cours d'un semestre en 2010, 212 kilos de cocaïne et 20 kilos d'héroïne avaient été saisis exclusivement ou essentiellement grâce au traitement des données PNR.

Dans sa communication intitulée « *présentation générale de la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice* » (COM (2010) 385 final) du 20 juillet 2010, la Commission européenne a fourni d'autres exemples dans lesquels l'utilisation des données PNR avait permis de lutter efficacement contre la criminalité grave transfrontalière. L'encadré suivant reproduit les exemples fournis en page 50 de la communication.

**Données relatives aux passagers aériens (PNR)**

**Exemples d'analyse PNR permettant de collecter des informations dans le cadre d'enquêtes sur des formes graves de criminalité transfrontalière**

**Traite des enfants**

L'analyse PNR a révélé que trois enfants non accompagnés voyageaient d'un Etat membre de l'UE vers un pays tiers, sans que l'on sache qui allait les accueillir à leur arrivée. Alertées par la police de l'Etat membre après le départ, les autorités du pays tiers ont arrêté la personne qui était venue chercher les enfants, qui s'est révélée être un délinquant sexuel enregistré dans l'Etat membre.

**Traite des êtres humains**

L'analyse PNR a permis de démasquer un groupe de trafiquants d'êtres humains qui empruntaient toujours le même itinéraire. Ceux-ci utilisaient des documents falsifiés pour procéder aux formalités d'enregistrement sur un vol intra-UE et utilisaient des documents authentiques pour procéder, simultanément, aux formalités d'enregistrement sur un autre vol à destination d'un pays tiers. Une fois dans la salle d'attente de l'aéroport, ils embarquaient sur le vol intra-UE.

**Fraude à la carte de crédit**

Plusieurs familles voyageaient à destination d'un Etat membre avec des billets achetés à l'aide de cartes de crédit volées. L'enquête a démontré qu'un groupement criminel utilisait ces cartes pour acheter les billets qu'il revendait ensuite librement, dans des centres de téléphonie longue distance. Ce sont les données PNR qui ont permis de faire le rapprochement entre les voyageurs, d'une part, et les cartes de crédit et les vendeurs, d'autre part.

**Trafic de drogue**

Les services de police d'un Etat membre disposaient d'informations suggérant qu'un homme était impliqué dans un trafic de drogue au départ d'un pays tiers, mais les gardes-frontières n'ont jamais rien trouvé sur lui à son arrivée dans l'UE. L'analyse PNR a révélé qu'il voyageait toujours avec un associé. La fouille de cet associé a permis de trouver d'importantes quantités de drogue.

En conclusion, le Royaume-Uni dispose du système PNR le plus abouti et plusieurs autres pays ont, soit adopté une législation relative à l'utilisation des données, soit les utilisent à titre expérimental. Il apparaît donc qu'à brève échéance, des règles divergentes seront amenées à s'appliquer aux données PNR, à la fois au regard des exigences posées à l'encontre des compagnies aériennes comme en matière de protection des données et de sécurité des transferts de données. Le rapporteur souligne les risques qui s'attachent à cette évolution car la coexistence de systèmes différents sera beaucoup plus coûteuse, probablement moins protectrice et beaucoup moins efficace que la mise en oeuvre d'un système européen harmonisé.

## II. UNE PROPOSITION DE DIRECTIVE PLUS ÉQUILIBRÉE

### A. La résolution européenne de l'Assemblée nationale du 18 octobre 2009

La Commission européenne avait, le 6 novembre 2007, déposé une proposition de décision-cadre qui, bien que fermement soutenue par le rapporteur dans son principe, soulevait un certain nombre de difficultés, telles que la durée de conservation ou le régime de protection des données. Des négociations menées notamment sous l'impulsion de la présidence française de l'Union avaient permis de remanier le texte en profondeur en vue d'aboutir à un équilibre. Toutefois, aucun accord n'ayant pu être trouvé avant l'entrée en vigueur du traité de Lisbonne, la proposition est devenue caduque et un nouveau projet de directive a été déposé, qui sera cette fois discuté dans le cadre de la procédure de codécision. La proposition est fondée sur l'article 82, paragraphe 1, point d), et l'article 87, paragraphe 2, point a) du traité sur le fonctionnement de l'Union européenne.

La résolution adoptée par la commission des affaires européennes puis confirmée par la commission des lois, devenue définitive le 18 octobre 2009, demeure pertinente. Elle est reproduite dans l'encadré suivant.

**Article unique**

L'Assemblée nationale,

Vu l'article 88-4 de la Constitution,

Vu la proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (*Passenger Name Record*, *PNR*) à des fins répressives (COM [2007] 654 final/n° E 3697),

1. Juge que les données PNR constituent un outil nécessaire à la lutte contre le terrorisme et les formes graves de criminalité et que l'institution d'un régime de transfert et de collecte harmonisé au niveau européen permettrait de renforcer l'efficacité des mesures prises au plan national par les Etats membres ;

2. Estime que certaines questions ne sont pas résolues et souhaite, dans le cadre des débats menés en 2009 ;

– que le plein respect des droits fondamentaux et, notamment, du droit à la vie privée et du droit à la protection des données soit assuré à chaque étape de la collecte et du traitement des données ;

– que la durée de conservation soit ramenée à un délai raisonnable compris entre trois et six années ;

– que la question des données sensibles fasse l'objet de protections spécifiques et cohérentes, quelle que soit l'option qui sera retenue entre l'exclusion de toute utilisation ou la possible utilisation à des fins d'enquêtes ou de poursuites en cours ;

– qu'un encadrement plus strict soit obtenu s'agissant des transferts de données vers des Etats tiers, de sorte qu'un Etat membre ne puisse être source de fuite de masses de données brutes vers un Etat tiers ;

– que les problèmes soulevés par les futures demandes d'accès aux données PNR à titre de réciprocité soient étudiés.

### B. Un nouveau texte plus protecteur que la proposition de décision-cadre de 2007

La proposition de directive, présentée le 2 février 2011 par la Commission européenne vise à assurer un équilibre entre les impératifs de sécurité publique et le respect des libertés publiques.

La charte des droits fondamentaux de l'Union définit notamment le droit au respect de la vie privée (article 7), le droit à la protection des données à caractère personnel (article 8) ainsi que le droit à la non discrimination (article 21). La convention de sauvegarde des droits de l'homme et des libertés fondamentales définit, quant à elle, ces droits en ses articles 8 et 14. Le traité sur le fonctionnement de l'Union européenne définit en son article 16 le droit à la protection des données à caractère personnel.

Il convient de rappeler que les données PNR peuvent être utilisées de manière proactive pour analyser et définir des critères d'évaluation qui sont ensuite appliqués pour évaluer le risque que représentent certains passagers avant leur arrivée et avant leur départ. Les données PNR peuvent également être utilisées en temps réel dans le but de prévenir une infraction, de surveiller ou d'arrêter des personnes avant qu'une infraction ne soit commise, les données PNR permettant d'identifier, sur la base des critères d'évaluation préétablis, des suspects qui étaient jusqu'alors inconnus ainsi que la confrontation avec des bases de données relatives aux personnes et aux objets recherchés. Enfin, les données PNR ont également fait la preuve de leur efficacité en mode réactif, dans le cadre d'enquêtes et de poursuites et dans le démantèlement de réseaux criminels après qu'une infraction a été commise.

Le rapporteur souligne le caractère pour le moins paradoxal de la situation actuelle dans laquelle des informations sur des passagers embarquant dans l'Union sont transmises aux autorités australiennes, canadiennes et américaines, sans que l'Union ne bénéficie de ces informations autrement que par le biais de la coopération instituée avec les autorités de ces Etats tiers. Ainsi, les données PNR des voyageurs européens font d'ores et déjà l'objet d'une collecte et d'un traitement lorsqu'ils se rendent dans ces Etats, lequel n'est pas toujours, loin

s'en faut, en conformité avec les standards européens de protection de la vie privée et des données personnelles. Il convient à cet égard de rappeler l'exemple de l'accord passé avec les Etats-Unis en 2007 qui pose des problèmes sérieux au regard de la réglementation européenne et qui est en cours de renégociation. S'agissant du premier projet de nouvel accord et de son caractère insatisfaisant, l'on peut se reporter à la communication du rapporteur devant la commission des affaires européennes du 13 juillet 2011[(4)].

La mise en œuvre d'un système PNR européen serait certainement coûteuse. Il n'a cependant pas été possible d'obtenir une évaluation chiffrée tout à fait fiable. La Commission européenne, dans le document de travail résumant l'analyse d'impact qui accompagnait la proposition de directive, estimait, selon les calculs effectués en 2007, le coût de mise en place à près de 615 millions d'euros pour les pouvoirs publics dans l'Union, ainsi que le coût pour les transporteurs de l'Union à 11,6 millions d'euros. Une nouvelle étude commandée par la Commission européenne fait état de coûts moindres. S'agissant des pouvoirs publics, le coût de mise en place atteindrait 221 millions d'euros et, pour les transporteurs, le coût total serait de 20 millions d'euros. La Commission européenne note que le surcoût, pour les transporteurs, dans les calculs de 2009, serait inférieur à 0,10 euro par billet, soit un montant négligeable par rapport au prix global d'un billet. À ces coûts de mise en oeuvre s'ajouteraient également les coûts de maintenance et de personnel récurrents.

*1. Le champ d'application de la directive*

Les finalités de la directive seraient la prévention et la détection des infractions terroristes et des infractions graves ainsi que les enquêtes et les poursuites en la matière.

Les infractions terroristes seraient celles visées aux articles un à quatre de la décision-cadre 2002/475/JAI du Conseil. Les infractions graves seraient celles visées par la décision-cadre 2002/584/JAI du Conseil relative au mandat d'arrêt européen, si elles sont passibles, dans le droit interne de l'Etat membre, d'une peine privative de liberté ou d'une mesure de sûreté d'une durée maximale d'au moins trois ans. De façon un peu floue, la proposition prévoyait également que les Etats membres pouvaient exclure les infractions mineures pour lesquelles, compte tenu de leurs systèmes respectifs de justice pénale, le traitement des données PNR conformément à la directive serait contraire au principe de proportionnalité. Cette rédaction a été abandonnée au profit d'une restriction de la liste des infractions visées pour le mandat d'arrêt européen et d'une énumération des infractions. Ainsi, différentes options sont en cours de discussion, éliminant

*(4) Dans l'attente de la sortie du prochain rapport d'information de M. Pierre Lequiller déposé par la commission des affaires européennes sur des textes soumis à l'Assemblée nationale en application de l'article 88-4 de la Constitution, il convient de se reporter au compte-rendu de la réunion de la commission des affaires européennes du 13 juillet 2011.*

notamment la corruption, la fraude, la cybercriminalité, le racisme et la xénophobie, le vol à main armée, le racket et l'extorsion ou encore le trafic de véhicules volés. La rédaction de la limitation des infractions graves visées, afin de garantir la proportionnalité du texte, n'est à ce jour pas suffisamment avancée. Il conviendra toutefois de veiller à maintenir le caractère opérationnel de l'instrument.

La proposition initiale prévoyait de ne viser que les vols internationaux à destination ou en provenance des Etats membres. Les vols intra-européens n'étaient pas concernés, pour des motifs de proportionnalité. À cet égard, les personnes auditionnées par le rapporteur ont rappelé à quel point une telle exclusion affaiblirait le dispositif dans son ensemble et priverait les services répressifs d'informations centrales. La rupture de voyage est en effet une technique très employée pour perdre les contrôleurs et les trafics élaborés utilisent les vols intra-communautaires. C'est pourquoi cette question doit être réévaluée, notamment à la lumière des exemples fournis par la pratique dans les Etats membres qui utilisent les données PNR. Il convient également de rappeler que les attentats du 11 septembre 2001 ont été commis sur des vols intérieurs aux Etats-Unis. Le dernier état du texte en discussion propose de permettre, lorsque cela est nécessaire, d'appliquer la collecte des données PNR à certains vols européens sélectionnés. L'Etat membre souhaitant appliquer la directive aux vols intra-européens qu'il a sélectionnés devrait, au préalable, en aviser la Commission européenne. Dans son rapport de 2009, le rapporteur exposait la proposition de décision-cadre résultant des travaux menés sous présidence française. Il était prévu que les éventuels segments intra-communautaires des vols internationaux seraient compris dans le champ d'application de la décision-cadre, la faculté de requérir les données PNR sur les vols intra-communautaires étant laissée ouverte aux Etats membres, en application de la législation nationale. Une incertitude pesait néanmoins sur la faisabilité technique et sur le caractère opérationnel de cette option.

En conclusion, le rapporteur est favorable au fait d'inclure les vols intra-européens dans le champ d'application de la directive.

Un enjeu important résidera également dans le fait que le texte limite ou non l'utilisation des données PNR dans les Etats membres aux seules fins définies par la directive, auquel cas le Royaume-Uni, qui utilise les données PNR à des fins douanières ou d'immigration, mais aussi la France, qui a prévu d'utiliser les données PNR à des fins de lutte contre l'immigration illégale en 2006, pourraient émettre des réserves importantes. Le rapporteur estime, comme en 2009, que le fait de laisser une marge de manoeuvre aux Etats membres ne remet pas en cause l'intérêt de la directive en termes d'harmonisation.

*2. Le sort des données collectées : une attention davantage portée vers le respect des droits fondamentaux*

**a) Le rôle central des unités de renseignements passagers : la collecte et l'analyse des données transmises**

Chaque Etat membre devrait mettre en place une autorité compétente pour la collecte des données, leur stockage, leur analyse et la transmission du résultat des analyses aux autorités compétentes : l'unité de renseignements passagers. Il convient de souligner qu'il n'est pas précisé dans la proposition de directive que les unités de renseignements passagers devront être des autorités publiques. Une telle précision apparaît indispensable même si, selon les informations communiquées au rapporteur, cela semble aller de soi pour les Etats membres. L'unité de renseignements passagers pourrait être un département de l'autorité compétente en matière de prévention et de détection d'infractions terroristes et d'infractions graves, ainsi que d'enquêtes et de poursuites en la matière.

Plusieurs Etats membres pourraient instituer la même autorité en tant qu'unité de renseignements passagers.

L'unité de renseignements passagers serait chargée de procéder à l'évaluation du risque représenté par un passager avant son arrivée ou son départ pour identifier les personnes qui pourraient être impliquées dans une infraction terroriste ou une infraction transnationale grave et pour lesquelles un examen approfondi par les autorités compétentes est requis.

Selon que l'objectif visé soit la criminalité grave transnationale ou non transnationale, les modalités de traitement des données seraient différentes. La détection préventive de personnes encore inconnues des services répressifs ne pourrait viser à prévenir que des infractions transnationales graves alors que la détection de personnes déjà connues par le croisement avec des fichiers existants concernerait toutes les infractions graves, transnationales ou non. En matière de criminalité grave transnationale, les données PNR pourraient être traitées au regard de critères préétablis. Tout résultat obtenu par un traitement automatisé devrait être contrôlé individuellement. Il est prévu que les critères préétablis ne soient en aucun cas fondés sur la race ou l'origine ethnique, les convictions religieuses ou philosophiques, les opinions politiques, l'appartenance à un syndicat, l'état de santé ou la vie sexuelle du passager.

En matière de criminalité grave, l'évaluation par l'unité de renseignements passagers pourrait être faite par la confrontation des données PNR aux bases de données pertinentes, notamment les bases de données internationales ou nationales ou les bases de données de l'Union créées pour recenser les personnes et objets recherchés ou visés par un signalement. Tout résultat positif

obtenu par un tel traitement automatisé devrait être contrôlé individuellement par des moyens non automatisés.

En conséquence, l'unité de renseignements passagers d'un État membre ne transférerait qu'au cas par cas les données PNR ou les résultats du traitement des données PNR des personnes identifiées aux autorités compétentes de l'Etat membre pour un examen plus approfondi.

L'unité de renseignements passagers devrait également répondre aux demandes motivées des autorités compétentes visant à obtenir des données PNR et le traitement de celles-ci dans des cas spécifiques.

Enfin, l'unité de renseignements passagers serait chargée de mettre à jour ou de définir de nouveaux critères pour la réalisation d'évaluations pour la lutte contre la criminalité grave transnationale.

L'encadré suivant reproduit les données PNR qui seraient transmises aux unités de renseignements passagers :

**Données PNR telles qu'elles sont recueillies par les transporteurs aériens**

(1) Code repère du dossier passager

(2) Date de réservation/d'émission du billet

(3) Date(s) prévue(s) du voyage

(4) Nom(s)

(5) Adresse et coordonnées (numéro de téléphone, adresse électronique)

(6) Moyens de paiement, y compris adresse de facturation

(7) Itinéraire complet pour le dossier passager spécifique

(8) Profil de passager fidèle

(9) Agence de voyages/agent de voyages

(10) Statut du voyageur (confirmations, enregistrement, non-présentation ou passager de dernière minute sans réservation)

(11) Indications concernant la scission/division du dossier passager

(12) Remarques générales (notamment toutes les informations disponibles sur les mineurs non accompagnés de moins de 18 ans, telles que le nom et le sexe du mineur, son âge, les langues parlées, le nom et les coordonnées du tuteur présent au départ et son lien avec le mineur, le nom et les coordonnées du tuteur présent à l'arrivée et son lien avec le mineur, agent présent au départ et à l'arrivée)

(13) Etablissement des billets (numéro du billet, date d’émission, allers simples, champs de billets informatisés relatifs à leur prix)

(14) Numéro du siège et autres informations concernant le siège

(15) Informations sur le partage de code

(16) Toutes les informations relatives aux bagages

(17) Nombre et autres noms de voyageurs figurant dans le dossier passager

(18) Toute information préalable sur les passagers (API) qui a été recueillie

(19) Historique complet des modifications des données PNR énumérées aux points 1 à 18

La transmission se ferait selon la méthode « *push* », par laquelle les compagnies aériennes transfèrent les données aux autorités compétentes, sans que celles-ci aient un accès aux bases de données des compagnies aériennes. Cette méthode est la plus protectrice des données personnelles.

Il ne serait pas exigé des transporteurs aériens qu'ils recueillent des données supplémentaires par rapport à leur pratique actuelle. Il ne serait pas non plus requis des passagers de transmettre de nouvelles données par rapport aux pratiques actuelles. Les transferts, par les transporteurs aériens, aux unités de renseignements passagers concernées par un vol (atterrissage ou décollage), auraient lieu de 24 à 48 heures avant le départ programmé, immédiatement après la clôture du vol et, au cas par cas, sur demande d'une unité de renseignements passagers, de manière supplémentaire pour réagir à une menace spécifique et réelle liée à des infractions terroristes ou à des infractions graves. La création d'un comité est proposée pour assister la Commission européenne afin de déterminer les protocoles communs et les formats de transmission des données PNR.

Le dispositif trouverait à s'appliquer de manière progressive (30 % des vols après 2 ans de mise en oeuvre, 60 % après 4 ans, 100 % après 6 ans).

L'utilisation des données dites sensibles serait exclue. Il s'agit des données à caractère personnel susceptibles de révéler l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance à un syndicat ainsi que les données qui concernent la santé ou la vie sexuelle de l'intéressé. De telles informations seraient susceptibles d'apparaître sous la rubrique n° 12 « remarques générales » ou pourraient se déduire d'autres informations telles que le nom de l'organisme qui aurait effectué la réservation ou l'adresse de facturation (syndicat ou parti politique). Déjà, lors de la discussion de la proposition de décision-cadre, cette question était problématique. Une utilisation au cas par cas des données sensibles apparaissant éventuellement dans un dossier PNR, pour des procédures policières et judiciaires bien spécifiques, était défendue par certains Etats membres tels que le Royaume-Uni. La présente proposition interdit tout traitement de données sensibles et précises qu'il reviendrait à l'unité de renseignements passagers d'effacer, dès leur réception, les données sensibles éventuellement transmises par les compagnies aériennes. En outre, comme cela a été précisé, les critères définis pour procéder à l'évaluation du risque représenté par un passager ne pourraient en aucun cas être fondés sur la race ou l'origine ethnique d'une personne, ses convictions religieuses ou philosophiques, ses opinions politiques, son appartenance à un syndicat, son état de santé ou sa vie sexuelle. Toutefois, dans le dernier état du texte en discussion, il

est fait référence aux données sensibles telles qu'elles sont définies à l'article 21 de la charte européenne des droits fondamentaux. Or, cet article 21 retient une définition plus large des données sensibles et dispose qu' « *est interdite toute discrimination fondée notamment sur le sexe, la race, la couleur, les origines ethniques ou sociales, les caractéristiques génétiques, la langue, la religion ou les convictions, les opinions politiques ou toute autre opinion, l'appartenance à une minorité nationale, la fortune, la naissance, un handicap, l'âge ou l'orientation sexuelle* ». Le paragraphe deux de l'article 21 dispose que « *dans le domaine d'application des traités et sans préjudice de leurs dispositions particulières, toute discrimination exercée en raison de la nationalité est interdite* ». En conséquence, les critères établis pour définir le niveau de risque d'un passager ne pourraient plus faire référence ni à son sexe, ni à son âge, ni à sa nationalité. Il paraît assez problématique de se passer de ces éléments dans le cadre de l'utilisation des données PNR. Par ailleurs, très concrètement, cela suppose un travail de tri important de la part de l'unité de renseignements passagers puisque l'âge (personne mineure) et le sexe font partie des données transmises par les compagnies aériennes.

**b) Pour une durée de conservation aussi brève que possible mais qui demeure compatible avec les objectifs du projet**

La durée de conservation des données est un aspect fondamental du dispositif, tant pour son efficacité opérationnelle que pour la protection des données personnelles. Dans son rapport publié en 2009, le rapporteur préconisait une durée de conservation très inférieure à celle applicable dans l'accord passé avec les Etats-Unis et qui soit comprise entre trois et six ans (la proposition de décision-cadre prévoyait une durée de conservation de 13 ans, dont huit années dans une base de données dite inactive, ce qui paraissait tout à fait excessif). Il est heureux que la proposition de directive s'éloigne de la durée de 13 ans initialement envisagée. En effet, il est proposé que les données ne puissent être conservées dans une base de données que pendant une période de 30 jours, à l'expiration de laquelle les données seraient conservées pendant une période supplémentaire de cinq ans, période au cours de laquelle tous les éléments d'information pouvant servir à identifier le passager auquel elles se rapportent serait masqués.

L'accès à l'intégralité des données PNR ne serait autorisé que par le responsable de l'unité de renseignements passagers et pour mener une enquête ou réagir à une menace spécifique et tangible. Il convient de noter que le masquage n'est, selon les informations transmises au rapporteur, pas utilisé à ce jour dans les fichiers de police en France et que cette notion n'est pas tout à fait claire. La Commission européenne n'a pas explicité ce que représente précisément le masquage ni ses caractéristiques techniques. Par rapport à une anonymisation, le masquage des données permet de retrouver l'intégralité des données originelles.

À l'issue des cinq années de conservation, les données PNR devraient être effacées, sauf dans le cas de poursuites ou d'enquêtes pénales en cours.

Les services opérationnels des douanes et de la police entendus par le rapporteur ont souligné que la durée de conservation de trente jours serait probablement beaucoup trop limitée pour permettre une utilisation efficace des données et pour la réalisation de critères de ciblage efficients. Les autorités françaises souhaitent donc que la première période de conservation soit portée à un an. Il convient en effet de ne pas perdre de vue qu'un historique suffisamment long des déplacements doit être conservé pour l'efficacité du dispositif. Des rapprochements doivent pouvoir être faits sur une durée suffisamment significative, s'agissant par exemple de personnes qui effectuent régulièrement des déplacements dans des pays jugés à risque. Dans le cas contraire, la définition de critères de ciblage pertinents ne serait pas possible.

Une fois les données ou le résultat du traitement des données entre les mains des autorités compétentes, habilitées à intervenir en matière de prévention ou de détection d'infractions terroristes et d'infractions graves, ainsi que d'enquêtes et de poursuites en la matière, les données ne pourraient faire l'objet d'un traitement ultérieur qu'aux fins de prévention et de détection d'infractions terroristes et d'infractions graves. Les autorités compétentes auraient l'interdiction de prendre toute décision susceptible de produire des effets juridiques préjudiciables à une personne ou de l'affecter gravement sur la seule base du traitement automatisé des données PNR. En outre, les décisions de cette nature ne pourraient être fondées sur des critères tels que la race ou l'origine ethnique d'une personne, ses convictions religieuses ou philosophiques, ses opinions politiques, l'appartenance à un syndicat ou des critères relatifs à la santé ou à la vie sexuelle.

**c) Les échanges de données au sein de l'Union et les transferts vers des Etats tiers**

Le principe retenu pour les échanges entre Etats membres est celui d'une communication d'unité de renseignements passagers à unité de renseignements passagers.

Si une unité de renseignements passagers considérait qu'il faut transférer les données à l'unité de renseignements passagers d'un autre Etat membre, elle pourrait procéder au transfert. L'unité de renseignements d'un Etat membre pourrait demander en cas de besoin à celle d'un autre Etat membre de lui communiquer des données PNR qui sont conservées dans sa base de données, dans un cas précis de prévention et de détection d'infractions terroristes, d'infractions graves, d'enquêtes ou de poursuites. Cette procédure vise les données conservées pendant la première période de 30 jours. S'agissant des données qui ont été masquées, l'unité de renseignements d'un Etat membre pourrait également adresser une demande à celle d'un autre Etat membre. Toutefois elle ne pourrait demander le transfert des données dans leur intégralité et sans passages tronqués que dans des circonstances exceptionnelles, afin de réagir à une menace spécifique ou dans le cadre d'une enquête ou de poursuites spécifiques.

Enfin, en cas de nécessité pour prévenir une menace immédiate et grave à la sécurité publique, les autorités compétentes d'un Etat membre pourraient demander directement à l'unité de renseignements passagers d'un autre Etat de leur communiquer les données PNR. De telles demandes ne pourraient prendre place que dans le cadre d'une enquête spécifique de poursuites spécifiques et devraient être motivées. À titre tout à fait exceptionnel, si un accès anticipé à des données PNR était nécessaire, l'unité d'un Etat membre aurait le droit de demander à celle d'un autre Etat membre de lui communiquer à tout moment les données PNR d'un vol à destination de son territoire ou en provenance de celui-ci.

Le transfert éventuel des données vers des pays tiers est une préoccupation majeure dans le domaine des données PNR. Le rapporteur a ainsi toujours défendu l'idée, notamment s'agissant des accords avec les Etats-Unis ou l'Australie, qu'un transfert ultérieur ne puisse se faire qu'avec l'accord de l'Etat d'origine des données. Dans le cas présent, le transfert pourrait avoir lieu à trois conditions :

- les conditions définies à l'article 13 de la décision-cadre sur la protection des données sont remplies, c'est-à-dire si l'autorité destinataire de l'Etat tiers destinataire est chargée de la prévention et de la détection des infractions pénales, des enquêtes et des poursuites en la matière ou de l'exécution des sanctions pénales, si l'Etat membre auprès duquel les données ont été collectées a donné son accord au transfert dans le respect de sa législation nationale, et si l'Etat tiers concerné assure un niveau de protection adéquat pour le traitement de données envisagé[(5)] ;

- le transfert est nécessaire aux fins de la directive ;

- le pays tiers n'accepte de transférer les données à un autre pays tiers que si c'est nécessaire aux fins de la directive et uniquement sur autorisation expresse de l'Etat membre d'origine des données.

Il conviendra de s'assurer qu'aucun transfert de données en masse ne puisse être effectué, même au cas par cas.

**d) Les autres éléments de protection des données personnelles**

Tout passager aurait un droit d'accès, de rectification, d'effacement et de verrouillage des données, ainsi qu'un droit à réparation et un droit à un recours

---

*[(5)] Un certain nombre de dérogations sont prévues dans l'article 13, qui s'appliqueraient également à la directive sur les PNR. Ainsi, le transfert sans accord préalable n'est autorisé que si le transfert de données est essentiel pour prévenir un danger immédiat et sérieux pour la sécurité publique d'un Etat membre ou d'un Etat tiers ou pour les intérêts essentiels d'un Etat membre et que l'accord préalable ne peut pas être obtenu en temps utile. En outre, par dérogation à l'exigence de niveau de protection adéquat, les données peuvent être transférées si la législation nationale de l'Etat membre qui transfère les données le prévoit, pour des intérêts spécifiques légitimes de la personne concernée, ou lorsque des intérêts légitimes prévalent, en particulier des intérêts publics importants, ou si l'Etat tiers ou l'instance internationale destinataire prévoit des garanties qui sont jugées adéquates par l'Etat membre concerné.*

juridictionnel qui soient identiques à ceux adoptés en droit national en application de la décision-cadre 2008/977/JAI du Conseil. Les articles 17 à 22 de la décision-cadre seraient applicables. Le rapporteur note que la directive ne devrait pas se contenter de renvoyer à la décision-cadre de 2008 mais devrait comprendre en son sein un régime de protection détaillé, tel que celui auquel les négociations avaient abouti en 2009. Le rapporteur souligne une nouvelle fois la nécessité d'un régime de protection des données parfaitement clair à chaque étape de la collecte, du traitement et de la conservation des données.

La question du régime de protection des données applicable entre compagnies ou intermédiaires et unités de renseignements passagers n'est pas résolue. Il semble que les dispositions de la décision-cadre de 2008 seraient applicables à tout traitement de données au titre de la directive, c'est-à-dire également au transfert de données entre les compagnies aériennes et des unités de renseignements passagers. La directive de 1995[6], relative à la protection des données dans l'ancien premier pilier, aurait également pu trouver à s'appliquer afin que les compagnies aériennes aient à respecter un ensemble uniforme de règles pour la manipulation des données, y compris pour leur transfert vers les unités de renseignements passagers.

Par ailleurs, il convient de noter que les Etats membres n'avaient pas souhaité que la décision-cadre de 2008 s'applique aux données traitées sur le plan interne, la décision-cadre ne visant que les données échangées entre Etats membres. Si le principe d'une application des normes posées par la décision-cadre de 2008 à toutes les étapes du traitement était adopté, cela constituerait donc un pas en avant positif dans l'harmonisation de la protection des données s'agissant de l'espace de liberté, de sécurité et de justice.

Tout traitement et toute opération ayant trait aux données PNR devraient faire l'objet d'une trace documentaire qui devrait être conservée par l'unité de renseignements passagers tant que les données le sont également.

Il appartiendrait aux Etats membres de veiller à ce que les transporteurs aériens ou les revendeurs de billets de transport ainsi que les passagers disposent d'informations étendues sur le traitement des données PNR. Des sanctions effectives, proportionnées et dissuasives devraient être prévues dans chaque Etat membre en cas de violation des dispositions de la directive.

L'autorité de contrôle national prévue par la décision-cadre de 2008 (article 25) serait également chargée de conseiller et de surveiller l'application de la directive.

---

[6] *Directive 95/46/CE du Parlement européen et du Conseil, 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.*

*3. Les avis du contrôleur européen de la protection des données, de l'agence européenne des droits fondamentaux et du G29 demeurent négatifs*

Dans son avis en date du 25 mars 2011, Peter Hustinx, contrôleur européen de la protection des données, salue le fait d'avoir été consulté par la Commission européenne. Il note que, d'une manière générale, la protection des données a été nettement accrue par rapport à la proposition de décision-cadre antérieure. Cependant, il insiste sur le fait que la démonstration de la nécessité et de la proportionnalité de la mesure est un prérequis absolu pour développer le système PNR. Il juge que les éléments contenus dans la proposition de directive ne suffisent pas à justifier la nécessité et la proportionnalité de la mesure.

Il note, s'agissant de l'exemple de la Belgique cité dans l'étude d'impact, qui a réalisé 95 % de ses saisies de drogue en 2009, exclusivement ou essentiellement grâce aux données PNR, que la Belgique n'exploite pas les données PNR de manière systématique, comme le propose la directive.

Le contrôleur note que les bases de données auxquelles les données PNR pourraient être comparées ne sont pas spécifiées, ce qui laisse la porte ouverte à des abus. Par ailleurs, l'harmonisation proposée serait limitée et les PNR nationaux utilisant ces données de manière plus large, par exemple pour combattre l'immigration illégale, pourraient être maintenus. Le contrôleur souligne également que la définition des crimes graves est trop large (il convient de relever que le contrôleur s'est prononcé sur la version initiale de la proposition). Par ailleurs, la notion d'infractions mineures n'était pas claire. Le contrôleur s'inquiétait également de la possibilité d'étendre le champ d'application aux vols intérieurs. Faire référence à la décision-cadre de 2008 s'agissant de la protection des données n'est, selon lui, pas satisfaisant, du fait des insuffisances de cette dernière, s'agissant notamment des exceptions très larges prévues aux principes posés pour le transfert des données à des Etats tiers. Au contraire, la directive de 1995 applicable à l'ancien premier pilier offre des standards de protection plus élevés. Le contrôleur estime enfin que la liste des données transférées est encore trop large et prône, à l'issue de la période de conservation de 30 jours, une anonymisation définitive des données, sans retour en arrière possible.

En conclusion, bien que de nets progrès aient été accomplis par rapport à la proposition de décision-cadre, des améliorations devraient encore être apportées au texte et le contrôleur juge que l'utilisation des données PNR ne doit pas être systématique mais limitée à certains cas spécifiques.

Dans son avis 10/2011 sur la proposition de directive, adopté le 5 avril 2011, le G29 (groupe dit de l'article 29 qui regroupe les autorités nationales chargées de la protection des données dans les Etats membres, telles que la CNIL en France) rappelle qu'il a invariablement mis en doute la nécessité et la proportionnalité des systèmes PNR et qu'il maintient cette position à l'égard de la

proposition de 2011. Ni la nécessité de la mesure ni sa proportionnalité aux objectifs poursuivis ne sont pertinemment justifiées, malgré les efforts qui ont été faits pour mieux encadrer le dispositif par rapport à la proposition de décision-cadre de 2007. Les finalités de la directive ne sont pas suffisamment restreintes, la durée de conservation est toujours jugée excessive, les droits des personnes concernées sont insuffisants, la liste des données transmises trop large et les possibilités de transfert ultérieur à des Etats tiers trop étendues.

L'Agence européenne pour les droits fondamentaux s'est, quant à elle, prononcée le 14 juin 2011 sur la proposition de directive. L'Agence a concentré son étude sur le droit au respect de la vie privée, le droit à la protection des données personnelles et l'interdiction de toute discrimination, tels que garantis par la charte européenne des droits fondamentaux ainsi que par la Convention européenne des droits de l'homme. L'Agence reconnaît l'introduction de garanties visant à réduire le risque de discrimination ou de profilage discriminatoire. Néanmoins, selon elle, il faudrait interdire la transmission de données sensibles par les compagnies aériennes. L'agence suggère également d'élargir la définition des données sensibles et de viser l'article 21 de la charte. Cette remarque a été prise en compte mais soulève également d'autres difficultés vues précédemment. Selon l'Agence, il serait nécessaire de mettre sur pied un recueil statistique des actions menées sur la base de la directive afin de recenser les cas dans lesquels une personne est affectée de manière négative et sans raison et de pouvoir prouver l'efficacité ou l'inefficacité du système. La nécessité d'un tel système n'est, selon l'Agence, toujours pas démontrée. La Commission européenne fournit des exemples qui se limitent aux crimes graves transnationaux. Ces derniers devraient donc être seuls visés par la directive.

Il convient de relever que, dans un avis en date du 12 avril 2011, le service juridique du Conseil de l'Union européenne a émis des critiques importantes sur le système PNR, tel qu'il est proposé dans la directive, quant au principe de proportionnalité et à sa motivation. Toutefois, l'analyse développée par le service juridique a été largement remise en cause par plusieurs Etats membres.

Il a en outre relevé les risques de contestation devant les cours constitutionnelles nationales. Il convient de rappeler que, s'agissant de la directive 2006/24/CE du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de communications électroniques accessibles au public ou de réseaux publics de communication, saisie d'un recours de 34 000 citoyens, la cour constitutionnelle allemande a, dans un arrêt du 2 mars 2010, donné son accord s'agissant du principe de conserver les données pendant six mois, tout en rappelant que l'obligation de conservation pesait sur les opérateurs eux-mêmes de manière non centralisée, ce qui était jugé positif. Mais la cour a annulé la loi allemande de transposition comme étant non conforme au principe de proportionnalité. La cour a demandé notamment que les données concernées ne puissent être accessibles que sur ordre d'un tribunal et seulement

dans le cas d'un «danger concret et imminent». Le fait qu'un très grand nombre de personnes qui ne sont suspectées de rien voient leurs données stockées nécessiterait, selon la cour, des normes de sécurité très élevées et une finalité des traitements très restrictive (crimes graves à énumérer). La cour a ajouté qu'une telle mesure de conservation préventive des données de télécommunications réduirait d'autant la possibilité d'adopter, même au niveau européen, d'autres mesures de conservation préventive (point 218 de l'arrêt 1 BvR 256/08 du 2 mars 2010).

La cour suprême administrative bulgare ainsi que la cour constitutionnelle roumaine ont, respectivement le 11 décembre 2008 et le 8 octobre 2009, rendu des arrêts proches s'agissant de la conservation de grande ampleur de données personnelles de personnes qui n'ont rien à se reprocher.

Les problèmes constitutionnels que la mise en oeuvre d'un système PNR européen est susceptible de générer dans plusieurs Etats membres ne doivent donc pas être ignorés.

## CONCLUSION

En conclusion, la proposition de directive s'attache très clairement à créer un équilibre satisfaisant entre les impératifs opérationnels de la lutte contre le terrorisme et la criminalité grave et les atteintes aux droits fondamentaux qu'impliquerait l'utilisation des données PNR.

Plusieurs Etats membres, au-delà de la France, soutiennent le projet. Ainsi, le Royaume-Uni, la Suède, le Danemark, la Belgique, les Pays-Bas et l'Espagne sont très impliqués dans les négociations.

Le Sénat, ayant examiné la proposition directive le 12 avril 2011, a pris acte de ce que le dispositif évoluait dans un sens plus conforme au respect des droits fondamentaux et rappelé les exigences de protection de ces doits.

Le rapporteur du Parlement européen pour la commission des libertés civiles, M. Thimothy Kirkhope, est favorable à la mise en œuvre d'un système PNR équilibré. Toutefois, il convient de noter que le projet d'avis déposé par Mme Lichtenberger de la commission transports et tourisme vise à réduire le champ des finalités à la seule lutte contre le terrorisme (hors tentative et complicité), les données transmises et à restreindre la durée de conservation à 30 jours. De telles modifications seraient de nature à remettre en cause l'intérêt même de l'instrument.

Il convient de noter que les débats qui se sont déroulés depuis 2007 n'ont pas été vains et que nombre des améliorations proposées, tant par l'Assemblée nationale et les parlements nationaux que par les autorités de protection des données, ont été retenues et retranscrites dans la proposition de directive.

Le rapporteur demeure convaincu de la nécessité d'utiliser les données PNR dans la lutte contre le terrorisme et la criminalité grave. Il se félicite que l'approche retenue en 2007 s'agissant de la durée de conservation, des données sensibles, des droits des personnes ou encore des échanges avec les pays tiers ait été revue dans un sens plus protecteur des droits fondamentaux.

Il convient toutefois également de veiller à préserver l'efficacité du dispositif, s'agissant de la durée de conservation qui ne doit pas être réduite à l'extrême, ainsi que de la question de l'application aux vols intra européens qui sont nécessairement empruntés par les trafiquants.

L'Union doit se doter d'un tel instrument, à la fois parce que les données PNR sont nécessaires à la lutte contre le terrorisme et la criminalité grave et parce que si l'Union se dotait d'une doctrine unifié en la matière, elle serait davantage en mesure de peser sur les accords PNR internationaux.

## TRAVAUX DE LA COMMISSION

La Commission s'est réunie le 16 novembre 2011, sous la présidence de M. Pierre Lequiller, Président, pour examiner le présent rapport d'information.

L'exposé du rapporteur a été suivi d'un débat.

« **M. Philippe Tourtelier.** Je remercie le rapporteur de son excellent travail et d'avoir bien posé la question. Il s'agit en effet d'une avancée mais on pourrait certainement faire plus. Conformément aux avis du contrôleur européen de la protection des données et du G29, je souhaite que le texte de la résolution prenne mieux en compte la proportionnalité.

**M. Guy Geoffroy, rapporteur.** Il est en effet possible d'insister sur la proportionnalité, cela ne nuisant pas à la cohésion du texte. Je souhaite toutefois souligner, de façon tout à fait respectueuse des avis de ces autorités mais avec une certaine conviction, que si l'on suivait les avis négatifs du contrôleur européen de la protection des données et du G29, qui concluent notamment à la diminution du délai maximum de conservation des données et à l'exclusion des vols intra-européens, on dépouillerait le dispositif de son utilité. Il vaudrait alors mieux en rester là où on est aujourd'hui car, sinon, nous serions fragilisés dans le dialogue avec nos partenaires, américains, notamment. Rappelons que demain, peut-être, d'autres partenaires, tels que la chine, souhaiteront avoir accès aux données PNR.

**M. Philippe Tourtelier.** Il faut donc réintégrer les critères de la nécessité et de la proportionnalité.

**M. Guy Geoffroy, rapporteur.** Cela peut en effet devenir un atout. La proportionnalité signifie également qu'il serait peu utile de ne garder les données qu'un mois et qu'il y a la nécessité de prendre en compte les vols intra-européens.

**M. Jérôme Lambert.** Je suis d'accord avec M. Tourtelier. Au point 4 de la proposition de résolution, le mot « importantes » me gêne.

**M. Guy Geoffroy, rapporteur.** Je propose « incontestables».

**M. Jérôme Lambert.** Je suis d'accord. Au point 5, il faudrait, selon moi, ajouter, à la fin, « ce qui n'est pas le cas actuellement » car il faut renforcer ainsi la demande dans la mesure où ce qui est proposé ne convient pas encore.

**M. Guy Geoffroy, rapporteur.** Je suis d'accord. Il s'agit là de souligner que le cadre de la protection des données doit être précisé dans la directive même.

**M. Jérôme Lambert.** Au point 6, Je ne m'oppose pas à la formulation proposée concernant la durée de conservation des données mais il est difficile de trouver un juste milieu entre les 30 jours proposés et plusieurs années. Ne serait-il pas préférable d'inscrire une durée dans la résolution ?

**M. Guy Geoffroy, rapporteur.** Il ne faut pas que la durée de conservation des données soit trop réduite, une durée effective d'un an permettant d'atteindre les objectifs visés. En partant d'une proposition de cinq ans sur une base active dans la décision-cadre de 2007, aboutir à un an me parait raisonnable. Il semble cependant préférable de s'en tenir à la formulation proposée.

Puis la Commission *a approuvé* la proposition de résolution dont le texte figure ci-après. »

**PROPOSITION DE RESOLUTION EUROPEENNE**

L'Assemblée nationale,

Vu l'article 88-4 de la Constitution,

Vu la proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière (COM [2011] 32 final/n° E 6014),

Vu la résolution de l'Assemblée nationale n° 352 du 18 octobre 2009 sur la proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (*Passenger Name Record*, PNR) à des fins répressives,

1. Souligne les critères de nécessité et de proportionnalité qui s'appliquent au traitement des données à caractère personnel ;

2. Rappelle sa position selon laquelle les données PNR constituent un outil nécessaire à la lutte contre le terrorisme et les formes graves de criminalité ainsi qu'aux enquêtes et poursuites en la matière ;

3. Estime que la mise en oeuvre d'un régime de transfert et de collecte harmonisé au niveau européen renforcerait l'efficacité des mesures prises au plan national par les Etats membres en matière de lutte contre le terrorisme et les formes graves de criminalité ;

4. Juge qu'un tel régime permettrait à l'Union de mieux imposer les standards européens s'agissant du droit au respect de la vie privée et du droit à la protection des données à caractère personnel dans les accords internationaux entre l'Union européenne et les Etats tiers ;

5. Se félicite que des améliorations incontestables aient été apportées dans la proposition de directive, conformément notamment aux demandes exprimées par l'Assemblée nationale dans sa résolution n° 352 du 18 octobre 2009 précitée ;

6. Demande que le cadre établi par la directive soit parfaitement clair et cohérent à chaque étape de la collecte, du traitement et de la conservation des données et assure le plein respect des droits fondamentaux, notamment du droit à la protection des données à caractère personnel et du droit au respect de la vie privée, ce qui n'est pas le cas actuellement ;

7. Estime que la durée de conservation des données ne doit pas être excessivement réduite car l'intérêt même du dispositif pourrait s'en trouver significativement affecté et que les vols intra-européens ne devraient pas être exclus du champ d'application de la directive.

## ANNEXE :
## LISTE DES PERSONNES ENTENDUES PAR LE RAPPORTEUR

- M. Emmanuel BARBE, secrétariat général des affaires européennes, secrétaire général adjoint ;

- M. Laurent MONBRUN, secrétariat général des affaires européennes, chef du secteur sécurité ;

- M. le Préfet Marc CABANE, directeur du projet API/PNR, conseiller du secrétaire général à l'intégration et à l'immigration ;

- M. Perry MENZ, directeur des services douaniers, chef de la division surveillance à Roissy ;

- M[me] Muriel SYLVAN, membre de la mission API/PNR, questions juridiques ;

- M. Gérard SCHOEN, Direction générale des douanes et des droits indirects, sous directeur des affaires juridiques, du contentieux, du contrôle et de la lutte contre la fraude ;

- M. Thierry PICARD, DGDDI/Bureau D3, chef de bureau de la lutte contre la fraude ;

- M. Jean MAFART, ministère de l'intérieur, de l'outre-mer, des collectivités territoriales et de l'immigration, directeur adjoint du cabinet du directeur général de la police nationale ;

- M[me] Armelle LEROY, ministère de l'intérieur, de l'outre-mer, des collectivités territoriales et de l'immigration, commissaire de police, direction centrale du renseignement intérieur ;

- M. Denis BRUEL, ministère de l'intérieur, de l'outre-mer, des collectivités territoriales et de l'immigration, direction des libertés publiques et des affaires juridiques, chef du bureau de la liberté individuelle ;

- M. Michael GIHR, magistrat, ministère de la justice et des libertés, direction des affaires criminelles et des grâces, mission négociation et transposition des normes pénales internationales ;

- M. Patrick LANSMAN, ministère de l'écologie, du développement durable, des transports et du logement, direction générale de l'aviation civile, direction du transport aérien, chef de la mission du droit des passagers ;

- M. Francis DELON, secrétaire général de la défense et de la sécurité nationale.