N° 1447

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

TREIZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 11 février 2009.

RAPPORT

FAIT

AU NOM DE LA COMMISSION CHARGÉE DES AFFAIRES EUROPÉENNES[1] *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),**

PAR M. Guy GEOFFROY,

Député

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

La Commission chargée des affaires européennes est composée de : M. Pierre Lequiller, *président ;* MM. Michel Herbillon, Thierry Mariani, Pierre Moscovici, Didier Quentin, *vice-présidents ;* MM. Jacques Desallangre, Jean Dionis du Séjour, *secrétaires ;* M. Alfred Almont, M^me^ Chantal Brunel, MM. Christophe Caresche, Bernard Deflesselles, Michel Delebarre, Daniel Fasquelle, Pierre Forgues, M^me^ Arlette Franco, MM. Jean-Claude Fruteau, Daniel Garrigue, Hervé Gaymard, Guy Geoffroy, M^mes^ Annick Girardin, Elisabeth Guigou, MM. Régis Juanico, M^me^ Marietta Karamanli, MM. Marc Laffineur, Jérôme Lambert, Robert Lecou, Céleste Lett, Lionnel Luca, Noël Mamère, Jacques Myard, Christian Paul, Didier Quentin, M^mes^ Valérie Rosso-Debord, Odile Saugues, MM. André Schneider, Philippe Tourtelier, Gérard Voisin.

SOMMAIRE

—

Pages

Mesdames, Messieurs,

Le présent rapport étudie la proposition de décision-cadre tendant à l'utilisation des données de 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.

Cet instrument 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.

Les données PNR ont plusieurs utilités : collectées en amont du décollage, elles peuvent être traitées en temps réel sur la base d'une analyse de risque et induire une conduite des forces de police si nécessaire puis, conservées dans des bases de données, elles permettent de procéder à des analyses de long terme en matière de terrorisme et de criminalité et de répondre, au cas par cas, aux besoins d'une enquête policière ou judiciaire.

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.

Tant la masse des données en cause que le fait qu'elles concernent des personnes dont l'immense majorité n'est suspectée de rien et n'a rien à se reprocher peuvent susciter une réaction de méfiance. Ce projet se situe face à deux enjeux fondamentaux : la lutte contre le terrorisme et les formes graves de criminalité, d'une part, et la préservation des droits fondamentaux, au premier rang desquels le droit au respect de la vie privée, d'autre part.

Une telle mesure serait coûteuse mais aucune évaluation réellement fiable n'est disponible, si ce n'est l'exemple du Royaume Uni, pays le plus avancé en la matière, qui a à ce jour dépensé 70 millions de Livres.

Au cours de ses travaux, 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. Comme l'ont souligné les personnes auditionnées, la politique européenne en matière de données des dossiers passagers ne s'est construite depuis dix ans que face aux exigences des pays tiers dans le cadre des accords négociés avec les Etats-Unis, le

Canada ou l'Australie. L'Union doit dorénavant veiller à ses propres intérêts dans la lutte contre le terrorisme et la criminalité grave et pouvoir imposer son approche de l'équilibre entre sécurité et respect des droits fondamentaux. L'institution d'un système de collecte des données PNR fondé sur ses valeurs permettra à l'Europe de faire entendre sa voix et de démontrer qu'il existe bien une autre voie possible que celle suivie par les Etats-Unis.

PREMIERE PARTIE :
LES REGIMES DE COLLECTE ET DE TRAITEMENT DES DONNEES PNR EXISTANTS

Le Conseil européen des 25 et 26 mars 2004 a invité la Commission européenne à soumettre une proposition en vue d'une approche commune de l'Union dans l'utilisation des données des dossiers passagers à des fins répressives. Cet objectif figure également dans le programme de La Haye.

La présente proposition de décision-cadre tendant à l'utilisation des données de dossiers passagers (*passenger name record* ou PNR) à des fins répressives fait suite à la « négociation » d'un accord conclu entre les Etats-Unis et l'Union européenne sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure (DHS) en juillet 2007.

L'introduction d'un système de collecte et de traitement des données des dossiers passagers en Europe revêt une grande importance pour la construction de l'espace commun de sécurité. Alors que l'Union européenne a accepté de transmettre des données PNR à des pays tiers (Etats-Unis, Canada, Australie), il est paradoxal qu'elle ne se soit pas dotée d'une législation lui permettant d'instituer un dispositif harmonisé à l'échelle européenne. Ce nouvel instrument est déjà mis en oeuvre ou à l'étude dans quelques pays européens (Royaume-Uni, Belgique, Danemark et France). Une approche européenne permettrait d'harmoniser les pratiques, d'améliorer l'efficacité des mesures prises en assurant la disponibilité des informations recueillies par 27 Etats membres et de limiter les contraintes éventuellement divergentes qui pourraient être imposées par le droit national des Etats membres aux transporteurs aériens.

Néanmoins, au vu de la nature des données en question et des fins pour lesquelles elles seraient collectées, la proposition de décision-cadre devra impérativement refléter fidèlement l'attachement de l'Union au respect des droits fondamentaux.

A l'issue de la présidence slovène, un texte de proposition de décision-cadre amendée a été publié. Mais il est apparu à la présidence slovène ainsi qu'à la présidence française que les débats techniques ne pourraient pas aller plus loin sans qu'un cadre global ait été préalablement arbitré au niveau politique. Il a été décidé de sérier les problèmes et d'établir la liste des principales questions qui se posent sur la proposition de décision-cadre puis d'organiser des débats thématiques afin de trancher sur les grandes orientations qui doivent prévaloir à

l'élaboration de la proposition de décision-cadre. Les travaux menés sous présidence française ont permis, avec succès, de dessiner les grandes lignes du projet sur lesquelles les Etats membres s'accordent. Un nouveau projet de texte a été publié le 23 janvier 2009, reflétant en bonne partie les orientations dégagées sous présidence française.

Comme cela été souligné par les personnes auditionnées par le rapporteur, la proposition de décision-cadre revêt une importance particulière, tant par le champ des données concernées, que par la difficulté de bâtir, alors que la plupart des Etats membres n'ont pas encore de système d'exploitation national, un régime européen harmonisant la collecte et le traitement des données PNR en prenant en compte l'ensemble des questions qui se posent, de la pure technique de transmission à la protection des droits des personnes concernées.

Avant de s'attacher à étudier le texte proposé, le rapporteur dressera un état des lieux de l'utilisation des données PNR en Europe.

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

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 quant aux repas par exemple ou en relation avec son état de santé.

Les données dites « APIS » (*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 APIS et les données PNR sont donc bien différentes. Les données APIS 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 %.

Les données APIS sont, comme l'expliquent les autorités britanniques, particulièrement intéressantes lorsqu'une personne attire déjà l'attention des

autorités alors que les données PNR sont particulièrement utiles pour identifier des personnes présentant un risque potentiel[(2)].

(2) The Passenger Name Record Framework Decision, Report with evidence*, House of Lords, European Union Committee, 11 juin 2008, Minutes of evidence, page 23.*

I. LES COLLECTES DE DONNEES RELATIVES AUX PASSAGERS AERIENS EN FRANCE

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 APIS) sont destinées au fichier des passagers aériens et, enfin, le cadre juridique permettant la collecte des données PNR a été créé en 2006.

A. 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.

Comme le rappelait notre collègue Alain Marsaud dans son rapport n° 2681 du 22 novembre 2005 sur le projet de loi relatif à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, 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

Comme l'indiquent nos collègues Eric Diard et Julien Dray dans leur rapport n° 683 du 5 février 2008 sur la mise en application de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme, l'utilisation du fichier national transfrontière demeure ciblée.

Seuls les vols à destination ou en provenance d'un nombre très limité de pays ont été concernés par l'automatisation du fichier. La CNIL reçoit la liste des pays concernés. Elle a ainsi reçu en mars 2007 une liste de 30 pays mais ce sont cinq destinations qui ont été surveillées jusqu'ici avec un objectif d'extension à 30 en 2009, selon les informations transmises au rapporteur.

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).

Ainsi que l'indiquaient les rapporteurs, « *l'avantage pour les services de lutte contre le terrorisme de disposer de ces données en temps réel est d'établir avec certitude l'arrivée d'une personne surveillée sur le territoire. Ces services ont donc commencé à s'équiper informatiquement afin d'avoir accès à ce traitement de données alimenté depuis février 2007. La DST, qui est principalement concernée, est ainsi reliée au système depuis décembre 2007.* »

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 œuvre un régime de transfert des données APIS des compagnies aériennes vers les autorités répressives sur demande de ces dernières. Elle a été adoptée afin de lutter plus efficacement contre l'immigration clandestine et d'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, ce qui brouille la compréhension des finalités de la mesure.

Les données sont transférées sur demande des Etats, ce qui constitue une différence importante avec le régime de collecte systématique envisagé pour les données PNR.

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).

Les transmissions de données APIS ne sont pour l'instant appliquées que de manière ciblée pour un petit nombre de pays qui ne sont concernés que par les liaisons aériennes.

S'agissant donc du transport aérien, le fichier des passagers aériens a été créé par l'article 7 de la loi du 23 janvier 2006. Ne sont pas concernés les vols en provenance ou à destination des pays membres de l'Union européenne.

Ce fichier regroupe les données collectées par les compagnies aériennes lors de l'enregistrement. Il s'agit des données dites APIS : *Advance passenger information system.* Elles recouvrent les données biographiques (nom, prénom, date de naissance, nationalité, sexe) et relatives au document de voyage (type et numéro). En outre, dans la transmission globale sur le vol se retrouvent le code de transport (numéro du vol et code du transporteur aérien), les heures de départ et d'arrivée, le point d'embarquement et le nombre total de personnes transportées.

Les données APIS ne sont pas collectées par les autorités de contrôle aux frontières mais par le personnel des compagnies aériennes. Les données sont recueillies pour des personnes dont on est certain qu'elles vont bien prendre le vol et sont disponibles peu avant l'embarquement.

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.

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).

Il appartient aux transporteurs de recueillir et de transférer leurs données au ministère de l'intérieur. 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 nouveau fichier peut théoriquement concerner l'ensemble des destinations mais se concentre également sur cinq pays à titre expérimental. Il est alimenté depuis mai 2007 par les données relatives aux passagers présents sur les aéroports de Roissy Charles de Gaulle, Orly et Marseille Marignane.

Les données sont envoyées par les compagnies aériennes à la société internationale de télécommunication aéronautique (SITA) qui les transmet au poste de la police aux frontières de Roissy (décret n° 2006-1630 du 30 décembre 2006).

C'est ensuite au ministère de l'intérieur (site de Lognes) que sont réalisées les interconnexions avec le fichier des personnes recherchées et le système d'information Schengen. Si la mention « connu » ressort du croisement, 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, le fichier connaît une montée en charge progressive. Les principales difficultés rencontrées, comme le soulignaient les rapporteurs Eric Diard et Julien Dray dans leur rapport sur la mise en application de la loi relative à la lutte contre le terrorisme, sont, outre le coût de ce type de dispositif, la seule prise en compte des vols directs (à l'exclusion des vols avec escale) et la question de la saisie des noms par le personnel des compagnies aériennes (avec notamment les problèmes liés à la transcription des noms à partir d'une langue dont l'alphabet n'est pas l'alphabet latin).

Le présent fichier est en place à titre expérimental pour une durée de deux ans (venue à échéance en décembre 2008,) et un arrêté de prorogation doit être publié tout prochainement.

Actuellement, une réflexion est engagée sur la nécessité de conserver en France deux types de fichiers pour les mêmes pays sensibles.

B. La France s'est dotée d'un cadre juridique mais ne procède pas à la collecte des données des dossiers passagers (PNR)

La France n'a pas mis en œuvre de régime de collecte des données des dossiers passagers, compte tenu de la présentation de la présente décision-cadre par la Commission européenne le 6 novembre 2007.

Néanmoins, 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 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* »[(3)] (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) ;

---

(3) Le I de l'article 8 de la loi relative à l'informatique, aux fichiers et aux libertés pose le principe de l'interdiction de la collecte de données dites « sensibles » : « il est interdit de collecter ou de traiter des données à caractère personnel 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. *»*

– 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.

Bien que le cadre juridique existe, aucun système de traitement n'a été mis en place, dans l'attente de l'adoption de la décision-cadre européenne.

II. LES COLLECTES DE DONNEES DES DOSSIERS PASSAGERS A DES FINS REPRESSIVES A L'ETRANGER

Depuis une dizaine d'années, la montée en charge des dispositifs de collecte des données PNR à des fins répressives est évidente. Trois accords ont été signés par l'Union européenne avec les Etats-Unis, le Canada et l'Australie. D'autres pays manifestent un intérêt pour les données PNR sans toutefois avoir créé de régime de collecte.

A. Les accords signés entre l'Union européenne et des pays tiers relatifs aux échanges de données des dossiers passagers

1. Le système PNR américain : un « accord » préoccupant

C'est à la suite des attentats du 11 septembre que les Etats-Unis ont imposé aux compagnies aériennes de communiquer aux douanes et aux services de la sécurité intérieure les données PNR des passagers des vols à destination ou au départ des Etats-Unis.

Les transferts de données sont actuellement régis par l'accord entre l'Union européenne et les Etats-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure (DHS) de juillet 2007 (JO L 204 du 4 août 2007).

Cet accord devait être réévalué au cours de la présidence française mais devrait finalement l'être au cours du premier semestre 2009.

Cet accord a suscité de nombreuses critiques du Parlement européen, des assemblées françaises et des autorités de contrôle (contrôleur européen de la protection des données, CNIL et groupe dit de l'article 29 regroupant la CNIL et ses homologues européennes).

Bien que constituant un progrès relatif en comparaison de l'accord précédent du 19 octobre 2006, le texte présente de graves imperfections, les principales étant les suivantes :

– l'accord prend la forme d'un échange de lettres et n'est pas contraignant ;

– les finalités du transfert sont très larges (lutter contre le terrorisme et la criminalité connexe, prévenir et combattre les infractions graves qui sont de nature

transnationale et empêcher que des personnes se soustraient aux mandats et mesures de détention provisoire émis à leur encontre pour ces infractions. Il est également prévu que les données puissent être traitées au cas par cas pour la protection des intérêts vitaux de la personne ou d'autres personnes ou en cas de risque important pour la santé publique ;

– c'est à la discrétion du DHS que celui-ci peut transférer les données PNR à d'autres autorités gouvernementales exerçant des fonctions de répression, de sécurité publique ou de lutte contre le terrorisme ;

– le DHS a accès, dans des circonstances exceptionnelles, aux données sensibles (pouvant révéler l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou les données relatives à la santé) ;

– les données sont conservées pendant une période de sept ans sur une base de données dite active et 8 ans supplémentaires sur une base de données dite dormante, soit 15 années au total.

Cet accord a été le fruit de négociations très difficiles, les Etats-Unis considérant notamment au départ qu'il n'était pas nécessaire de passer un accord avec l'Union pour appliquer leur loi sur leur territoire. L'enjeu principal pour l'Union était d'assurer certaines garanties en matière de protection des données (le bénéfice de la loi américaine sur la protection de la vie privée s'appliquant théoriquement aux ressortissants européens sur la base de la décision prise par le DHS. Néanmoins, la loi américaine n'a jamais été modifiée en ce sens. La protection promise apparaît donc tout à fait douteuse).

La Délégation pour l'Union européenne de l'Assemblée nationale, saisie du projet d'accord avait adopté les conclusions suivantes au cours de sa réunion du 18 juillet 2007 :

« *La Délégation,*

Vu l'article 88-4 de la Constitution,

Vu le projet d'accord sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure (E 3568),

Vu la proposition de décision du Conseil relative à la signature, au nom de l'Union européenne, d'un accord entre l'Union européenne et les Etats-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure (E 3575),

1. prend acte, qu'au terme de négociations difficiles, les autorités américaines et l'Union européenne sont parvenues à un accord, propre à permettre la mise en place d'un cadre juridique stable ;

2. constate que les autorités américaines ont accepté d'introduire quelques améliorations, ayant notamment pour effet d'accroître les droits garantis aux passagers européens ;

3. déplore que les déclarations d'engagement des autorités américaines ne figurent pas dans le corps même de l'accord ;

4. s'inquiète de l'utilisation rendue possible, dans certains cas, de données sensibles et des risques attachés au partage des données recueillies avec d'autres autorités gouvernementales américaines ainsi qu'avec des pays tiers ;

5. déplore, dès lors, que les nombreuses et les graves imperfections que recèle l'accord, comme la durée excessive de conservation des données collectées, puissent réduire la portée des améliorations qu'il comporte ;

6. demande, avec insistance, que, conformément aux conclusions adoptées par la Délégation lors de la précédente législature, le Gouvernement fasse usage de la réserve prévue par l'article 24, paragraphe 5, du traité sur l'Union européenne, de telle sorte que le Parlement puisse donner son approbation, lorsqu'un accord conclu sur la base de l'article 24 du traité sur l'Union européenne pose des questions majeures dans les domaines politique et juridique ;

7. demande aux autorités françaises d'obtenir que :

a) soit supprimée la dernière phrase de l'accord, selon laquelle la version anglaise prévaudrait en cas de divergence d'interprétation ;

b) la Commission, dans une déclaration, précise les modalités selon lesquelles se déroulera l'évaluation annuelle des conditions d'application de l'accord, afin qu'un large débat puisse s'engager au sein des instances communautaires et des parlements nationaux ».

L'accord prévoit que les versions établies dans les langues autres que la langue anglaise font également foi et l'évaluation prévue en 2008 a été reportée à mars 2009 suite aux élections américaines. De très nombreuses questions demeurent en suspens et devront faire l'objet d'un examen approfondi dans, faut-il espérer, de bonnes conditions.

La politique américaine de « *no fly list* » a été à l'origine de nombre de polémiques sur les données PNR à partir desquelles cette liste est constituée. La *no fly list* regroupe les noms des personnes qui ne sont pas autorisées à monter à bord d'un avion en provenance ou à destination des Etats-Unis. Michael Chertoff, ministre de la sécurité intérieure, a indiqué en octobre 2008 que 2.500 personnes

figuraient sur la *no fly list*, dont 10 % de citoyens américains. Par ailleurs, 16.000 personnes figureraient sur la liste des « *selectees* » (*Secondary Security Screening Selection*) et seraient soumises à des obligations de contrôle et de fouille des bagages renforcées, tout en étant autorisées à voler. Les principaux problèmes soulevés par les listes sont les homonymies, qui ont abouti à une multiplication des incidents. Un nouveau système de surveillance devant parer aux difficultés actuelles a été annoncé en application duquel il serait demandé aux personnes de donner leur nom complet, leur date de naissance et leur genre lorsqu'elles effectuent une réservation.

M. Alex Türk, président de la commission nationale de l'informatique et des libertés, auditionné par la Commission le 25 novembre 2008, a estimé :

« […] *les sujets délicats ne manquent pas dans les relations de l'Europe avec les Etats-Unis.*

Le premier, ce sont évidemment les PNR. Par exemple, la durée de conservation des données des passagers des compagnies aériennes européennes est, à mes yeux, très excessive car elle atteint quinze ans. Autre exemple : les autorités américaines n'ont jamais pu, ou voulu, communiquer la liste des autorités américaines destinataires des données en question. Or le territoire fédéral n'abrite pas moins de 18 000 autorités susceptibles de l'être. Nous pensons aussi que les références – une trentaine – qui sont exigées des passagers vont trop loin : avec qui vous êtes allé à tel endroit, pour quel motif, ce que vous avez mangé à bord… Les autorités de contrôle européennes sont en porte-à-faux complet, car la réaction de l'exécutif européen a été de s'aligner, au lieu de limiter les prétentions américaines. »

2. Les accords signés avec le Canada et l'Australie sont plus équilibrés

➢ Suite aux attentats du 11 septembre 2001, le Canada a mis en place une législation permettant à l'agence des services frontaliers du Canada (ASFC) de recueillir les données APIS et PNR pour les passagers à destination du Canada. Le recueil des données a été mis en œuvre progressivement et, à partir de février 2005, un régime de pénalités en cas de non respect de leurs obligations par les compagnies aériennes a été institué.

L'Union européenne disposait d'une dérogation jusqu'au 1er juillet 2005 avant la conclusion d'un accord avec le Canada permettant de s'assurer

notamment du respect de la directive 95/46 CE du 24 octobre 1995 relative à la protection des données à caractère personnel[4].

Les données sont transférées dans le seul but de prévenir et combattre le terrorisme, 25 rubriques de données PNR sont concernées (contre 34 dans les accords précédemment conclus avec les Etats-Unis), les droits d'accès, de rectification et d'opposition reconnus par le droit canadien aux résidents canadiens sont étendus aux européens dont les données sont conservées par l'ASFC. Le commissariat canadien à la protection de la vie privée peut examiner les plaintes qui lui sont adressées par les autorités de contrôle nationales (la CNIL en France) au nom d'un particulier estimant que sa plainte n'a pas été traitée de manière satisfaisante par l'ASFC. Les données sont transférées par les compagnies aériennes selon la méthode d'exportation « *push* ». La durée de conservation est limitée à trois ans et demi. Pendant 72 heures, toutes les informations APIS/PNR sont accessibles uniquement à un nombre limité d'agents de l'ASFC et d'agents des services de renseignement. Puis les données sont dépersonnalisées pendant deux ans, à moins qu'il ne soit nécessaire d'avoir accès à un nom pour les besoins d'une enquête. Puis, pendant la période de deux ans à trois ans et demi, les données ne sont conservées que de façon dépersonnalisée (les données pouvant être personnalisées à nouveau uniquement avec l'autorisation du président de l'ASFC).

Les autorités françaises et européennes avaient estimé, lors de la signature de l'accord euro canadien le 3 octobre 2005[5], que la plupart de leurs demandes avaient été satisfaites et que l'ensemble de l'accord était plus équilibré que l'accord signé avec les Etats-Unis quelques mois plus tôt.

➢ L'accord avec l'Australie[6] est également plus satisfaisant que celui applicable aux vols vers les Etats-Unis. Les données sont traitées aux fins de lutter contre le terrorisme et la criminalité connexe, prévenir et combattre les infractions graves qui sont de nature transnationale et empêcher que des personnes se soustraient aux mandats et mesures de détention provisoire émis à leur encontre pour ces infractions. Ces finalités sont les mêmes que celles prévues par l'accord avec les Etats-Unis. Il est également prévu que les données puissent être traitées au cas par cas pour la protection des intérêts vitaux de la personne ou d'autres personnes ou en cas de risque important pour la santé publique, ce qui suscite des réserves.

---

(4) 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.

(5) JOUE L 82/15 du 21 mars 2006.

(6) Décision du Conseil 2008/651/PESC/JAI du 30 juin 2008 relative à la signature, au nom de l'Union européenne, d'un accord entre l'Union européenne et l'Australie sur le traitement et le transfert de données des dossiers passagers (données PNR) provenant de l'Union européenne par les transporteurs aériens au service des douanes australien.

Les données sont communiquées au service des douanes.

L'accès aux données des transporteurs se fait aujourd'hui selon la méthode de la lecture seule (*read only*) sans possibilité de conservation des données ou de croisement de fichiers.

Après une période transitoire de deux ans, un système dit *push* serait créé, permettant aux transporteurs aériens d'exporter leurs données vers les autorités compétentes. Les données sensibles seront filtrées par les douanes et supprimées sans autre traitement. Les données seront conservées par les douanes pendant une durée de trois ans et demi au maximum, puis pourront être archivées pendant deux ans. Une fois les données archivées, il ne sera possible d'y avoir accès qu'au cas par cas à des fins d'enquête.

Les personnes concernées bénéficient des dispositions des lois australiennes relatives à la protection de la vie privée. La liste des autorités du gouvernement australien auxquelles les douanes pourraient transmettre les données en provenance de l'Union européenne, au cas par cas et après examen de la demande, est fixée dans l'annexe à l'accord, les transferts ne pouvant se faire qu'en vue de remplir les objectifs qui fondent cet accord.

Selon les informations transmises au rapporteur, la Corée du Sud souhaite également qu'un accord PNR soit signé avec l'Union européenne.

B. Les régimes de collecte des données PNR mis en place dans les pays membres de l'Union

➢ Le Royaume-Uni est l'Etat membre ayant le plus avancé dans la mise en œuvre d'un régime de collecte et de traitement des données PNR. Dans un premier temps, un projet pilote dit « *Semaphore* » a été créé en 2005 afin de déterminer l'utilité d'utiliser à la fois les données APIS disponibles à l'enregistrement et les données PNR collectées au stade de la réservation commerciale. Selon les autorités britanniques, cette double collecte a permis l'arrestation de 1.300 personnes pour crime, le débarquement de passagers non autorisés à pénétrer le territoire et de nombreuses saisies de faux documents et produits stupéfiants. Fin 2007, le projet avait permis de couvrir 38 millions de mouvements de passagers et généré 17.000 alertes. Une personne sur douze interrogée à partir de ces alertes a été arrêtée[(7)].

Les dernières données communiquées au rapporteur font état de 31.000 alertes et 2.600 arrestations.

---

(7) The Passenger Name Record Framework Decision, Report with evidence*, House of Lords, European Union Committee, 11 juin 2008, Minutes of evidence, page 9.*

Le projet *e-borders*, qui a pris la suite du programme *Semaphore,* est entré en vigueur en mars 2008 et connaît une progression rapide. Il devrait couvrir, s'agissant des données APIS, 100 millions de mouvements de passagers d'ici avril 2009 et 95 % des mouvements de passagers au Royaume Uni d'ici 2010, avec un but de couverture totale en 2014.

En revanche, s'agissant des données PNR, le Royaume-Uni a fait le choix de se concentrer sur certains itinéraires et destinations et collecte aujourd'hui les données de manière encore relativement sélective. Il vise une collecte sur 100 millions de mouvements de passagers en 2014 (pour 200 millions de mouvements de passagers traversant les frontières britanniques recensés en 2006).

La législation britannique permet la collecte de données PNR à des fins larges de police, de lutte contre le terrorisme, de lutte contre l'immigration illégale et à des fins douanières. Tous les vols, y compris les vols intra européens, sont théoriquement concernés par la collecte ainsi que tous les moyens de transport.

Les données sont collectées par le *Joint border operation center* (JBOC) dont le personnel est composé de policiers, de douaniers et d'agents de l'administration de l'immigration. Il procède à l'analyse des données collectées puis avertit les autorités compétentes par un système d'alerte.

La durée de conservation des données est de dix ans.

➢ Au Danemark, un cadre juridique pour un régime de collecte et de traitement des données PNR existe depuis 2006. Les données APIS et PNR seraient collectées par les compagnies aériennes et conservées pendant un an. Elles ne seraient accessibles qu'aux services de renseignement (secret intelligence service) et à des fins de lutte antiterroriste.

Néanmoins, comme en France, dans l'attente de l'adoption de la décision-cadre relative à l'utilisation des données PNR à des fins répressives, aucune mesure n'a été mise en œuvre.

Les autorités danoises souhaitent aujourd'hui que la décision-cadre permette de viser la criminalité grave et d'ouvrir l'accès aux autorités de police.

➢ En Belgique, les autorités de police peuvent, sous certaines conditions, et dans le cadre d'une autorisation judiciaire donnée par le parquet, demander aux compagnies aériennes un accès à leurs données PNR.

Enfin, d'autres pays, tels que la Suède, l'Espagne, l'Italie ou encore l'Estonie réfléchissent à ce type de dispositif selon les informations transmises au rapporteur.

SECONDE PARTIE :
LA PROPOSITION DE DECISION-CADRE

I. LES AVIS DU CONTROLEUR EUROPEEN DE LA PROTECTION DES DONNEES, DU « G29 », DE L'AGENCE EUROPEENNE DES DROITS FONDAMENTAUX ET DU PARLEMENT EUROPEEN

De manière résumée, la proposition de décision cadre institue une obligation de transmission des données des dossiers passagers, avant le décollage des vols en provenance ou à destination des pays tiers, des compagnies aériennes vers des unités de renseignements passagers, autorités publiques qui seraient créées dans chaque Etat membre. Ces unités auraient la charge d'effectuer en temps réel des analyses de risque sur la base de critères élaborés par les services opérationnels et de transmettre à ces derniers les résultats des analyses de risque. Les unités de renseignements passagers auraient également la charge de la conservation et de la protection des données PNR sur une durée restant à définir afin de répondre au cas par cas à des besoins d'enquête et de poursuite. La collecte et le traitement de ces données seraient réservés à la lutte contre le terrorisme et certaines formes graves de criminalité.

Il convient de souligner que l'avis très négatif du contrôleur européen de la protection des données, celui du G29 ainsi que celui de l'agence européenne des droits fondamentaux ont été rendus sur la base de la proposition initiale de la Commission européenne qui était, nous le verrons, très insuffisante. Nombre des observations formulées ont depuis trouvé une réponse adaptée.

A. L'avis très critique du contrôleur européen de la protection des données

Dans son avis sur la proposition de décision-cadre du 20 décembre 2007 et publié au Journal officiel de l'Union européenne le 1er mai 2005, suite à une demande de la part de la Commission européenne, le contrôleur européen de la protection des données, M. Peter Hustinx, a formulé un grand nombre de très sérieuses réserves sur la proposition initiale.

Interrogé par le rapporteur le 26 janvier 2009, le contrôleur européen a estimé que cet avis était le plus négatif qu'il ait eu à formuler. Selon lui, ce texte est l'exemple même d'un projet présenté trop tôt alors que le débat était loin d'être mûr. Les travaux organisés par la présidence française ont eu le mérite de

progresser d'un point de vue politique sur les grandes orientations du texte car le débat technique s'était enlisé.

Les critiques de fond du contrôleur sont sévères.

Une des finalités poursuivies par la mesure est de procéder à des évaluations de risque des personnes pour identifier les personnes qui sont ou qui pourraient être impliquées dans une infraction terroriste ou la criminalité grave ainsi que leurs associés. L'élaboration d'indicateurs de risques et de modèles de déplacement et de comportement constitue un aspect central dispositif et nécessite la conservation des données.

Selon le contrôleur, le profilage peut être défini comme « *une méthode informatisée ayant recours à des procédés de fouille de données* (data mining) *sur des entrepôts de données* (data warehouse) *permettant ou devant permettre de classer avec une certaine probabilité et donc avec un certain taux d'erreur induit un individu dans une catégorie particulière afin de prendre des décisions individuelles à son égard* » (définition tirée d'une étude récente du Conseil de l'Europe sur le profilage). La définition de la notion de profilage fait encore l'objet de discussions. Quoi qu'il en soit, le contrôleur européen s'est dit très préoccupé que des décisions concernant des personnes puissent être prises à partir de modèles et de critères établis en faisant appel aux données relatives à l'ensemble des passagers. Il est extrêmement difficile pour les particuliers de se défendre contre de telles décisions et cela constitue un sujet d'inquiétude majeur.

Sur cette question, les travaux de la présidence française ont permis de progresser : les données sensibles ne seraient jamais utilisées dans le cadre des analyses de risques. La proposition initiale prévoyait déjà qu'aucune décision concernant un passager ne pourrait avoir de caractère automatique fondé sur une seule analyse de risque effectuée informatiquement. Toute analyse de risque ferait l'objet d'une expertise par les services opérationnels compétents qui sont les seuls aptes à prendre une décision opérationnelle.

Selon le contrôleur, la nécessité des mesures envisagées est loin d'être démontrée. Aucun chiffre précis ni aucune analyse des régimes existants n'a été fournie. S'il est fait mention de « *nombreuses arrestations* » dans le cadre du système Sémaphore au Royaume Uni, aucune donnée précise n'est fournie sur le programme américain. En conséquence, en l'absence de toute évaluation sérieuse, l'adoption d'un système PNR européen est injustifiée.

La proportionnalité de la mesure aux fins poursuivies est un élément essentiel. Or, en l'état actuel des informations transmises, selon le contrôleur, il ne peut pas être considéré que le régime PNR répond aux critères de proportionnalité. Il s'agit en effet d'investigations proactives effectuées à une échelle sans précédent qui s'appliquent à tous les passagers, que ceux-ci aient ou non quelque chose à se reprocher, et pouvant déboucher sur des mesures répressives.

« *Au vu de ce qui précède, le CEPD tire au sujet de la légitimité des mesures proposées les conclusions ci-après. Accumuler les bases de données sans disposer d'une vision globale des résultats concrets et des lacunes :*

- est contraire à une politique législative rationnelle dans le cadre de laquelle il n'y a pas lieu d'adopter de nouveaux instruments tant que les instruments existants n'ont pas été pleinement mis en oeuvre et que leur insuffisance n'a pas été démontrée,

- pourrait ouvrir la voie à une évolution vers une société de surveillance totale. »

Le droit applicable en matière de protection des données s'avère, dans la proposition initiale de la Commission européenne, totalement insatisfaisant. S'il est fait référence à la décision-cadre relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale[8], il n'apparaît pas clairement dans quelle mesure cette décision-cadre peut effectivement s'appliquer au traitement des données PNR.

Plusieurs problèmes se posent aux différentes étapes du traitement des données :

– les données utilisées par les compagnies aériennes dans le cadre de leur exploitation commerciale ainsi que par les intermédiaires aériens (SITA ou Amadeus) auxquels elles confient la gestion de fichiers sont soumises aux règles de protection de la directive de 1995 ;

– quelle serait ensuite la protection qui s'applique aux données lors de leur transmission par les intermédiaires aux unités de renseignements passagers ?

– quelle protection s'appliquerait au sein de l'unité de renseignements passagers ?

– quel régime serait applicable à la transmission de données analysées entre l'unité de renseignements passagers et les services opérationnels puis au sein des services opérationnels ?

– quelles protections sont prévues pour les échanges entre Etats membres, d'une part, et avec des Etats tiers, d'autre part ?

– comment les personnes concernées pourront-elles exercer leur droit d'accès, leur droit de rectification, d'effacement et de verrouillage des données ainsi que leur droit à réparation et au recours juridictionnel ? Le préambule de la proposition de décision-cadre indique que ces droits sont ceux prévus par la

(8) Décision-cadre 2008/977/JAI du Conseil 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.

décision-cadre relative à la protection des données. Néanmoins, ce seul renvoi ne constitue pas un cadre juridique sécurisé. En premier lieu, vers qui la personne serait-elle amenée à se retourner ? Les droits applicables dans le troisième pilier sont différents de ceux qui prévalent dans le premier pilier. Faut-il considérer que les personnes doivent se retourner vers les unités de renseignements passagers, dont on ne sait pas si elles constituent des services répressifs ? Enfin, comment sera réglée la situation dans laquelle les données d'une personne seront transmises à plusieurs Etats (cas d'un vol avec escale ou bien d'une unité de renseignements passagers commune à plusieurs Etats). Ce sont autant d'éléments qui démontrent la vacuité du régime de protection prévu initialement.

La décision-cadre du 27 novembre 2008 a un champ d'application restreint. En effet, elle s'applique aux données collectées et traitées par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquête et de poursuites en la matière et d'exécution de sanctions pénales. Mais elle se limite aux données échangées entre Etats membres et à leur transmission ultérieure à des pays tiers.

En conséquence, la seule référence à la décision-cadre de 2008 ne peut suffire à assurer la sécurité juridique du régime de protection des données PNR.

A ce sujet, les personnes auditionnées par le rapporteur le 7 janvier et le 14 janvier 2009, ont indiqué que, si toutes ces questions n'ont pas encore trouvé de réponse totalement finalisée, il est possible de bâtir un régime de protection juridique sur les bases suivantes :

– la transmission entre les compagnies ou intermédiaires aériens et les unités de renseignements passagers devrait, en toute logique, bénéficier de la même protection que celle qui s'applique aux échanges de données PNR dans le cadre des activités commerciales des compagnies aériennes. Il faut éviter que les acteurs privés doivent, selon les finalités pour lesquelles ils conservent les données (fins commerciales ou transmission aux unités de renseignements passagers à des fins répressives), appliquer deux régimes de protection distincts pour le même type de données. Néanmoins, une simple référence à la directive de 1995 pose de sérieuses interrogations dans la mesure où elle ne s'applique qu'au premier pilier communautaire. La question se pose de savoir s'il sera nécessaire d'inscrire dans la décision-cadre un régime de protection calqué sur celui de la directive de 1995 ;

– une fois entre les mains des unités de renseignements passagers, un régime de protection spécifique, qui sera détaillé ci-après, s'appliquerait. Une fois les données transférées sous forme d'analyses aux autorités opérationnelles, le droit national s'applique ;

– les échanges de données PNR entre Etats membres susceptibles de se faire au cas par cas seront, quant à eux, bien encadrés par la décision-cadre de 2008 relative à la protection des données dans le troisième pilier (le détail des mesures prévues sera exposé ci-après) ;

– les échanges de données avec des pays tiers devraient également être soumis à la décision-cadre de 2008, à une réserve majeure près : il est expressément prévu que le régime de protection qu'elle institue ne prime par sur les accords internationaux en vigueur en la matière.

Le contrôleur européen de la protection des données remet en cause le manque flagrant de précisions quant à la qualité des destinataires des données (intermédiaires, unités de renseignements passagers ou autorités compétentes).

Le contrôleur estime également que les conditions de communication des données à des pays tiers ne sont pas suffisamment encadrées. La proposition de décision-cadre prévoit que la décision-cadre relative à la protection des données dans le troisième pilier soit applicable, définit la limitation de la finalité des transferts et indique que l'accord de l'Etat membre d'origine est nécessaire à des transferts ultérieurs. Le transfert devrait également se faire dans le respect de la législation nationale de l'Etat membre concerné et de tout accord international applicable. La décision-cadre relative à la protection des données prévoit un certain nombre de garanties : limitation de la finalité, qualité des destinataires, accord de l'Etat membre et principe d'adéquation du niveau de protection assuré dans l'Etat destinataire. Cependant, elle prévoit un grand nombre de dérogations à ces conditions de transmission et il conviendra de s'assurer que les exceptions très larges prévues par la décision-cadre de 2008 ne priment par sur les garanties applicables en cas de transferts de données PNR.

En ce qui concerne les pays avec lesquels l'Union européenne a signé des accords d'échanges de données PNR, les conditions d'accès aux données sont plus souples et les données ne font pas l'objet d'une sélection avant d'être transmises à ces pays tiers. Dans ces conditions, quel serait l'impact des verrous posés dans la décision-cadre relative à l'utilisation des données PNR à des fins répressives en matière d'échanges avec des pays tiers ? Le contrôleur européen regrette le manque de clarté de la proposition sur ce point déterminant et estime « *qu'il est de la plus haute importance que les conditions de la transmission des données PNR à des pays tiers soient cohérentes et soumises à un niveau harmonisé de protection.* »

B. L'avis du G29

Le groupe de travail des autorités européennes de protection des données (dit « G29 ») et le groupe de travail sur la police et la justice ont rendu **un avis commun sur la proposition initiale de la Commission européenne** en décembre 2007 (respectivement les 5 et 18 décembre).

Selon cet avis, qui porte sur la proposition initiale de la Commission européenne, « *les points litigieux relatifs à la protection des données soulevés par cette proposition peuvent* […] *se résumer comme suit :*

1. la proposition ne justifie aucunement qu'il y ait un besoin urgent de collecter des données autres que les données API ;

2. la quantité de données à caractère personnel à transférer par les transporteurs aériens est excessive ;

3. le filtrage des données sensibles devrait être effectué par le responsable du traitement des données ;

4. la méthode « push *» devrait s'appliquer à tous les transporteurs aériens ;*

5. la durée de conservation des données est disproportionnée ;

6. le régime de protection des données est totalement insatisfaisant: les droits des personnes concernées et les obligations des responsables du traitement ne sont mentionnés nulle part ;

7. le large pouvoir d'appréciation laissé aux Etats membres risque de conduire à des interprétations différentes de la décision-cadre ;

8. le régime de protection des données transférées ultérieurement à des pays tiers est vague. »

Selon le G29, l'urgence sociale de la collecte et de l'analyse des données PNR à des fins de prévention et de lutte contre le terrorisme n'a pas été justifiée. L'évaluation de la nécessité et de la proportionnalité de la proposition est impossible, dans la mesure où trop peu d'éléments d'information ont été fournis. Il n'a pas été prouvé qu'un nouvel instrument soit indispensable. Par ailleurs, la liste des rubriques de données collectées apparaît excessive et n'est nullement justifiée dans la proposition. Les dispositions en matière de données sensibles et de protection des données sont inacceptables en l'état. Les informations aux personnes concernées ainsi que les modalités pratiques du droit d'accès sont insuffisantes.

M. Alex Türk, président de la CNIL, auditionné le 25 novembre 2008 par la Commission chargée des affaires européennes, a indiqué que :

« *S'agissant des PNR, nous voudrions concilier les exigences de la sécurité et le respect des droits individuels en établissant des durées de conservation courtes, en définissant précisément la liste des destinataires et en précisant l'usage des données. Nous étions contre le traitement américain du problème. Maintenant que l'Europe s'y met, nous espérons que ce seront des PNR à l'européenne, reflet du droit communautaire, plutôt qu'une imitation du*

système américain. Nous serons plus forts vis-à-vis des Américains si nous leur démontrons qu'il est possible d'assurer la sécurité du transport aérien sans aller aussi loin qu'eux. »

C. L'Agence européenne des droits fondamentaux

Invitée par la présidence française à émettre un avis sur cette proposition de décision-cadre, l'agence européenne des droits fondamentaux a remis son avis en octobre 2008.

L'Agence a examiné la conformité de la proposition aux dispositions de l'article 8 de la Convention européenne des droits de l'homme(9) et à l'article 7 de la Charte européenne des droits fondamentaux(10).

Elle estime que la proposition de décision-cadre contient des définitions imprécises et ouvertes qui ne doivent pas être utilisées (crime organisé, associés…). Les utilisations de profils pour trier les données ont pour conséquence qu'il est impossible pour un individu de savoir exactement quel usage sera fait de ses données. Or, les opérations de traitement doivent être très précises car une définition légale stricte constitue une garantie essentielle contre l'arbitraire, arbitraire pouvant encore être renforcé dans le cadre de mesures de surveillance secrètes.

S'agissant de la proportionnalité, l'Agence estime elle aussi que les informations sont très parcellaires et imprécises. Or, la démonstration claire de la valeur ajoutée et de la nécessité de la collecte des données PNR pour les fins poursuivies doit encore être faite avant toute intervention du législateur. Elle demande, comme le contrôleur européen de la protection des données et le G29, que soit très précisément examinée l'articulation d'un régime de collecte des données PNR avec les instruments existants (système d'information Schengen, système d'information sur les visas).

L'Agence a également examiné le texte au regard du droit à la protection des données personnelles (article 8 de la Charte européenne des droits

---

*(9) « **Article 8 - Droit au respect de la vie privée et familiale** :*

***1.** Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.*

***2.** Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »*

*(10) « **Article 7 - Respect de la vie privée et familiale** : Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications. »*

fondamentaux)[11]. Elle conclut que les dispositions prévues dans la proposition de décision-cadre ne sont pas suffisantes, notamment du fait des incertitudes quant à l'application de la directive de 1995 relative au premier pilier et à la décision-cadre de 2008 relative au troisième pilier. Les simples renvois qui sont prévus dans le texte initial ne sauraient constituer un cadre juridique adapté. Suite à ces critiques et à celles du contrôleur européen de la protection des données, un cadre juridique spécifique à l'utilisation des données dans les unités de renseignements passagers a été introduit.

Enfin, l'Agence a également examiné le texte au regard des risques de discrimination dus à l'utilisation possible des données sensibles. Elle a exprimé des craintes très sérieuses si les données sensibles devaient être utilisées dans le cadre du profilage (notamment s'agissant du respect de l'article 21 de la Charte européenne des droits fondamentaux posant le principe de non discrimination et d'autres instruments internationaux). Le rapporteur rappelle qu'il est exclu que le profilage puisse être fait à partir de données sensibles, et que la dernière version du texte le mentionne expressément.

D. Le Parlement européen ne s'oppose pas par principe à la création d'un régime de collecte et de traitement des données PNR mais estime que les garanties apportées sont insuffisantes

Le Parlement européen a adopté le 20 novembre 2008 une résolution (n° 2008/0561) très réservée sur le projet de décision-cadre, notamment au vu de toutes les incertitudes qui pèsent sur le projet et du manque d'éléments d'informations sur l'utilité de la collecte des données PNR. Le Parlement européen :

« *1. reconnaît la nécessité d'une coopération plus forte, au niveau européen comme international, dans la lutte contre le terrorisme et la grande criminalité; admet que la collecte et le traitement de données puissent être un outil apprécié à des fins répressives ;*

2. est d'avis que les autorités chargées de faire appliquer la loi devraient disposer de tous les outils qui leur sont nécessaires pour mener à bien leurs missions, y compris l'accès aux données; souligne toutefois, puisque de telles mesures ont des effets considérables dans le domaine de la vie privée des citoyens de l'Union, qu'il faut que leur justification en termes de nécessité, de

---

*(11) « **Article 8: Protection des données à caractère personnel***

***1.** Toute personne a droit à la protection des données à caractère personnel la concernant.*

***2**. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.*

***3.** Le respect de ces règles est soumis au contrôle d'une autorité indépendante. »*

proportionnalité et d'utilité en vue de la réalisation de leurs objectifs déclarés soit fournie de manière convaincante et insiste sur la nécessité de mettre en place des garanties efficaces de protection juridique et de respect de la vie privée; estime que c'est là une condition préalable pour conférer la nécessaire légitimité politique à une mesure que les citoyens peuvent considérer comme une intrusion injustifiable dans leur vie privée ;

3. regrette que la formulation et la justification de la proposition de la Commission laissent subsister tant d'incertitudes juridiques quant à sa compatibilité avec la CEDH et la Charte des droits fondamentaux, mais aussi quant à sa base juridique, ce qui n'a pas manqué de poser des questions quant au rôle dévolu au Parlement européen dans la procédure législative; observe que les mêmes inquiétudes concernant l'absence de sécurité juridique de la proposition :

- sont évoquées dans les avis rendus par l'Agence des droits fondamentaux de l'Union européenne (l'Agence des droits fondamentaux), par le contrôleur européen de la protection des données (CEPD) et par le groupe de travail "article 29", ainsi que par le groupe de travail sur la police et la justice,

- requièrent du Conseil qu'il procède à un examen approfondi du champ éventuellement couvert par une future initiative de l'Union en la matière et de son possible impact, et qu'il y incorpore d'importantes quantités d'informations supplémentaires, notamment les avis cités ; […]

5. maintient ses fortes réserves quant à la nécessité et à la valeur ajoutée de la proposition de création d'un système PNR de l'Union et quant aux garanties qui y sont associées, nonobstant les explications et les précisions apportées jusqu'à présent par la Commission et le Conseil, soit par oral, soit par écrit; observe en outre que nombre des questions posées par lui-même, ainsi que par le groupe de travail "article 29", par le groupe de travail sur la police et la justice, par le contrôleur européen de la protection des données et par l'Agence des droits fondamentaux, n'ont pas reçu de réponse satisfaisante ; […]

17. s'inquiète du fait que la proposition, fondamentalement, permette aux autorités répressives d'accéder sans mandat à toutes les données; fait remarquer que la Commission ne démontre pas la nécessité de nouvelles compétences des autorités répressives, ni qu'il est impossible d'atteindre cet objectif au moyen de mesures d'une moins grande portée; critique le fait que la proposition n'indique pas en quoi les compétences des autorités répressives ne sont pas à la hauteur des besoins, ni où et quand les autorités ont à l'évidence été dépourvues des compétences dont elles avaient besoin pour l'objectif fixé; demande qu'une révision des mesures existantes, déjà mentionnées, ait lieu avant que soit développé un système européen d'utilisation des données des dossiers passagers ; […]

21. réaffirme que les données des dossiers passagers peuvent être très utiles comme éléments de preuve accessoires, supplémentaires, dans une enquête

donnée sur des suspects de terrorisme et leurs complices connus; remarque cependant qu'il n'est pas prouvé qu'elles aient un quelconque intérêt pour des recherches automatisées sur une très grande échelle et pour une analyse sur la base de schémas ou de critères de risques (par exemple, établissement de profils ou extraction de connaissances à partir de données) en vue de détecter des terroristes potentiels […]. »

Le Parlement a adopté cette résolution à une écrasante majorité (512 voix pour, 5 contre et 19 abstentions). L'ensemble des points soulevés par le Parlement européen sur les incertitudes en matière de base juridique, la proportionnalité, la définition et l'encadrement des usages des données ainsi que la protection des données devront donc obtenir des réponses.

Cette résolution ne constitue pas son avis officiel sur ce texte qui sera rendu ultérieurement.

Une dernière étude du Parlement européen publiée fin janvier a dressé un bilan des questions posées par le projet européen au regard du respect des droits fondamentaux(12). La Cour européenne des droits de l'homme a, de jurisprudence constante, jugé que les atteintes au respect du droit à la vie privée devaient être strictement nécessaires et proportionnées. Des limitations précises doivent être posées à l'exercice des pouvoirs de mémoriser et d'utiliser les informations. La question de l'accessibilité et de la prévisibilité de la loi est cruciale.

Outre le respect des engagements internationaux se pose la question de la validité des mesures nationales d'application du droit européen au regard des exigences constitutionnelles des Etats membres. A cet égard, l'Allemagne est très réservée sur le projet de régime de collecte des données PNR européen. Un recours a notamment été introduit auprès de la Cour constitutionnelle allemande contre les dispositions nationales d'application de la directive 2006/24/CE(13) prévoyant une obligation de conservation de certaines données par les opérateurs de services de communications électroniques afin que les services répressifs puissent y avoir accès. L'issue de ce contentieux aura des répercussions importantes sur la position de l'Allemagne ainsi que sur le projet de décision cadre.

La convention n° 108 du Conseil de l'Europe du 28 janvier 1981 relative à la protection des personnes à l'égard du traitement automatisé des données constitue le premier instrument international contraignant tendant à

---

(12) Etude du Parlement européen : vers un système PNR européen ? Questions sur la valeur ajoutée et la protection des droits fondamentaux, Evelien Brouwer, janvier 2009.

(13) Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications.

protéger les personnes contre l'usage abusif des traitements automatisés de données à caractère personnel. La convention a été complétée par une recommandation du Conseil de l'Europe (recommandation n° R (87) 15 du Conseil des ministres du 17 septembre 1987) tendant à réglementer l'utilisation des données à caractère personnel dans le secteur de la police mais cette recommandation n'a pas de valeur contraignante pour les Etats membres. Une référence à ces textes est inscrite dans les considérants de la proposition de décision cadre. La Charte européenne des droits fondamentaux a posé le principe d'un droit à la protection des données. Les principes essentiels à la protection des données devant être pris en considération s'agissant des dossiers passagers sont les suivants selon l'étude du Parlement européen : principe de finalité limitée, interdiction de l'automatisation des décisions, qualité des données, limites dans le temps, droits de la personne à accéder à ses données et à les corriger, supervision par des responsables nationaux et européens de la protection des données, niveau adéquat de protection des données dans les pays tiers et sécurité des données.

En conclusion, il convient de souligner que si le traité de Lisbonne entrait en vigueur avant l'adoption de ce texte, la procédure de codécision serait applicable. C'est pourquoi les travaux menés par le Conseil se sont d'ores et déjà orientés vers une collaboration étroite avec le Parlement européen, ce dont il faut se féliciter.

II. LA PROPOSITION DE DECISION-CADRE EN L'ETAT ACTUEL DES NEGOCIATIONS

La proposition de décision-cadre doit réussir à concilier deux objectifs fondamentaux : la sécurité publique, d'une part, et le respect des droits fondamentaux, au premier rang desquels le droit à la vie privée et à la protection des données.

Une majorité d'Etats membres sont convaincus de la nécessité de disposer d'un outil de collecte et de traitement des données des dossiers passagers. Les Etats les plus réservés sont l'Allemagne et l'Autriche.

A. Les finalités poursuivies par la mesure et la question de la base juridique

1. La lutte contre le terrorisme et les formes graves de criminalité

A l'origine, la proposition de décision-cadre présentée par la Commission européenne visait la lutte contre le terrorisme et la lutte contre la criminalité organisée.

Les infractions terroristes entrant dans le champ d'application du texte sont celles définies aux articles 1er à 4 de la décision-cadre 2002/475/JAI du Conseil relative à la lutte contre le terrorisme. La décision-cadre 2008/919/JAI du Conseil du 28 novembre 2008 modifiant la décision-cadre de 2002 devra bien entendu être prise comme référence car elle modifie les articles 3 et 4 du texte de 2002 afin de mieux prendre en compte la provocation publique et le recrutement.

Décision-cadre du Conseil du 13 juin 2002 relative à la lutte contre le terrorisme telle que modifiée par la décision cadre du 28 novembre 2008

Article premier

Infractions terroristes et droits et principes fondamentaux

1. Chaque Etat membre prend les mesures nécessaires pour que soient considérés comme infractions terroristes les actes intentionnels visés aux points a) à i), tels qu'ils sont définis comme infractions par le droit national, qui, par leur nature ou leur contexte, peuvent porter gravement atteinte à un pays ou à une organisation internationale lorsque l'auteur les commet dans le but de :

— gravement intimider une population ou

— contraindre indûment des pouvoirs publics ou une organisation internationale à accomplir ou à

s'abstenir d'accomplir un acte quelconque ou

— gravement déstabiliser ou détruire les structures fondamentales politiques, constitutionnelles, économiques ou sociales d'un pays ou une organisation internationale ;

a) les atteintes contre la vie d'une personne pouvant entraîner la mort ;

b) les atteintes graves à l'intégrité physique d'une personne ;

c) l'enlèvement ou la prise d'otage ;

d) le fait de causer des destructions massives à une installation gouvernementale ou publique, à un système de transport, à une infrastructure, y compris un système informatique, à une plate-forme fixe située sur le plateau continental, à un lieu public ou une propriété privée susceptible de mettre en danger des vies humaines ou de produire des pertes économiques considérables ;

e) la capture d'aéronefs et de navires ou d'autres moyens de transport collectifs ou de marchandises ;

f) la fabrication, la possession, l'acquisition, le transport ou la fourniture ou l'utilisation d'armes à feu, d'explosifs, d'armes nucléaires, biologiques et chimiques ainsi que, pour les armes biologiques et chimiques, la recherche et le développement ;

g) la libération de substances dangereuses, ou la provocation d'incendies, d'inondations ou d'explosions, ayant pour effet de mettre en danger des vies humaines ;

h) la perturbation ou l'interruption de l'approvisionnement en eau, en électricité ou toute autre ressource naturelle fondamentale ayant pour effet de mettre en danger des vies humaines ;

i) la menace de réaliser l'un des comportements énumérés aux points a) à h).

2. La présente décision-cadre ne saurait avoir pour effet de modifier l'obligation de respecter les droits fondamentaux et les principes juridiques fondamentaux tels qu'ils sont consacrés par l'article 6 du traité sur l'Union européenne.

Article 2

Infractions relatives à un groupe terroriste

1. Aux fins de la présente décision-cadre, on entend par «groupe terroriste» l'association structurée, de plus de deux personnes, établie dans le temps, et agissant de façon concertée en vue de commettre des infractions terroristes. Le terme «association structurée» désigne une association qui ne s'est pas constituée au hasard pour commettre immédiatement une infraction et qui n'a pas nécessairement de rôles formellement définis pour ses membres, de continuité dans sa composition ou de structure élaborée.

2. Chaque Etat membre prend les mesures nécessaires pour rendre punissables les actes intentionnels suivants :

a) la direction d'un groupe terroriste ;

b) la participation aux activités d'un groupe terroriste, y compris en fournissant des informations ou des moyens matériels, ou par toute forme de financement de ses activités, en ayant connaissance que cette participation contribuera aux activités criminelles du groupe terroriste.

Article 3

Infractions liées aux activités terroristes

1. Aux fins de la présente décision-cadre, on entend par :

a) “provocation publique à commettre une infraction terroriste”, la diffusion ou toute autre forme de mise à la disposition du public d’un message, avec l’intention d’inciter à la commission d’une des infractions énumérées à l’article 1er, paragraphe 1, points a) à h), lorsqu’un tel comportement, qu’il préconise directement ou non la commission d’infractions terroristes, crée le risque qu’une ou plusieurs de ces infractions puissent être commises ;

b) “recrutement pour le terrorisme”, le fait de solliciter une autre personne pour commettre l’une des infractions énumérées à l’article 1er, paragraphe 1, points a) à h), ou à l’article 2, paragraphe 2 ;

c) “entraînement pour le terrorisme”, le fait de fournir des instructions pour la fabrication ou l’utilisation d’explosifs, d’armes à feu, d’autres armes ou de substances nocives ou dangereuses, ou pour d’autres méthodes ou techniques spécifiques, aux fins de commettre l’une des infractions énumérées à l’article 1er, paragraphe 1, points a) à h), en sachant que la formation dispensée a pour but de servir à la réalisation d’un tel objectif.

2. Chaque Etat membre prend les mesures nécessaires pour que soient également considérés comme des infractions liées aux activités terroristes les actes intentionnels suivants :

a) la provocation publique à commettre une infraction terroriste ;

b) le recrutement pour le terrorisme ;

c) l’entraînement pour le terrorisme ;

d) le vol aggravé en vue de commettre l’une des infractions énumérées à l’article 1er, paragraphe 1 ;

e) le chantage en vue de commettre l’une des infractions énumérées à l’article 1er, paragraphe 1 ;

f) l’établissement de faux documents administratifs en vue de commettre l’une des infractions énumérées à l’article 1er, paragraphe 1, points a) à h), ainsi qu’à l’article 2, paragraphe 2, point b).

3. Pour qu’un acte soit punissable comme le prévoit le paragraphe 2, il n’est pas nécessaire qu’une infraction terroriste soit effectivement commise.»

Article 4

Complicité, incitation et tentative

1. Chaque Etat membre prend les mesures nécessaires pour que soit rendu punissable le fait de se rendre complice d’une infraction visée à l’article 1er, paragraphe 1, et aux articles 2 ou 3.

2. Chaque Etat membre prend les mesures nécessaires pour que soit rendu punissable le fait d’inciter à commettre une infraction visée à l’article 1er, paragraphe 1, à l’article 2 ou à l’article 3, paragraphe 2, points d) à f).

3. Chaque Etat membre prend les mesures nécessaires pour que soit rendu punissable le fait de tenter de commettre une infraction visée à l’article 1er, paragraphe 1, et à l’article 3, paragraphe 2, points d) à f), à l’exclusion de la possession prévue à l’article 1er, paragraphe 1, point f), et de l’infraction visée à l’article 1er, paragraphe 1, point i).

4. Chaque Etat membre peut décider de prendre les mesures nécessaires pour que soit rendu punissable le fait de tenter de commettre une infraction visée à l'article 3, paragraphe 2, points b) et c).»

Il est vite apparu que la finalité de lutte contre la criminalité organisée posait problème dans la mesure où il n'est pas possible de déterminer, au moment du traitement des données PNR, si l'on a affaire à une criminalité organisée. Les négociations menées sous présidence française ont abouti au rejet de la notion de criminalité organisée au profit de celle de « criminalité grave » telle que définie dans la liste des 32 infractions graves du mandat d'arrêt européen.

L'article 2 de la décision-cadre du Conseil du 13 juin 2002, relative au mandat d'arrêt européen et aux procédures de remise entre Etats membres, définit les infractions pour lesquelles la double incrimination par l'Etat requis n'a pas à être vérifiée :

« 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'Etat 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'Etat 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'Etat 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 oeuvres 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. »

Les finalités visées par l'instrument sont donc définies en référence à des textes existants.

Par ailleurs, il ne sera pas possible d'imposer à un Etat membre de se limiter aux fins visées par l'instrument européen dans l'élaboration de sa législation nationale, voire, en ce qui concerne le Royaume Uni, de revenir sur les pouvoirs dont disposent déjà les autorités répressives dans l'utilisation des données PNR. Les Etats membres conservent donc, en cohérence avec les dispositions du traité sur l'Union européenne, le droit d'élargir les finalités de cet outil.

Le Royaume-Uni utilise les données PNR à des fins douanières ou d'immigration et la France a prévu d'utiliser les données PNR à des fins de lutte contre l'immigration illégale dans le cadre juridique adopté en 2006.

Bien que ceci constitue une limite à l'effort d'harmonisation souhaité par le texte, le rapporteur estime que laisser une marge de manœuvre aux Etats ne remet pas en cause l'intérêt de la décision-cadre.

2. La question de la base juridique du texte fait débat

La question de savoir quelle est la base juridique dans les traités européens appropriée à la proposition de décision-cadre présentée par la Commission européenne est épineuse et n'a pas encore été tranchée.

Il n'est notamment pas évident que la proposition de décision-cadre entre, dans son ensemble, dans le champ de la coopération policière et judiciaire en matière pénale (troisième pilier).

Dans sa proposition de décision-cadre la Commission européenne propose de se fonder sur l'article 29, l'article 30, premier paragraphe, point b), et l'article 34, deuxième paragraphe, point b) du traité sur l'Union européenne. Mais faut-il considérer que la collecte des données PNR puis leur transmission aux unités d'informations passagers nationales afin de les mettre à disposition des

autorités répressives constituent réellement une coopération plus étroite entre les forces de police ou les autorités douanières des Etats membres ou une coopération plus étroite entre les autorités judiciaires des Etats membres ?

En outre, en application de l'article 29 du traité sur l'Union européenne cité plus haut, et de l'article 47 du traité sur l'Union européenne, l'Union exerce ses compétences législatives sans préjudice des compétences de la Communauté européenne et sans porter atteinte aux compétences que le traité CE confère à la Communauté.

Au cours des discussions sur le projet de décision-cadre, il est apparu que certaines dispositions de la proposition (obligations s'imposant aux transporteurs aériens) pourraient en fait relever des compétences communautaires (article 80 du traité CE sur la politique commune des transports) et que, si la Communauté s'avérait être compétente, cela exclurait toute action de l'Union.

C'est bien une directive communautaire qui avait institué l'obligation de prévoir la mise à disposition des données APIS afin de lutter contre l'immigration illégale et d'améliorer les contrôles aux frontières (directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers). En conséquence, elle était logiquement fondée sur les articles 62 et 63 du traité CE (article 62, point 2, relatif au franchissement des frontières extérieures et article 63, point 3, b), relatif aux mesures prises dans le cadre de la politique sur l'immigration clandestine).

La directive 2006/24/CE[(14)], qui impose aux Etats membres de prendre les mesures par lesquelles les fournisseurs de services de télécommunications conservent les données des télécommunications pendant une durée de 6 mois à 2 ans pour permettre aux autorités répressives d'y avoir accès dans certaines conditions, a été adoptée sur la base de l'article 95 du traité CE relatif aux mesures tendant « *au rapprochement des dispositions législatives, réglementaires et administratives des Etats membres qui ont pour objet l'établissement et le fonctionnement du marché intérieur* ». Cependant, un des objectifs de la directive était de faciliter l'exercice de leurs obligations par les fournisseurs de services de télécommunications car ils étaient confrontés à des législations nationales divergentes qui constituaient un problème dans leur activité commerciale.

Néanmoins, il faut bien remarquer que dans le cas présent, les données PNR ne sont pas conservées par les opérateurs et accessibles ensuite aux autorités répressives. Il ne s'agit pas d'une mesure de conservation mais bien de collecter

(14) Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications.

des données sur lesquelles des analyses de risques seront effectuées et devant notamment avoir une utilité dans le cadre de mesures proactives de la police et des autorités douanières.

Le contrôleur européen à la protection des données, dans son avis sur le projet de proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (*Passenger Name Record* — PNR) à des fins répressives, « *remet en question le fait même qu'un instrument relevant du troisième pilier crée des obligations légales de routine à des fins répressives, pour des acteurs du secteur privé ou public qui ne relèvent pas, en principe, de la coopération entre services répressifs*. »

Il convient de rappeler que dans les affaires relatives aux accords passés en matière de données PNR avec les Etats-Unis fondés sur l'article 95 du traité instituant la Communauté européenne, la CJCE a jugé que le traité CE n'était pas la base juridique appropriée, lu en combinaison avec la directive de 1995 sur la protection des données. Le transfert de données PNR au bureau des douanes et de la protection des frontières des Etats-Unis «*constitue des opérations de traitement concernant la sécurité publique et [les] activités de l'Etat en matière pénale*»(15). L'accord signé ultérieurement avec les Etats-Unis (accord PNR 2007) a été fondé sur les articles 24 et 38 du traité sur l'Union européenne.

Le rapporteur estime, compte tenu de ces éléments, que le doute principal tient aux articles instituant l'obligation pour les transporteurs aériens de transmettre leurs données PNR aux unités d'informations passagers. Il pense qu'il serait regrettable et absurde de devoir adopter deux instruments différents et que les dispositions constituent bien un ensemble cohérent visant la lutte contre le terrorisme et certaines formes graves de criminalité.

Par ailleurs, il convient de noter que l'Irlande a introduit un recours contre la directive 2006/24/CE sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications. Elle estime que « *le choix de l'article 95* [du traité CE] *comme base juridique de la directive* […] *est une erreur fondamentale. L'Irlande soutient en outre que ni l'article 95 du traité ni aucune autre des dispositions du traité ne sont susceptibles de fournir une base juridique appropriée à la directive. L'Irlande prétend principalement que l'unique objectif ou, subsidiairement, l'objectif principal ou prédominant de la directive est de faciliter la recherche, la détection et la poursuite d'infractions graves, y compris en matière de terrorisme* »(16).

(15) Arrêt de la Cour de justice du 30 mai 2006 dans les affaires jointes Parlement européen contre Conseil (C‑317/04) et contre Commission (C‑318/04).

(16) Recours introduit le 6 juillet 2006 — Irlande/Conseil de l'Union européenne, Parlement européen (Affaire C-301/06).

Dans ses conclusions, l'avocat général propose à la Cour de rejeter le recours, estimant que c'est à bon droit que la directive a été fondée sur le traité CE. « *A cet égard, l'avocat général souligne que les mesures prévues par la directive n'impliquent aucune intervention directe des autorités répressives des Etats membres. La directive contient des mesures qui se situent à un stade antérieur à la mise en oeuvre éventuelle d'une action de coopération policière et judiciaire en matière pénale. Elle n'harmonise ni la question de l'accès aux données par les autorités nationales compétentes en matière répressive ni celle relative à l'utilisation et à l'échange de ces données entre ces autorités, par exemple dans le cadre d'enquêtes criminelles. Ces questions, qui relèvent, à son avis, du domaine couvert par la coopération policière et judiciaire en matière pénale, ont été à juste titre exclues des dispositions de la directive* »[(17)].

La CJCE ne s'est pas encore prononcée. De tels arguments pourraient plaider en faveur de la base juridique choisie pour la proposition de décision-cadre relative aux données PNR, dans la mesure où il s'agit bien d'harmoniser les conditions dans lesquelles les autorités répressives ont accès aux données, les utilisent et les échangent au sein de l'Union ou avec des Etats tiers.

B. De l'utilité des données PNR

Il convient ici de détailler l'utilisation pratique qui sera faite au plan opérationnel des données PNR. Deux grands types d'utilisation doivent être distingués :

– l'utilisation « traditionnelle » à partir des données conservées dans une banque de données afin de procéder à des vérifications pour des enquêtes (recherche d'un individu disparu ou en fuite, vérifications de la présence dans un pays sensible, confirmation ou infirmation d'un alibi dans le cadre des procédures judiciaires). Par ailleurs, l'intérêt de la conservation des données s'explique également par la possibilité de mener, ce qui constituerait une nouveauté, des analyses sur le long terme et de dégager des critères de ciblage des passagers à risque en fonction des données passées analysées ;

– l'utilisation en temps réel, suite à une analyse de risque effectuée sur les passagers d'un vol, et pouvant induire des conduites policières proactives principalement au moment du passage de la frontière par le voyageur (interpellation, contrôle approfondi, mise en place d'une surveillance).

L'ensemble des instances ayant eu à émettre un avis sur le projet de PNR a souligné la nécessité de disposer d'éléments concrets permettant de conclure à l'utilité réelle des données PNR avant la mise en oeuvre d'un système de collecte et de traitement aussi massif.

---

(17) Communiqué de presse n° 70/08 du 14 octobre 2008.

S'il est certain qu'en matière de lutte contre le terrorisme et les formes graves de criminalité, beaucoup d'éléments ne peuvent pas être portés sur la place publique, les indications fournies dans la proposition de décision-cadre initiale peuvent laisser le lecteur perplexe. L'exposé des motifs précise que « *l'UE a pu tirer parti de l'expérience acquise par ces pays tiers* [ayant mis en place un système PNR] *dans l'utilisation des données PNR et elle a également bénéficié de l'expérience du Royaume-Uni avec son projet pilote. Plus spécifiquement, en deux ans de fonctionnement de son projet pilote, le Royaume-Uni a pu opérer de nombreuses arrestations, identifier des réseaux de traite d'êtres humains et obtenir de précieux renseignements concernant le terrorisme.* »

Le rapporteur a déjà cité plus haut les chiffres des arrestations liés à l'utilisation des données PNR au Royaume Uni.

Afin de justifier la collecte des données PNR alors qu'il existe déjà une obligation de collecte des données APIS à des fins de lutte contre l'immigration illégale, l'exposé des motifs indique que « *les données API sont des données officielles, puisqu'elles proviennent des passeports, et suffisamment précises en ce qui concerne l'identité d'une personne. En revanche, les données PNR contiennent plus éléments et sont disponibles avant les données API. Ces éléments sont très importants pour procéder à des évaluations de risques des personnes, pour obtenir des informations et pour établir des liens entre des personnes connues et des personnes inconnues.* »

Mme Michèle Alliot-Marie, ministre de l'intérieur, de l'outre-mer et des collectivités territoriales a indiqué, lors de son audition par la Commission le 3 décembre 2008 :

« *Autre moyen de détection précoce, le PNR permet un contrôle aux frontières aériennes à partir des données des compagnies aériennes sur leurs passagers et un suivi des déplacements des personnes signalées comme susceptibles d'avoir des liens avec le terrorisme – c'est le cas, par exemple, lorsque certaines personnes résidant sur notre territoire effectuent un séjour au Pakistan, en Afghanistan ou en Irak. En sériant les problèmes, la présidence française a permis de lever les blocages de plusieurs pays à ce sujet. Les inquiétudes portaient notamment sur la protection des données personnelles et sur le gigantisme du système ; certains voulaient que les vols intracommunautaires soient exclus, d'autres objectaient que ce serait risquer de perdre la trace de certaines personnes.*

Nous disposons de plusieurs précédents démontrant l'utilité d'un PNR. Ainsi, en octobre 2007, les services britanniques sont parvenus à démanteler un réseau en recherchant avec qui les deux personnes qu'ils avaient identifiées voyageaient régulièrement. »

Les travaux menés sous présidence française ont permis d'avancer sur la question de l'utilité réelle des données PNR dans les pays dans lesquels elles

sont collectées. Les autorités répressives du Royaume-Uni, de la Belgique et de la France ont été entendues ainsi que celle des Etats-Unis.

Il ressort notamment de l'audition de la douane française que de 60 à 80 % des saisies de stupéfiants sur les aéroports de Roissy et d'Orly sont réalisées grâce aux données PNR.

Interrogé à ce sujet lors de l'audition du 7 janvier 2009, M. Gérard Schoen, sous directeur des affaires juridiques, du contentieux, des contrôles et de la lutte contre la fraude à la direction générale des douanes, a confirmé que les statistiques établies sur les 10 dernières années permettent de conclure que sur ces aéroports, de 60 à 80 % des produits stupéfiants saisis sur les passagers (à titre d'illustration, ce sont deux tonnes de stupéfiants qui sont saisies chaque année à Roissy) le sont grâce à l'utilisation des données PNR.

A l'heure actuelle, en effet, les douanes procèdent à quatre types de contrôle pour rechercher des produits stupéfiants, des armes ou des produits contrefaits :

– le contrôle à 100 % des passagers d'un avion, ce type de contrôle étant absolument exceptionnel car il bloque l'ensemble des passagers pour une demi-journée et nécessite des moyens humains considérables ;

– le contrôle de routine faisant suite à quelques questions posées par le douanier, qui est marginal ;

– le contrôle sur profilage en fonction de l'attitude d'une personne ;

– le contrôle ciblé grâce à l'utilisation des données des dossiers passagers. En effet, les douanes, s'appuyant sur l'article 65 du code des douanes, ont la possibilité de demander aux compagnies aériennes de leur transmettre des données PNR. Les compagnies peuvent refuser, auquel cas une procédure civile peut théoriquement être entamée. Dans la pratique, il est parfois difficile d'obtenir des renseignements de certaines compagnies aériennes, soit qu'elles fassent preuve de mauvaise volonté, soit qu'elles ne soient pas au niveau d'un point de vue informatique.

Malgré cette utilisation relativement restreinte des données PNR, leur efficacité est démontrée selon les services des douanes françaises.

Les services de police ont également fait part de leur très grand intérêt pour les données PNR. Par rapport aux données APIS, les données PNR sont beaucoup plus nombreuses et de nature très différente. Elles ont un champ bien plus vaste et constituent objectivement des données très utiles pour les services. Elles sont intéressantes à la fois en amont de l'arrivée de l'avion afin d'anticiper les mesures à prendre mais également *a posteriori* à des fins d'enquête ou afin d'établir des critères de ciblage. Ce sont des données essentielles afin d'établir des

liens entre criminels connus et inconnus et pour évaluer les risques liés à une personne.

Il a été souligné que les données PNR permettent également d'innocenter des personnes lorsqu'elles sont utilisées dans le cadre d'enquêtes.

L'avantage des données PNR pour l'ensemble des passagers a été avancé sur la base de l'expérience du Royaume-Uni. En effet, dans la mesure où ces données permettent de mieux cibler les contrôles, les contrôles réalisés sur l'immense majorité des passagers s'en trouvent nettement allégés.

Cependant, certaines faiblesses des données PNR (qui sont saisies par des opérateurs privés, génèrent des risques d'homonymie, sont sujettes à modification et concernent avant l'embarquement des personnes dont on ne peut être sûr qu'elles vont bien prendre l'avion) ont également amené les autorités opérationnelles à conclure à la nécessité de pouvoir croiser ces données :

– d'une part avec les données APIS qui permettent d'identifier des terroristes et criminels connus grâce à des systèmes d'alerte et sont des données officielles issues des documents d'identité qui permettent d'éliminer les problèmes d'homonymie grâce à la date de naissance ;

– d'autre part avec les fichiers nationaux des personnes recherchées et le système d'information Schengen.

Les croisements ne devraient pas être systématiques mais concerner uniquement les personnes ou les vols étant ressortis des analyses effectuées par les unités de renseignements passagers. Les autorités françaises estiment que le croisement ciblé constituerait un outil important. Néanmoins, au niveau européen, aucun accord n'a été trouvé à ce jour sur l'encadrement du croisement. Faudrait-il le limiter à une personne sélectionnée dans le cadre des analyses PNR ou pourrait-on l'étendre à un vol ? Cette question devra être tranchée. Il n'est en revanche aucunement question de croiser l'ensemble des données, étant entendu que l'ensemble des données ne seraient de toute façon jamais soumises à analyse de la part des unités de renseignements passagers, à la fois parce que cela est impossible matériellement et parce que cela ne présente aucun intérêt pour les services.

Le rapporteur souligne que, si une possibilité de croisement était instituée, les autorités pourraient vérifier dans la base SIS ou dans un fichier national des personnes recherchées si une personne ayant fait l'objet d'une analyse au titre des données PNR figure dans un autre fichier. Il ne s'agirait en aucun cas d'alimenter le fichier SIS qui, rappelons-le, peut permettre aux Etats membres de refuser l'accès à leur territoire d'un ressortissant de pays tiers, à partir des analyses faites sur les données PNR par les unités de renseignements passagers.

Enfin, il est nécessaire de répondre à une critique formulée à de multiples reprises par les autorités de protection des données ainsi que par le

Parlement européen : dans quelle mesure cet instrument est-il ou non redondant avec les autres instruments et fichiers existant au niveau européen et qui n'ont d'ailleurs, pour la plupart, pas encore fait l'objet d'évaluations ?

Il convient de souligner que la proposition de décision-cadre n'institue pas un fichier « européen » : elle se contente d'harmoniser la manière dont les données PNR sont transmises aux Etats membres et dont elles sont collectées et traitées par ces derniers à des fins répressives.

Les instruments existant au niveau européen sont les suivants :

– 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 œuvre un régime de transfert des données APIS des compagnies aériennes vers les autorités répressives sur demande de ces dernières. Elle a été adoptée afin de lutter plus efficacement contre l'immigration clandestine et d'améliorer les contrôles aux frontières ;

– Eurodac : le système Eurodac créé en 2000 permet aux Etats membres d'identifier les demandeurs d'asile ainsi que les personnes ayant été appréhendées dans le contexte d'un franchissement irrégulier d'une frontière extérieure de la Communauté. En comparant les empreintes, les Etats membres peuvent vérifier si un demandeur d'asile ou un ressortissant étranger se trouvant illégalement sur son territoire a déjà formulé une demande dans un autre Etat membre ou si un demandeur d'asile est entré irrégulièrement sur le territoire de l'Union. Il se compose d'une unité centrale gérée par la Commission européenne, d'une base de données centrale informatisée d'empreintes digitales et de moyens électroniques de transmission entre les Etats membres et la base de données centrale ;

– Système d'information Schengen (SIS) : le SIS, créé par la Convention d'application de l'Accord de Schengen du 19 juin 1990, est un fichier commun à l'ensemble des Etats membres de « l'espace Schengen », qui a pour objet de centraliser et de faciliter l'échange d'informations détenues par les services chargés de missions de police afin de préserver l'ordre et la sécurité publics. Le SIS comporte deux grandes catégories d'informations : les personnes recherchées, placées sous surveillance ou jugées « indésirables » dans « l'espace Schengen » et les véhicules ou objets recherchés. La modernisation du SIS et la création d'un système de deuxième génération, intégrant notamment les données biométriques, rencontrent de grandes difficultés et ont été repoussées à maintes reprises ;

– le système d'information sur les visas (VIS) (en cours de mise en œuvre) : il améliore la mise en œuvre de la politique commune en matière de visas, la coopération consulaire et la consultation des autorités consulaires centrales, dans le but de prévenir les menaces pesant sur la sécurité intérieure des Etats membres, faciliter la lutte contre la fraude documentaire, faciliter les contrôles aux points de passage aux frontières extérieures et contribuer au retour

des personnes en situation irrégulière. Sont enregistrées dans le VIS les données alphanumériques sur le demandeur et sur les visas demandés, délivrés, refusés, annulés, retirés ou prorogés, les photographies digitales et les données biométriques ;

– le traité de Prüm tend à approfondir la coopération transfrontalière policière dans les domaines de la lutte contre le terrorisme, la criminalité organisée et la migration illégale. Le traité permet notamment les échanges d'informations en matière de profils ADN, de données dactyloscopiques (empreintes digitales) et de registres d'immatriculation des véhicules ;

– par ailleurs, la Commission européenne a proposé l'institution d'un régime de facilitation des contrôles aux frontières sans intervention des gardes frontières pour les voyageurs de bonne foi s'étant préalablement « enregistrés » ainsi que la création d'un système d'enregistrement des entrées et des sorties des ressortissants de pays tiers afin d'identifier les personnes dépassant la durée de séjour autorisée.

Ces brèves descriptions démontrent que l'objet de la collecte des données PNR n'est pas couvert par d'autres instruments européens, qui ont trait à la lutte contre l'immigration irrégulière, aux contrôles aux frontières ou à la coopération policière dans le cadre d'enquêtes et dont aucun ne regroupe les données très spécifiques comprises dans un dossier passager ni ne permet de disposer des données aussi en amont d'un déplacement aérien.

C. Quels déplacements viser ?

1. Les vols entrant dans le champ de la collecte de données

Un consensus a été atteint pour limiter le champ d'application de la décision-cadre européenne au transport aérien. Cette orientation n'empêcherait toutefois pas les Etats membres qui le souhaitent d'utiliser les données disponibles dans le cadre d'autres modes de transport (le Royaume-Uni ayant, à titre d'exemple, un système de collecte des données sur les passagers transportés par voie maritime ou ferroviaire).

Dès lors qu'il a été acté que la proposition de décision-cadre se concentre sur le mode de transport aérien, la première étape a consisté à définir les vols qui seraient inclus dans le champ d'application de la mesure.

Il est possible d'inclure ou d'exclure les vols intracommunautaires. Les principaux arguments en faveur de l'inclusion des vols intracommunautaires sont les suivants[18] :

– le fait que certains Etats membres exploitent les données PNR des vols intracommunautaires (Royaume Uni) ;

– le fait que les services de lutte anti-terroriste aient avancé l'intérêt de ces données ;

– pour les Etats membres principalement desservis par des vols intracommunautaires, l'outil PNR perd beaucoup de sa valeur ajoutée si l'on exclut ces vols.

S'agissant de l'exclusion des vols intracommunautaires de l'instrument, les arguments favorables étaient les suivants :

– le nombre restreint d'Etats favorables à ce que soient inclus dans le champ de la décision-cadre les vols intracommunautaires ;

– l'aggravation de la charge financière pesant sur les compagnies (même si cet argument doit être relativisé comme nous le verrons plus loin) et le fait qu'existe un risque de distorsion de la concurrence par rapport aux modes de transport concurrents (maritime et ferroviaire) ;

– de réelles questions sur la proportionnalité d'une telle mesure, avec le nombre de collectes qu'elle implique, par rapport aux objectifs poursuivis (lutte contre le terrorisme et certaines formes graves de criminalité) ;

– la possibilité ultérieure d'étendre, en cas de besoin, l'instrument aux vols intracommunautaires.

Les débats conduits notamment sous présidence française ont permis d'apporter une réponse et il a été décidé que les vols vers ou en provenance d'un pays tiers seraient visés par la proposition de décision-cadre. Ces trajets incluent les éventuels segments intracommunautaires (passagers en transit).

Dans le cas des passagers en transit, la transmission des données se ferait vers l'Etat concerné par le vol extracommunautaire ainsi que vers le ou les Etats concernés par un segment intracommunautaire.

Les organisations de transporteurs aériens ont fait valoir que, l'unité de transmission étant le vol, il ne serait pas envisageable, sur un vol intra européen, de distinguer entre les personnes en transit et les autres. Les intermédiaires (qui

---

(18) Note de la présidence, groupe multidisciplinaire contre la criminalité organisée, 13286/08, 22 septembre 2008.

gèrent le plus souvent les dossiers passagers pour les compagnies) ont quant à eux estimé que cela était techniquement possible.

Par ailleurs, la faculté de requérir les données PNR sur les vols intracommunautaires devrait être laissée ouverte aux Etats membres par la proposition de décision-cadre, en application de la législation nationale.

Ce dernier point a suscité de nombreux débats mais est apparu à la présidence française comme la seule piste viable d'élaboration d'un système de collecte des données PNR en Europe. Revenir, par cet instrument, sur les pouvoirs dont bénéficient les autorités répressives dans certains Etats membres est apparu impossible ou susceptible de bloquer l'avancement des travaux sur ce texte.

Le rapporteur est favorable à cette limitation, au moins dans un premier temps, sous réserve que cela soit techniquement opérationnel et sans préjudice d'un réexamen futur sur ce point si cela devait s'avérer nécessaire.

Il convient de noter que les vols charter et les taxis aériens qui ne figuraient pas dans la proposition initiale sont inclus dans le champ de la décision-cadre dans sa version du 23 janvier. A l'heure actuelle, beaucoup de ces transporteurs n'ont pas de dossiers passagers. Il ne leur serait pas imposé d'en constituer mais, s'ils devaient s'en doter un jour, alors ils seraient bien couverts par la décision cadre au même titre que les autres compagnies.

2. Quel type de collecte prévoir : une collecte sélective ou systématique sur les vols concernés par la proposition de décision-cadre ?

Le Royaume Uni dispose actuellement d'un système de collecte des données PNR sélectif et centré sur les « routes » jugées à risques. Il a, au cours des débats, souhaité qu'une approche sélective de l'obligation de transmission soit adoptée, ce qui réduirait les coûts et serait davantage proportionné aux objectifs.

Néanmoins, il est apparu qu'une route dangereuse ou à risques pour un Etat ne l'est pas pour un autre et que la limitation à certains vols sélectionnés sur la base de critères nationaux fait perdre beaucoup de son intérêt à la mesure. Les données non recueillies par un Etat pourraient ensuite manquer à un autre Etat dans le cadre des échanges de données entre Etats membres.

Par ailleurs, s'agissant des transporteurs aériens, des règles de collecte différenciées selon les Etats posent des problèmes pratiques et complexifient les échanges. L'harmonisation recherchée par la décision-cadre serait dès lors très limitée.

Ce sont donc l'ensemble des vols entrant dans le champ de la mesure qui feraient l'objet d'une transmission.

D. Les données collectées et le sort des données sensibles

La proposition de décision-cadre élaborée par la Commission européenne a dressé la liste suivante des données en annexe :

ANNEXE

Données PNR au sens de l'article 2

Données pour tous les passagers

1) Code repère 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 coordonnées (numéro de téléphone, adresse électronique)

6) Moyens de paiement, y compris l'adresse de facturation

7) Itinéraire complet pour le dossier passager concerné

8) Informations "grands voyageurs"

9) Agence de voyage/agent de voyage

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

11) Informations "PNR scindé/divisé"

12) Remarques générales (y compris toute information disponible concernant les mineurs de moins de dix-huit ans non accompagnés, telle que le nom et le sexe du mineur, son âge, la/les langue(s) parlée(s), le nom et les coordonnées de l'accompagnateur au départ et à l'arrivée et le lien avec le mineur, l'agent au départ et à l'arrivée

13) Etablissement des billets (numéro du billet, date d'émission, allers simples, données ATFQ - *Automated Ticket Fare Quote*)

14) Numéro de siège et autres informations concernant le siège

15) Informations sur le partage de code

16) Informations relatives aux bagages

17) Nombre et autres noms de voyageurs figurant dans le PNR

18) Toute information API

Historique complet des modifications des PNR énumérées aux points 1 à 18.

En l'état actuel des discussions, il est apparu que les données complémentaires concernant les mineurs non accompagnés ne sont pas nécessaires aux services opérationnels. Il a donc été décidé de supprimer les informations sur les mineurs non accompagnés bien qu'elles apparaissent encore dans la liste. Il conviendra de s'assurer de cette suppression.

Par ailleurs, l'exploitation de certaines informations à caractère sensible qui peuvent éventuellement être saisies dans le dossier PNR d'un passager a fait l'objet de nombreux débats. En l'état actuel du texte, les données sensibles pouvant apparaître notamment sous la rubrique n° 12 « remarques générales » pourraient être utilisées uniquement à des fins d'enquête en cours ou de poursuites déjà engagées afin de prévenir ou de détecter une infraction terroriste ou criminelle grave. Néanmoins, aucun accord n'a été obtenu sur cette question jusqu'à présent. En effet une majorité d'Etats est opposée à ce que les données sensibles puissent être exploitées, quelques Etats (par exemple le Royaume Uni) souhaitant qu'une utilisation au cas par cas à des fins d'enquêtes ou de poursuite puisse être possible.

Mme Michèle Alliot-Marie, ministre de l'intérieur, de l'outre-mer et des collectivités territoriales a indiqué, lors de son audition par la Commission le 3 décembre 2008 :

« *Les principales données qui nous intéressent sont le nom du voyageur, son pays d'origine, le lieu de l'achat du billet et le moyen de paiement utilisé. Ces deux derniers éléments étant particulièrement importants en matière de lutte contre le trafic de stupéfiants : on sait par exemple que l'on doit plus particulièrement surveiller les personnes qui ont acheté leur billet dans la région de Bogota et qui ont payé en liquide ou dans une certaine agence. En revanche, d'autres informations, telles que le régime alimentaire suivi par le passager, ne nous intéressent nullement.* »

Le rapporteur est d'avis que le débat sur ces questions doit être approfondi.

En premier lieu, il faut rappeler que les cas dans lesquels les données sensibles sont susceptibles d'être saisies dans le dossier PNR sont rares. Il s'agira principalement des données saisies dans la rubrique « remarques générales ». Il peut notamment s'agir de demandes particulières ayant trait à la restauration ou à l'état de santé (demande d'un siège particulier ou d'un fauteuil roulant à cause d'une jambe cassée par exemple). Outre cette rubrique « remarques générales », on peut également penser au cas dans lequel un parti politique ou un syndicat ou encore une église effectue la réservation pour une personne puis procède au paiement et peut dans ce cas peut –être apparaître dans le dossier (adresse de facturation ou adresse électronique).

Comme l'a indiqué M. Jonathan Faull, directeur général de la direction générale « Justice liberté et sécurité » à la Commission européenne, au rapporteur,

par le simple fait que l'on doive inscrire dans la décision-cadre relative aux données PNR la définition des données sensibles telle qu'elle existe notamment dans la directive de 1995[19] ou la décision-cadre de 2008[20], la lecture du texte suscite un émoi bien compréhensible. En effet, les données dites sensibles sont les « *données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que* […] *les données relatives à la santé et à la vie sexuelle*. » Or, la quasi totalité de ces données ne figure jamais sur un dossier passager.

En second lieu, il convient de souligner que, si les données sensibles devaient être utilisées, ce ne serait qu'au cas par cas, et aucunement sous la forme d'un traitement de masse. Il est exclu que les données sensibles fassent l'objet du même traitement en masse que les autres.

A l'heure actuelle, deux options sont possibles :

– soit exclure totalement l'utilisation des données sensibles à quelque étape que ce soit. Dans ce cas, il a été acté que la responsabilité du tri entre les données sensibles et les autres ne devrait pas revenir aux compagnies aériennes. Les unités de renseignements passagers seraient chargées de faire le tri ;

– soit permettre une utilisation des données sensibles au cas par cas, dans le cadre de procédures policières et judiciaires bien spécifiques.

La dernière version de la proposition de décision-cadre prévoit que, si des données sensibles devaient pouvoir être exploitées à des fins d'enquête en cours ou de poursuites déjà engagées afin de prévenir ou de détecter une infraction terroriste ou criminelle grave, elles ne le soient que si l'évaluation informatisée du risque a été menée à bien le cas échéant, le traitement est absolument nécessaire aux fins de l'enquête ou des poursuites, le droit interne du pays prévoit des garanties nécessaires (article 11 *bis*). La consultation de ces données serait réservée à certains membres du personnel de l'unité de renseignements passagers et la consultation se ferait selon des procédés manuels.

Le texte interdit qu'un profilage puisse être effectué sur la base des données sensibles, ce qui constitue une garantie fondamentale. Par ailleurs, il est prévu que les autorités opérationnelles compétentes ne prennent aucune décision qui produise des effets juridiques défavorables pour une personne ou qui l'affecte de manière significative au seul motif de la race ou de l'origine ethnique de ladite personne, de ses convictions religieuses ou philosophiques, de ses opinions politiques, de son appartenance à un syndicat, de sa santé ou de son orientation sexuelle.

---

(19) N° 95/46 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.

(20) Décision-cadre n° 2008/977/JAI du Conseil 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.

Le rapporteur insiste pour que l'ensemble des dispositions du texte sur les données sensibles soit complet et cohérent et ne laisse aucune place au doute, quelle que soit l'option retenue.

E. Les aspects concrets des transferts de données

Le groupe multidisciplinaire contre la criminalité organisée a, au cours de ses travaux sous présidence française, auditionné les représentants des principales organisations professionnelles des transporteurs aériens au plan international et européen. Pour les transporteurs, il apparaît nécessaire d'harmoniser la définition des obligations au plan européen quant aux règles de collecte des données. Du point de vue des Etats membres, il est clair que la mise en oeuvre du PNR européen ne doit pas générer de contraintes supplémentaires pour les transporteurs aériens. Il a par ailleurs été souligné que les données collectées au stade de la réservation se limitent à celles fournies par la clientèle sur une base volontaire et ne sont ni vérifiées ni vérifiables par les transporteurs.

Par ailleurs, le nombre de données collectées peut varier en fonction du système de réservation utilisé.

Les lignes directrices de l'OACI sur les données des dossiers passagers d'avril 2006 seront respectées. Ces lignes ont pour objet d'établir des mesures uniformes pour le transfert des données PNR et leur traitement ultérieur par les Etats intéressés.

Le groupe multidisciplinaire contre la criminalité organisée a également auditionné les représentants de deux des plus grandes entreprises parmi celles qui gèrent concrètement les données PNR pour les transporteurs aériens. Il s'agit ici des « intermédiaires » au sens de la proposition de décision-cadre.

Selon eux, pour les besoins d'échanges d'informations commerciales, toute compagnie doit être connectée au réseau informatisé d'un intermédiaire, celui-ci étant capable de transmettre les données PNR aux autorités publiques. En conséquence, il ressort des travaux du groupe multidisciplinaire que les coûts d'investissement liés à la création d'un système propre à chaque compagnie aérienne peuvent être évités et que les coûts de connexion au réseau sont déjà couverts. Il ne faut donc considérer que les coûts supplémentaires liés à la transmission des données PNR aux autorités publiques.

Néanmoins, il ne peut être exclu que certaines compagnies ne soient pas connectées au réseau des intermédiaires. Pour celles-ci se poserait la question de la création d'un système de transmission propre, ce qui parait peu probable car très coûteux, ou de l'adhésion aux services des intermédiaires.

Le coût de la transmission des données d'un dossier passager est évalué, par transmission et par passager, entre dix et vingt centimes d'euro. Il est probable

que le coût des transmissions envisagées soit répercuté sur le prix des billets acquitté par le passager.

Les estimations Eurostat font état, pour l'année 2007, d'un nombre de passagers égal à 244 millions pour des vols entre l'Union européenne et des pays tiers.

Le transfert des données vers les unités de renseignements passagers des Etats membres constituerait une obligation imposée aux transporteurs aériens. Une montée en charge progressive de l'obligation devrait vraisemblablement être prévue dans la proposition de décision-cadre. En l'état actuel du texte, un délai de six ans à compter de l'entrée en vigueur a été proposé avant que l'ensemble des données sur l'ensemble des vols prévus soit effectivement transféré. Avant cette date, les données pourraient n'être collectées que pour les vols considérés comme étant à risque et définis par chaque Etat, cette solution posant des problèmes d'harmonisation importants.

Les Etats membres devraient veiller à ce que des sanctions dissuasives, effectives et proportionnées, y compris d'ordre pécuniaire, soient prévues à l'encontre des transporteurs aériens qui ne transmettraient pas les données requises.

Le mode de transmission des données par les opérateurs aériens devrait être la méthode « *push* », par laquelle ce sont les compagnies ou intermédiaires qui exportent leurs données vers les autorités publiques et non la méthode « *pull* » par laquelle les autorités publiques extraient les données des réseaux des compagnies. La méthode *push* est celle apportant le plus de garanties du point de vue de la sécurité des réseaux et de la protection des données. À titre transitoire, la méthode *pull* pourrait être admise, le temps que les compagnies se mettent techniquement à niveau (une période transitoire de trois ans est proposée dans la dernière version de la proposition de décision-cadre). Pendant cette période transitoire, les unités de renseignements passagers seraient autorisées à extraire les données des bases de données des transporteurs au moyen de la méthode « *pull* ».

Le nombre de transmissions ainsi que le moment auquel elles sont opérées ont également été débattus. Il semble que, en l'état actuel des négociations, l'on s'oriente vers deux transmissions :

– une transmission de 72 à 48 heures avant le vol, afin de permettre une analyse en amont et de faciliter la réactivité des services opérationnels (les données de la réservation pouvant encore être modifiées à ce stade) ;

– une transmission à la clôture de l'embarquement, lorsque les données ne peuvent plus être modifiées et présentent une meilleure fiabilité.

Une faculté d'adaptation pourrait en outre être offerte aux Etats membres, en leur permettant de requérir une transmission supplémentaire face à

une situation particulière d'urgence ou de danger. Là encore, cette faculté d'adaptation laissée aux Etats membres doit être encadrée car elle limite l'harmonisation souhaitée.

Dans sa proposition de décision-cadre, la Commission européenne a souhaité instituer des normes obligatoires de cryptage pour la transmission des données par les compagnies et intermédiaires aux autorités publiques. Mais il s'avère que les données circulent déjà pour les besoins commerciaux entre compagnies aériennes et entre aéroports dans des conditions de sécurité en lien avec l'exploitation commerciale et sans cryptage. Par ailleurs, le coût du cryptage pour les transporteurs aériens et les intermédiaires est extrêmement élevé. En conséquence, compte tenu de ce que les données sont déjà en circulation, il n'a pas été jugé opportun d'imposer un cryptage. Néanmoins, la sécurité des réseaux devrait être vérifiée.

F. Les autorités bénéficiaires des données

Les autorités bénéficiaires des données des dossiers passagers recouvrent deux types d'entités distinctes, ayant des attributions propres et travaillant en étroite collaboration :

– le transfert des données s'effectuerait vers les unités de renseignements passagers créées dans les Etats membres. Ces dernières seraient, en résumé, chargées des manipulations informatiques et de l'analyse des données afin de transmettre aux autorités répressives des analyses ciblées ;

– les autorités répressives, qui seraient définies par les Etats membres en fonction de leur organisation interne et des objectifs fixés par la décision-cadre. Les autorités répressives bénéficieraient des analyses effectuées par les unités de renseignements passagers et seraient également chargées d'établir les critères selon lesquels les unités procèdent au tri parmi les données qu'elles reçoivent et effectuent le profilage.

1. Les unités de renseignements passagers

Il est apparu au cours des négociations que les garanties portant sur les unités de renseignements passagers devaient être largement renforcées par rapport à la proposition initiale de la Commission européenne. En effet, ce sont ces unités qui seront destinataires des données PNR et qui auront la charge de cibler les données intéressantes pour les services opérationnels afin de les leur transmettre.

En premier lieu, un consensus s'est dégagé pour viser, comme le prévoit la Commission européenne dans sa proposition de décision-cadre, un système PNR décentralisé. Ainsi, ne serait pas créée une instance centralisée au niveau européen qui réaliserait les analyses et les transmettrait vers les services

opérationnels des Etats membres. Tant les Etats membres que la Commission européenne étaient hostiles à une telle solution, notamment en raison de la complexité technique de cet outil, des coûts qu'une telle structure générerait (supportés par le budget de l'Union si cette instance était européenne) et des questions soulevées en matière de sécurité des données vu la masse des données à traiter.

Dans chaque Etat membre serait donc créée une unité de renseignements passagers. Cette autorité devra être une autorité publique ou un département d'une autorité publique « *chargé de la collecte des données PNR auprès des compagnies aériennes, de leur conservation, de leur analyse et de la transmission aux autorités compétentes des résultats des analyses.* » L'unité sera la gardienne de la base de données PNR dans chaque Etat ainsi que la garante du respect des règles de collecte et de traitement. Que les unités de renseignements passagers doivent être une autorité publique constitue un point fondamental de la sécurité générale du dispositif pour le rapporteur.

Il n'est pas imaginable que de tels traitements de données puissent être confiés à des entités extérieures. Les traitements seraient réservés à des agents individuellement désignés et spécialement formés à cet outil.

En France, il est probable que l'unité de renseignements passagers soit constituée principalement de policiers et de douaniers informaticiens ainsi que de policiers et de douaniers chargés de faire la liaison avec les services opérationnels.

S'agissant de la situation spécifique des petits Etats membres, il sera possible de créer une unité de renseignements passagers commune à plusieurs Etats membres afin de permettre de mutualiser les moyens.

Les compétences de ces unités de renseignements passagers ont été clarifiées au cours des débats menés sous présidence française. La transparence des attributions est indispensable à la bonne marche d'un régime de collecte des données PNR.

Le rapport rendu par la présidence française le 28 novembre 2008[(21)] a identifié les tâches suivantes pour les unités de renseignements passagers :

– collecte des données auprès des compagnies de transport ;

– analyse, en temps réel, des données PNR afférentes à certains vols présélectionnés, dans le but d'évaluer le risque éventuel présenté par certains passagers ;

---

(21) Conseil de l'Union européenne, Proposition de décision-cadre relative à l'utilisation des données des dossiers passagers à des fins répressives. Bilan des travaux thématiques réalisés de juillet à novembre 2008, *16457/08, 28 novembre 2008.*

– analyse des données, en temps différé, dans le but d'actualiser les indicateurs de risques ;

– analyse de la base de données PNR sur la requête d'une autorité compétente en charge d'une enquête ;

– transmission des résultats des analyses aux autorités compétentes ;

– échanges d'informations avec les unités des autres Etats membres ;

– enregistrement des analyses faites et des résultats obtenus, des requêtes reçues et des transmissions effectuées ;

– stockage des données.

L'article 12 de la proposition énumère les obligations de l'unité de renseignements passagers en matière de sécurité des données : il lui reviendra d'assurer le contrôle de l'accès aux installations, des supports de données, du stockage, des utilisateurs, de l'accès aux données, de la transmission, de l'introduction et du transport des données, d'assurer la restauration en cas d'interruption et de garantir la fiabilité et l'intégrité du système. L'article 11 *nonies* prévoit que les personnes ayant accès aux données PNR ne puissent traiter ces données qu'en application de leur mission au sein de l'unité ou sur instruction de l'unité, sauf obligation légale complémentaire. Les personnes qui travaillent au sein de l'unité seraient soumises à toutes les obligations auxquelles l'unité est soumise. Il est possible qu'un régime de sanctions spécifiques doive être adopté dans les Etats membres pour réprimer la violation des règles de traitement prévues par la décision-cadre.

L'unité de renseignements passagers devra systématiquement assurer la sécurité des données, vérifier la légalité des requêtes reçues, assurer une traçabilité rigoureuse de tous les accès à la base de données, de toutes les analyses et de toutes les transmissions, assurer la rectification des données inexactes ou incomplètes, effacer le résultat des analyses de risque après transmission de ces résultats aux autorités compétentes (à moins que la conversation permette de protéger les intérêts des passagers aériens par l'élimination de faux positifs) et assurer la sécurité des données. Tout accès aux données serait répertorié nominativement (l'article 11 *ter* prévoit une journalisation et une documentation sur toute transmission de données PNR ainsi que sur toute demande des autorités compétentes ou d'une autre unité de renseignements passagers).

Les opérations d'analyse de risque doivent être précisément définies en raison des inquiétudes que suscite le profilage. L'analyse doit permettre d'identifier les passagers susceptibles de présenter un risque, sur la base de critères établis par les autorités opérationnelles, d'être impliqués dans une activité terroriste ou criminelle, indique le rapport final de la présidence française (rapport du 28 novembre). L'article 3 de la proposition de décision-cadre dispose dans sa

dernière rédaction que l'unité traite les données PNR afin d'« *évaluer en temps réel le risque présenté par les passagers afin d'identifier les personnes qui pourraient d'être impliquées dans une infraction terroriste ou dans une forme grave de criminalité et devraient faire l'objet d'un examen plus approfondi par les autorités compétentes de l'Etat membre visées à l'article 4. Lorsqu'elle procède à une telle évaluation du risque, l'unité de renseignements passagers peut traiter les données PNR en les confrontant à des critères de risque prédéterminés et au contenu des bases de données pertinentes, en conformité avec les dispositions européennes, internationales et nationales applicables auxdites bases de données. Lorsque le traitement automatique débouche sur une correspondance positive, celle-ci est vérifiée par l'unité de renseignements passagers selon une procédure manuelle pour déterminer s'il est nécessaire de transmettre ces données à l'autorité compétente visée à l'article 4 en vue de prévenir ou de détecter les infractions terroristes et les formes graves de criminalité ou de procéder à des enquêtes ou à des poursuites en la matière* ».

La détermination des critères de risque auxquels les données passagers pourront être confrontées serait encadrée par le droit national ainsi que par les dispositions suivantes :

– les Etats membres veillent à ce que les critères d'évaluation du risque soient fixés par les autorités compétentes et à ce que ces critères 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, la santé ou l'orientation sexuelle d'une personne (article 3). La question de la nationalité pourrait en outre poser des difficultés et générer des discriminations ;

– les autorités compétentes ne prendront aucune mesure qui produise des effets juridiques défavorables pour une personne ou qui l'affecte de manière significative uniquement en raison du traitement automatisé des données. Une analyse humaine du traitement est obligatoire (article 4) ;

– un comité composé des représentants des Etats membres et présidé par le représentant de la Commission européenne assistera cette dernière et pourra effectuer des recommandations sur l'évaluation du risque (article 14).

Les recoupements avec les données APIS ainsi que les fichiers européens et nationaux de personnes ou d'objets recherchés ou faisant l'objet d'un signalement pas les autorités répressives devrait, dans un second temps, permettre de compléter l'analyse de risque ou d'éliminer certains risques d'erreur.

Comme il a été indiqué, les services opérationnels estiment nécessaires de pouvoir effectuer ces recoupements. Néanmoins, cette question n'a pas été suffisamment débattue au cours des travaux menés jusqu'à présent et aucun accord de principe n'a été obtenu. Le rapporteur estime que les croisements avec le SIS et les fichiers nationaux des personnes recherchées, une fois que les analyses de risque ont été effectuées, constitueraient un outil important.

2. Les autorités publiques opérationnelles

Le rapport rendu par la présidence française le 28 novembre 2008 a identifié les tâches suivantes pour les autorités publiques opérationnelles :

– établissement des critères pour la présélection des vols qui feront l'objet de l'analyse de risque ;

– requêtes à l'unité de renseignements passagers en vue d'analyser les données en temps différé pour l'actualisation des critères de risques ;

– requêtes spécifiques à l'unité de renseignements passagers en vue d'analyser les données PNR dans le cadre d'une enquête nationale déterminée ;

– requêtes spécifiques à l'unité de renseignements passagers en vue d'analyser les données PNR pour répondre à une demande de coopération de la part d'une autorité compétente requérante, réception et retransmission des résultats à ladite autorité ;

– décisions relatives aux actions à prendre en cas d'analyse positive.

Chaque Etat membre devra adopter une liste des autorités compétentes habilitées à demander ou recevoir les données PNR ou les analyses de données PNR de la part des unités de renseignements passagers (article 4 de la proposition de décision-cadre). Cette liste est transmise dans les douze mois suivant l'entrée en vigueur du texte à la Commission européenne et au Conseil. Elle peut faire l'objet d'actualisation.

Le rapporteur estime que cette lite est positive car les données PNR ne doivent être transmises qu'à des autorités limitativement énumérées.

Les autorités compétentes ne comprennent que les autorités des Etats qui sont chargées de prévenir et de détecter les infractions terroristes et les formes graves de criminalité ou de procéder à des enquêtes ou des poursuites en la matière. Elles ne peuvent traiter les données PNR ou les analyses qu'aux fins prévues par la décision-cadre. Cependant, cette restriction ne porte pas atteinte aux pouvoirs de ces autorités dans le cas où d'autres infractions, réelles ou présumées, sont détectées au cours de l'action répressive menée à la suite de ce traitement.

Le transfert de données brutes des unités de renseignements passagers vers les autorités compétentes, qui auront accès aux données et en feront usage en application des législations nationales, n'est pas exclu par la dernière version du texte, ce que le rapporteur juge préoccupant. En effet, l'idée du texte est que ce soient les unités de renseignements passagers qui procèdent aux analyses à partir des données brutes afin de les livrer aux autorités compétentes. Ces dernières ne devraient pas avoir accès aux données brutes en masse, car, dans ces conditions, à quoi bon encadrer sévèrement le fonctionnement des unités de renseignements

passagers ? Les autorités françaises souhaitent également voir les transmissions de données brutes limitées à des cas exceptionnels.

La proposition de décision-cadre devrait être modifiée en ce sens.

Par ailleurs, il est rappelé que les autorités compétentes ne pourraient prendre aucune décision qui produise des effets juridiques défavorables pour une personne ou qui l'affecte de manière significative uniquement en raison du traitement automatisé des données PNR.

G. La durée de conservation

La proposition initiale de la Commission européenne qui, il faut le rappeler, était intervenue peu après la négociation de l'accord PNR avec les Etats-Unis, prévoyait de fixer à 13 ans la durée totale de conservation des données, dont huit années dans une base de données dite inactive.

Après la période initiale de cinq ans, l'accès, le traitement et l'utilisation des données PNR ne pourrait « *se faire qu'avec le consentement de l'autorité compétente et uniquement dans des circonstances exceptionnelles en réponse à une menace ou un risque spécifique et réel dans le cadre de la prévention d'infractions terroristes et de la criminalité organisée ou de la lutte contre ces phénomènes* » (article 9).

A l'expiration du délai de 13 ans, les données devaient être effacées, sauf si elles étaient utilisées dans le cadre d'une enquête criminelle en cours et qui concerne une infraction terroriste ou la criminalité organisée.

Au cours des négociations, il est clairement apparu qu'aucun pays membre ne souhaitait disposer d'une durée de rétention des données de 13 ans. Cette période est en effet bien trop longue et a suscité une opposition unanime, tant de la part des autorités de contrôle que du Parlement européen.

A l'heure actuelle, et bien que ce point n'ait pas fait l'objet d'un accord, il semble que les Etats puissent s'entendre sur une durée de conservation minimum et sur une durée de conservation maximum. Il est tout à fait possible que le texte aboutisse à fixer une fourchette de conservation afin de laisser une marge de manoeuvre aux Etats membres. La durée minimum de conservation pourrait être fixée à trois ans. Une possibilité de conservation supplémentaire de trois à sept années pourrait être accordée. Ainsi, la durée de conservation des données pourrait varier de trois à dix ans selon les pays. Ce sont notamment le Royaume-Uni et le Danemark qui souhaitent une possibilité de conservation maximale de dix ans.

Pour l'instant, l'idée de scinder la période de conservation en deux entre, d'une part, la conservation sur une base de données active et, d'autre part, la

conservation sur une base de données dite inactive, n'a pas fait l'objet d'un accord. Il a été observé que ce type de procédure relève principalement d'une tradition anglo-saxonne. La dernière version du texte de la proposition de décision-cadre prévoit qu'à l'issue d'une période de trois ans, les données PNR soient archivées dans l'unité de renseignements passagers pour une période complémentaire dont la durée resterait à fixer. L'accès à ces données ne serait alors autorisé qu'en réponse à une menace ou un risque spécifique et réel ou dans le cadre d'une enquête et de poursuites spécifiques ou à des fins d'analyse.

Le rapporteur estime que le fait de laisser une certaine marge de manoeuvre aux Etats peut être un élément important permettant d'aboutir à un accord sur le texte. Néanmoins, il observe que la marge laissée entre trois et dix ans est très importante et tend à accréditer l'idée que les Etats ne parviennent pas à se mettre d'accord sur la durée de conservation nécessaire. Or, ceci constitue un élément fondamental de la proportionnalité du dispositif aux objectifs poursuivis.

Il conviendrait donc de réduire la durée possible de conservation à une fourchette de trois à six ans.

H. Autorités de contrôle nationales et droits des personnes concernées

La question du régime de protection applicable au transfert entre compagnies ou intermédiaires et unités de renseignements passagers n'est pas résolue. Le rapporteur estime que la protection devrait être calquée sur celle prévue par la directive de 1995 afin que les compagnies aériennes ou leurs intermédiaires soient soumis à un ensemble de règles uniforme lorsqu'ils manipulent ces données, y compris pour leur transfert vers les unités de renseignements passagers.

S'agissant du traitement des données au sein des unités de renseignements passagers, les droits des particuliers prévus dans la dernière rédaction de la proposition de décision-cadre sont inspirés de la décision-cadre du 27 novembre 2008 relative à la protection des données dans le cadre du troisième pilier.

L'article 11 *quater* de la proposition prévoit une information des passagers par les transporteurs aériens sur les destinataires et les finalités du traitement, les possibilités d'échanges de données, la période de conservation ainsi que sur leurs droits. Il appartiendrait aux Etats de veiller à l'affichage de ces informations dans les aéroports.

L'article 11 *decies* prévoit qu'une ou plusieurs autorités publiques soient chargées de contrôler l'application, sur son territoire, des dispositions adoptées par l'Etat membre en application du chapitre relatif à la protection des données. Ces autorités devraient exercer en toute indépendance les missions dont elles sont investies. Elles disposeraient de pouvoirs d'investigation réels, de

pouvoirs effectifs d'intervention (verrouillage, effacement ou destruction de données, interdiction d'un traitement si nécessaire, saisine des parlements nationaux) et du pouvoir d'ester en justice ou de porter des violations des dispositions nationales à la connaissance de l'autorité judiciaire. Les autorités de contrôle auraient accès aux journaux et à la documentation des transmissions et des demandes conservés par les unités de renseignements passagers pendant cinq années. Chaque autorité de contrôle devra pouvoir être saisie directement par un particulier pour la protection de ses droits et libertés. Les membres et agents des autorités de contrôle devront être liés par les dispositions relatives à la protection des donnés prévues par la décision-cadre. La Commission européenne et le Conseil doivent être informés de l'autorité ou des autorités de contrôle désignées par l'Etat.

Un droit d'accès pour les particuliers serait prévu par l'article 11 *quinquies*. Il concernerait la confirmation, soit de l'unité de renseignements passagers, soit de l'autorité de contrôle nationale, que les données ont ou n'ont pas été transmises à une autorité compétente et, dans la mesure du possible, des informations sur cette autorité, ainsi que la confirmation que les vérifications nécessaires ont bien eu lieu.

Le droit d'accès pourrait être limité dans certains cas, en tenant dûment compte des intérêts de la personne concernée, afin d'éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires, de protéger la sécurité publique, de protéger la sûreté de l'Etat ou de protéger la personne concernée ou les droits et libertés d'autrui.

En cas de refus de l'accès, qui devrait être communiqué par écrit et motivé, un droit de recours pourrait être exercé, soit auprès de l'autorité de contrôle nationale, soit auprès d'une autorité judiciaire.

L'article 11 *sexies* instituerait un droit de rectification et d'effacement. L'unité de renseignements passagers aurait le devoir de rectifier des données si elle apprend qu'elles sont incorrectes, de les mettre à jour si possible et d'effacer les données si elles ont été transférées par le transporteur en violation des disposions nationales d'application de la décision-cadre. Il appartiendrait aux Etats membres de décider si les particuliers peuvent faire valoir ces droits directement auprès des unités de renseignements passagers ou par l'intermédiaire de l'autorité de contrôle compétente. Un refus de rectification ou d'effacement devrait être, le cas échéant, communiqué par écrit et pouvoir faire l'objet d'un recours sur lequel la personne est informée.

Un droit à réparation pour les personnes lésées par les actions de l'Etat membre ou d'un transporteur aérien compléterait ce dispositif (article 11 *septies*).

Un droit de recours juridictionnel devrait être prévu en cas de violation des droits garantis aux particuliers par les dispositions nationales prises en application de la décision-cadre (article 11 *octies*).

Il convient de noter que cet ensemble de droits applicable aux données traitées par les unités de renseignements passagers, c'est-à-dire par des autorités publiques nationales, est inspiré des droits de la décision-cadre de 2008 dont les Etats membres n'avaient pas voulu qu'elle s'applique aux 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.

Le rapporteur souligne le caractère positif des droits et garanties prévus pour les personnes concernées.

Une fois les données transmises de l'unité de renseignements passagers aux autorités compétentes, le droit national en vigueur en matière de protection des données par les autorités répressives s'appliquera.

I. Les échanges de données entre Etats membres et avec les pays tiers

1. Les échanges de données entre Etats membres

La dernière version du texte prévoit que les garanties en matière de protection des données définies dans la décision-cadre de 2008 s'appliquent au transfert de données PNR par l'unité de renseignements passagers d'un Etat membre à l'unité de renseignements passagers ou à l'autorité compétente d'un autre Etat membre, tout comme à l'échange de données PNR entre les autorités compétentes de plusieurs Etats membres (considérant 10 *bis*).

L'article sept de la proposition de décision-cadre prévoit que les données PNR ou les analyses de ces données portant des personnes qui ont été identifiées par une unité de renseignements passagers soient transmises à l'unité de renseignements passagers d'un autre Etat membre uniquement dans la mesure où cette transmission est nécessaire pour prévenir ou détecter des infractions terroristes et les formes graves de criminalité ou procéder à des enquêtes et des poursuites en ces matières. L'unité de renseignements passagers d'un Etat membre serait autorisée à demander à une autre unité de renseignements passagers de lui communiquer des données. Cette demande pourrait être limitée au cas par cas ou également applicable de façon régulière selon les besoins de l'Etat membre.

La question des échanges de masses de données doit ici être abordée car, si l'on comprend que les unités de renseignements passagers puissent avoir accès à des masses de données reçues par une autre unité dans la mesure où la transmission est nécessaire aux finalités visées par la décision-cadre, cela devient beaucoup plus problématique si les données sont transférées aux autorités compétentes.

Les accès des autorités compétentes seront régis par le droit national de chaque Etat. Néanmoins, le texte prévoit dans sa rédaction actuelle que :

– les autorités compétentes d'un Etat pourront avoir accès à des données brutes transmises par l'unité de renseignements passagers nationale aux fins de la directive, sans que le transfert de masses de données soit exclu ;

– les autorités compétentes d'un Etat membre pourront être également habilitées à demander au cas par cas le transfert de données à l'unité de renseignements passagers d'un autre Etat. Cette demande devrait s'inscrire dans le cadre d'enquêtes ou de poursuites spécifiques concernant des infractions terroristes ou des formes graves de criminalité. Cependant, le point de savoir si un Etat membre devrait pouvoir adresser une demande directe à une unité de renseignements passagers d'un autre Etat membre est encore sujet à débat. Les transferts de masses de données ne sont pas expressément exclus, ce qui est problématique.

Il faut considérer que les accès aux données brutes non analysées doivent être très limités.

C'est d'autant plus vrai que l'article 19 de la proposition dispose que les Etats membres peuvent continuer à appliquer les accords ou arrangements bilatéraux antérieurs en vigueur au moment de l'adoption du texte « *dans la mesure où ils sont compatibles avec la réalisation des objectifs visés* », ce qui est plutôt vague.

Il pourrait donc y avoir un Etat source de fuite vers un Etat tiers avec lequel il aurait passé un accord bilatéral. Un frein doit être posé pour que les données issues des autres Etats membres ne puissent pas être transférées.

Une clause serait prévue en cas de circonstances exceptionnelles, lorsqu'il existe des éléments indiquant qu'un accès rapide est nécessaire pour aider à réagir face à une menace spécifique et réelle en matière d'infraction terroriste ou de formes graves de criminalité : l'unité de renseignements passagers d'un Etat membre ou ses autorités compétentes pourraient être habilitées à demander à l'unité de renseignements passagers d'un autre Etat membre de leur communiquer des données avant le départ d'un vol.

En outre, les Etats membres continueront à s'échanger des données sur les bases de la coopération policière et judiciaire. La proposition de décision-cadre prévoit que : « *Les règles de la décision-cadre relative à l'échange de données PNR entre les unités de renseignements passagers des différents Etats membres sont sans préjudice de l'échange de données PNR entre les autorités répressives ou judiciaires, y compris par l'intermédiaire d'Eurojust et d'Europol, qui ont obtenu de telles données de leur unité de renseignements passagers conformément à la présente décision-cadre. Cet échange de données PNR entre autorités*

répressives ou judiciaires est régi par les règles relatives à la coopération policière et judiciaire » (considérant 21 *bis*).

2. Les échanges de données avec des pays tiers

La question des échanges de données avec les pays tiers n'a malheureusement pas pu être débattue sous présidence française par manque de temps. Il s'agit d'un point crucial en matière de protection des données et de respect de la vie privée.

Les Etats membres sont à l'heure actuelle réticents à négocier sur ce point qui relève finalement pour partie de leur politique extérieure.

Pour autant, la confiance des citoyens européens dans ce système reposera sur la capacité des Etats à maîtriser et à réglementer strictement les transferts des données.

Toutes les autorités de contrôle ont souhaité que les transferts de données soient très protégés et que les conséquences des dispositions des accords internationaux déjà en vigueur soient clarifiées.

« *Les Etats membres devraient au besoin partager avec les autres Etats membres les résultats du traitement des données PNR qu'ils reçoivent. Les transferts à des pays tiers par un Etat membre de données PNR devraient être autorisés uniquement au cas par cas et respecter des conditions supplémentaires relatives à la finalité du transfert, à la qualité de l'autorité destinataire et au niveau de protection des données dans le pays tiers. Lorsque les Etats membres ou l'Union ont conclu des accords internationaux en matière de transferts de données avant l'entrée en vigueur de la présente décision-cadre, les dispositions de ces accords devraient s'appliquer*. » (considérant 21)

En conséquence, lorsque les conditions d'un accord sont plus souples que celles prévues par la présente proposition, ces dernières s'inclineraient.

L'article huit de la proposition de décision-cadre, dans sa dernière rédaction, dispose que :

« *1. Les données PNR et les analyses des données PNR ne peuvent être transférées à un pays tiers ou mises à sa disposition par un Etat membre qu'au cas par cas et que si l'Etat membre a l'assurance que :*

a) le transfert est nécessaire pour prévenir ou détecter des infractions terroristes et des formes graves de criminalité, ou procéder à des enquêtes ou des poursuites en la matière ;

b) l'autorité destinataire du pays tiers est une autorité chargée de la prévention et de la détection des infractions terroristes et des formes graves de criminalité, des enquêtes ou des poursuites en la matière ;

c) si les données PNR ont été obtenues auprès d'un autre Etat membre, ledit Etat membre a consenti au transfert conformément à son droit national ;

d) le pays tiers assurera un niveau de protection adéquat au traitement des données qui est prévu et

e) le pays tiers ne transmettra pas les données à un autre pays tiers sans le consentement exprès de l'Etat membre.

2. Par dérogation au paragraphe 1, point c), les données peuvent être transférées à un pays tiers sans le consentement préalable de l'Etat membre auprès duquel les données ont été obtenues uniquement si ce transfert est essentiel pour prévenir une menace imminente et grave liée à la prévention ou à la détection des infractions terroristes et des formes graves de criminalité ou aux enquêtes ou aux poursuites en la matière et si le consentement préalable ne peut pas être obtenu en temps voulu. L'Etat membre qui procède au transfert informe sans délai l'Etat membre auprès duquel les données ont été obtenues.

3. Le niveau de protection adéquat visé au paragraphe 1, point d), est évalué à la lumière de l'ensemble des circonstances dans lesquelles ont été effectués les transferts. Une attention particulière est accordée à la finalité de l'utilisation des données, à la période de conservation des données, au pays de destination finale des données, à la situation en matière d'Etat de droit dans le pays tiers et aux mesures de sécurité mises en place.

4. En outre, ces transmissions ne peuvent se faire que dans le respect du droit national de l'Etat membre concerné et des accords internationaux éventuellement applicables. »

Le point 1 pose donc un certain nombre de principes absolument nécessaires dans l'éventualité d'un transfert. Il convient de noter que les transferts en masse ne sont pas exclus. Les garanties figurant au 1 sont celles prévues par la décision-cadre du 27 novembre 2008. L'exception au principe de l'accord de l'Etat membre d'origine des données en cas de menace grave et imminente est également inspirée de la décision-cadre du 27 novembre 2008, tout comme le descriptif du caractère adéquat de la protection des données qui doit être assurée dans le pays de destination.

La dernière version du texte constitue bien un progrès par rapport à la première version présentée en 2007 et répond à un certain nombre d'interrogations du contrôleur européen de la protection des données.

Il faudra être très attentif à ce que les données transmises « au cas par cas » soient bien des données analysées ou une donnée PNR brute isolée mais en aucun cas un transfert de masse de données qui peut également se faire « au cas par cas ». Il s'agit là d'un aspect important de l'encadrement des transferts sur lequel le texte devra être précisé.

L'article 19 de la proposition dispose que les Etats membres peuvent continuer à appliquer les accords ou arrangements bilatéraux antérieurs en vigueur au moment de l'adoption du texte « *dans la mesure où ils sont compatibles avec la réalisation des objectifs visés* », ce qui est plutôt vague.

Des accords pourront ensuite être conclus dans la mesure où ils sont compatibles avec la réalisation des objectifs visés.

Un autre point de première importance doit être souligné : le fait que l'Union se dote d'un régime applicable à la collecte et au traitement des données PNR constituera un élément clé dans la renégociation des accords actuels. L'on pense bien entendu à l'accord avec les Etats-Unis pour lequel, face aux exigences américaines, l'Union n'avait en 2007 pas de position commune à opposer, notamment s'agissant de la durée acceptable de conservation.

Enfin, une question primordiale s'agissant des pays avec lesquels l'Union n'a pas signé d'accord se pose : qu'en sera-t-il de la réciprocité ? Dans sa première proposition de décision-cadre en 2007, la Commission européenne indiquait que « *on ne peut exclure que certains pays demandent, à titre de réciprocité, un accès aux données PNR pour les vols à partir de l'UE vers leur territoire, même si en pratique c'est très peu probable. Les accords existants entre l'Union européenne et les Etats-Unis et le Canada en matière de données PNR prévoient cette réciprocité qui peut être appliquée automatiquement.* »

Bien au contraire, le rapporteur estime qu'il est tout à fait probable que des Etats intéressés par les données PNR veuillent disposer des données à titre de réciprocité. Cette question n'a pas encore fait l'objet de débats mais devra impérativement être encadrée. En effet, des pays peu sûrs en termes de protection des données ne doivent pas pouvoir avoir accès aux données PNR.

CONCLUSION

En conclusion, le rapporteur estime que la proposition de décision-cadre serait un outil de premier plan dans la lutte contre le terrorisme et les formes graves de criminalité.

Il est convaincu à la fois que les données PNR sont nécessaires aux autorités répressives et qu'elles ne sont redondantes avec aucun autre instrument européen existant (notamment la possibilité d'avoir accès aux données APIS dans la lutte contre l'immigration illégale).

Le rapporteur pense également que la mesure est, sous réserve des observations formulées ci-après, proportionnée aux finalités prévues.

De par l'ampleur de la collecte et le champ très vaste des questions posées (pour beaucoup de façon inédite), un réexamen de la mesure est prévu dans les trois années suivant sa mise en œuvre, ce qui constitue une nécessité.

Un réexamen est aussi nécessaire compte tenu des marges de manœuvre qui seront laissées aux Etats membres afin de s'assurer qu'elles ne nuisent pas à l'harmonisation recherchée ni à l'échange d'informations.

Certaines questions n'ont pas trouvé de réponse à l'heure actuelle mais le rapporteur est confiant sur les perspectives de cette décision-cadre qui est très importante pour les Etats membres dans la lutte contre le terrorisme et la criminalité organisée ainsi que dans l'élaboration des échanges de données PNR avec des pays tiers.

Un texte équilibré adopté au sein de l'Union permettra de renforcer les droits des passagers et de remettre au centre des préoccupations la protection des droits fondamentaux.

*

* *

TRAVAUX DE LA COMMISSION

1. Audition de M. Alex Türk, président de la Commission nationale de l'informatique et des libertés (CNIL), sur la sécurité et la protection des données, le mardi 25 novembre 2008

Le Président Pierre Lequiller. La Commission chargée des affaires européennes est heureuse d'accueillir aujourd'hui M. Alex Türk, Président de la Commission nationale de l'informatique et des libertés, à la veille du Conseil des ministres « Justice et affaires intérieures », qui devrait adopter le projet de décision-cadre pour la protection des données à caractère personnel dans le domaine de la coopération policière et judiciaire en matière pénale. Deux autres textes sont en discussion : l'un sur le *Passenger Name Record* – PNR – européen, et l'autre sur les scanners corporels, qui a été provisoirement retiré par la Commission. Quelle est la position de la CNIL sur ces projets ? Quelles perspectives ouvrent-ils ?

M. Alex Türk, Président de la Commission nationale de l'informatique et des libertés. C'est la première fois que je suis auditionné par votre Commission et je la remercie de m'avoir invité. Je m'exprimerai en tant que président non seulement de la CNIL mais aussi du G29, le groupe dit de l'article 29 sur la protection des données qui rassemble les vingt-sept autorités européennes homologues de la CNIL.

En préambule, une remarque incidente sur la langue, que je ne manque jamais de faire. La situation du français est plus que catastrophique. Quand j'ai commencé à fréquenter ce milieu il y a seize ans, 75 % des questions étaient traitées en français, contre 5 % à 10 % aujourd'hui. Le phénomène est encore aggravé par la prétention d'un nombre croissant de Français à parler anglais, ce qu'ils ne font pas toujours bien. Pourtant, les interprètes sont là et les auditeurs préféreraient souvent que les orateurs s'expriment dans leur langue maternelle, qu'ils maîtrisent mieux. Il faut faire un effort, sinon le français disparaîtra complètement.

La CNIL est de plus en plus impliquée dans les sujets internationaux. Son service spécialisé s'est beaucoup développé depuis quatre ans car nous devons être présents dans des domaines qui sont d'un intérêt vital.

Parmi les grands enjeux, le plus important, celui qui nous préoccupe le plus, concerne les relations entre les Etats-Unis et l'Europe en matière de transfert des données. Aujourd'hui, il n'est pratiquement plus possible de faire du commerce international sans transfert de données personnelles. Or la directive

européenne de 1995 fixe des conditions à ce transfert vers des pays tiers : le responsable du traitement des données doit pouvoir démontrer que le pays destinataire offre un niveau de protection des données comparable à celui qui prévaut en Europe. C'est un immense problème car, depuis la loi de 2004, tous les jours, la CNIL doit se prononcer sur les demandes d'autorisation de transferts de données de la France vers des pays tiers. Or il n'y a guère plus de quarante à cinquante pays – dont certains très petits – qui ont un niveau de protection équivalent à celui en vigueur dans l'Union. Outre les vingt-sept Etats membres, il y a Monaco, Andorre, la Suisse, l'Australie, le Canada, la Nouvelle-Zélande, mais aussi l'Argentine, le Burkina Faso et, très bientôt, le Maroc et le Sénégal. Mais certaines grandes puissances restent rétives : la Chine, l'Inde, le Japon, la Russie, une grande partie de l'Asie, de l'Amérique latine, de l'Afrique, et, aussi, bien sûr, les Etats-Unis.

Ces derniers nous disent qu'ils n'ont pas de leçons à recevoir et que les concepts qu'ils ont développés depuis trente ans assurent une protection suffisante. Ils n'ont pourtant ni autorité indépendante de contrôle ni loi fondamentale, qui sont les deux critères fondamentaux retenus par la Commission européenne et par le G29. Les Européens doivent constater que l'écart est grand entre la vision américaine et la vision européenne : juridiquement parlant, les Etats-Unis sont dans la même situation que les autres pays qui ne remplissent pas ces deux critères. La difficulté tient à ce que nous n'arrivons pas à inventer un concept juridique qui permettrait d'harmoniser les systèmes européen et américain, pour favoriser le développement du commerce international. C'est pourtant un point décisif.

On recourt à des ersatz comme le *Safe Harbor* – ou sphère de sécurité –, qui s'apparente à un port virtuel dans lequel viennent s'amarrer quelques centaines d'entreprises qui acceptent de reconnaître la validité des concepts juridiques européens et adhèrent à nos principes. Cela marche plus ou moins. Le G29 vient de passer deux jours à négocier avec les autorités américaines à Bruxelles et nous en sommes sortis assez perplexes. Une autre technique réside dans les clauses contractuelles types qui permettent d'assurer les transferts de données personnelles sous l'égide de la Commission européenne. Cela aussi marche plus ou moins. Il y a encore les *Binding Corporate Rules*, les BCR, ou règles internes d'entreprise, qui permettent de mettre en place, à l'intérieur des grands groupes internationaux, un régime juridique qui leur est propre. Ainsi, General Electric peut décider d'instaurer dans ses filiales installées partout dans le monde un cadre juridique conforme aux principes européens. Nous travaillons d'arrache-pied pour y parvenir. Mais nous rencontrons de grandes difficultés, en particulier parce que le G29 ne dispose d'aucun moyen si ce n'est pour la traduction, et pas dans toutes les langues – ce qui est scandaleux. Il est choquant par exemple que la CNIL seule doive financer une journée de travail entre une trentaine de pays pour élaborer ces BCR qui sont indispensables pour le développement du commerce international. Chaque fois que je réclame de l'argent à certains de mes homologues en tant que président du G29, je m'entends dire que le G29 est un outil magnifique, mais qu'il n'a pas besoin d'argent ! J'espère votre soutien sur ce sujet.

C'est d'autant plus grave que les sujets délicats ne manquent pas dans les relations de l'Europe avec les Etats-Unis.

Le premier, ce sont évidemment les PNR. Par exemple, la durée de conservation des données des passagers des compagnies aériennes européennes est, à mes yeux, très excessive car elle atteint quinze ans. Autre exemple : les autorités américaines n'ont jamais pu, ou voulu, communiquer la liste des autorités américaines destinataires des données en question. Or le territoire fédéral n'abrite pas moins de 18 000 autorités susceptibles de l'être. Nous pensons aussi que les références – une trentaine – qui sont exigées des passagers vont trop loin : avec qui vous êtes allé à tel endroit, pour quel motif, ce que vous avez mangé à bord… Les autorités de contrôle européennes sont en porte-à-faux complet, car la réaction de l'exécutif européen a été de s'aligner, au lieu de limiter les prétentions américaines.

En revanche, nous avons obtenu des résultats plus tangibles dans le dossier SWIFT, ce fameux système de transfert de données bancaires. Pour lutter contre le terrorisme, dans le cadre du *Patriot Act*, les Etats-Unis avaient décidé d'accéder à toutes les informations qui passaient par deux centres, dont l'un se trouve en Belgique et l'autre aux USA. Nous avons constaté qu'un grand nombre de données personnelles relatives aux transactions européennes étaient contrôlées par les services de sécurité américains, sans que nous sachions qui étaient les destinataires de ces données. Nous nous sommes demandé notamment si la politique tarifaire d'EADS n'avait pas fait l'objet d'un contrôle de la part des services américains. Mais, cette fois, nous avons été entendus à la fois par les autorités françaises – le Gouvernement et le gouverneur de la Banque de France –, européennes, et même américaines. Davantage de contrôles sur place seront diligentés et un troisième centre devrait être installé en Suisse pour qu'au moins les transactions bancaires intra-européennes ne passent plus par le système américain.

Autre grave préoccupation : l'affaire du *discovery* (échange d'un maximum d'informations avant un procès ou *pre-trial discovery*). Les Etats-Unis demandent de plus en plus que les sociétés françaises, et leurs filiales implantées en France, transmettent systématiquement certaines informations les concernant pour permettre le respect du contradictoire au sens du droit américain. Autrement dit, les sociétés françaises sont obligées de communiquer des renseignements qui sont considérés, de ce côté-ci de l'Atlantique, comme confidentiels. Tant le G29 que la CNIL travaillent sur ce point, mais ils se heurtent à de très sérieux obstacles.

Le G29 est par ailleurs confronté à d'importants problèmes concernant Internet, et particulièrement les moteurs de recherche et les réseaux sociaux. Le G29 a rendu en mars dernier une recommandation qui marque des limites, notamment en ce qui concerne la durée de conservation des données acquises par les moteurs de recherche, qui sera alignée sur le droit européen, et la nécessité de requérir le consentement des intéressés pour utiliser leurs références à des fins de

profilage. Aujourd'hui, ce n'est pas toujours le cas. Au départ, la société Google – qui conservait naguère les données sans limitation de durée – nous a fait savoir qu'elle avait accepté de limiter la durée de conservation à dix-huit mois. Notre recommandation, votée à l'unanimité, prévoit six mois. Finalement, Google a transigé à neuf mois. Mais, jusqu'à présent, cette entreprise refuse totalement d'appliquer le droit européen. Nous avons prévu à Bruxelles une série d'auditions des grandes sociétés telles que Google ou Microsoft, pour qu'elles répondent à nos questions. Il en sera de même avec les réseaux sociaux pour essayer d'aboutir à une recommandation avant la fin de 2009, afin d'assurer la protection des jeunes.

S'agissant du *body scanner*, autrement dit du système de scanner corporel dans les aéroports, il soulève avant tout le problème de savoir si la CNIL est compétente en la matière. Tous les commissaires de la CNIL, qu'ils soient de gauche ou de droite, sont choqués par de telles pratiques. Mais cela ne suffit pas et il faut étudier le système pour savoir s'il pose un problème touchant à la protection des données ; pour le moment, un doute subsiste sur notre compétence juridique. Certains de mes collègues considèrent néanmoins qu'il nous incombe de mener cette analyse, ne serait-ce que pour la communiquer au Parlement auquel, de plus en plus, la CNIL estime devoir apporter son éclairage. A plusieurs reprises, le Président du Sénat m'a dit souhaiter commander des études à la CNIL. Elle est, bien sûr, également à votre disposition pour vous fournir une assistance technique.

Un autre projet préoccupe beaucoup le G29, c'est le système *Op Tag*, envisagé par la Commission européenne qui a commandé une étude de 3 millions d'euros. Le but du dispositif est de rechercher les flâneurs dans les aéroports grâce à un couplage du dispositif de vidéosurveillance avec des puces RFID (Radio Frequency Identification) qui permettent de suivre les personnes à distance. L'objectif est de repérer les passagers qui arrivent en retard à l'embarquement et qui coûtent cher aux compagnies aériennes : un retard à l'envol fait perdre son tour à destination, ce qui fait consommer davantage de kérosène. Il serait donc question d'équiper tous les aéroports européens d'un tel système. Ainsi, les personnes dont le billet serait porteur d'une puce RFID seraient repérées et conduites par des vigiles à la zone d'embarquement. C'est un projet qui nous laisse perplexes, mais il est très avancé.

Je laisse à Mme Sophie Nerbonne, directrice adjointe des affaires juridiques, internationales et de l'expertise, le soin de faire le point sur la décision-cadre.

M^me^ Sophie Nerbonne, directrice adjointe des affaires juridiques, internationales et de l'expertise. La décision-cadre relative à la protection des données a pour objectif de favoriser les échanges entre États membres des données traitées dans le cadre des activités policières et judiciaires. La CNIL a fait valoir à plusieurs reprises que ce texte présente des garanties insuffisantes au regard de la loi française informatique et libertés ou même de la directive européenne de 1995. Il convient de le compléter par des garanties portant sur la pertinence des

informations transmises et leur adéquation au regard de la finalité poursuivie, la sécurisation technique des échanges et la limitation de la durée de conservation.

Le Président Pierre Lequiller. Je vous remercie d'avoir proposé de nous transmettre les études dont nous pourrions avoir besoin ; au-delà de cette réunion, une coopération suivie s'impose.

Notre Commission présente une particularité : ses membres appartiennent à une autre Commission, l'une des Commissions permanentes de l'Assemblée, comme la Commission des lois, avec laquelle je suppose que vous avez également des contacts.

M. Alex Türk. J'ai déjà été auditionné par la Commission des lois et la Commission des affaires économiques.

M. Thierry Mariani. Le problème que nous évoquons aujourd'hui n'est pas considéré à sa juste valeur. Le débat politique se polarise parfois sur des atteintes mineures à la vie privée, sans commune mesure avec ce dossier. Quand on part au Mexique par Air France, la compagnie vous demande maintenant de fournir des informations personnelles « par précaution », au cas où l'avion devrait atterrir aux Etats-Unis ! Cela devient hallucinant. Mais quel est notre poids pour pouvoir imposer notre conception face aux Etats-Unis ?

M. Alex Türk. Il est très courant que des autorités ou des entreprises prennent ainsi les devants, « au cas où », y compris en France, et conservent plus de données qu'il n'est nécessaire. La loi pose pourtant un principe simple de pertinence et d'adéquation des données recueillies à la finalité poursuivie.

Le poids de nos positions dépend de vous et de nous. Nous souhaitons vous informer de nos préoccupations afin que le Parlement français pèse par rapport aux Etats-Unis, et cela vaut aussi pour les autres grands pays européens. Depuis que le G29 a durci sa position vis-à-vis de Google, cette entreprise a accepté le dialogue.

Il ne s'agit pas de considérer les Américains comme des adversaires mais de faire respecter nos droits. Les États européens ne doivent pas accepter le refus de Google de reconnaître l'applicabilité du droit européen en Europe. Notre rôle consiste à fournir des argumentaires aux pouvoirs publics sur ces sujets. Les CNIL jouent un rôle essentiel mais doivent être soutenues par les Parlements ; ce n'est pas toujours facile car ceux-ci n'ont pas toujours les mêmes opinions qu'elles.

M. Thierry Mariani. Je suis choqué de voir Air France recueillir ce type de données « au cas où ».

M. Alex Türk. Quand les Etats-Unis ont fixé la règle du PNR, les compagnies européennes se sont immédiatement rangées à leurs vues: elles ont ensuite dit à leurs Gouvernements qu'elles y étaient contraintes pour pouvoir

continuer à développer leurs lignes transatlantiques et qu'il n'y avait aucune négociation possible. Seuls le Parlement européen et la CNIL ont déploré cette occasion manquée de négocier.

M. Guy Geoffroy. Nous sommes inquiets mais lucides et persévérants. Nous sommes prêts à faire cause commune avec vous pour que la France joue un rôle déterminant en Europe et pour que l'Europe soit ainsi capable de jouer vis-à-vis des Etats-Unis un rôle qu'aujourd'hui elle peine à jouer. À l'époque de l'affaire des PNR, la Délégation pour l'Union européenne avait conclu que la France n'avait pas le choix. Je suis d'autant plus sensible à la question qu'il m'a été donné de goûter aux délices vertigineux du scanner corporel américain, ce qui amène à s'interroger sur les notions de libertés fondamentales et de patrie des libertés…

Dans le rapport de forces entre l'Europe et les Etats-Unis, quel poids vos observations ont-elles eu ? Le projet de décision-cadre que devrait approuver le Conseil JAI en tient-il compte ? Qu'apportera cette décision-cadre à la France et à l'Europe ? S'agissant du projet de PNR européen, il semblerait que la durée de conservation, initialement fixée à cinq ans, soit ramenée à trois ans. N'est-ce pas encore un peu long ? En unissant les efforts de contrôle européens, serons-nous vraiment mieux armés pour ralentir le mouvement vers une société de surveillance totale ?

M. Alex Türk. Nous restons inquiets sur les deux sujets distincts que vous évoquez : la décision-cadre relative à la protection des données dans le troisième pilier et les PNR.

La décision-cadre est en voie d'adoption et je vois mal, hélas, comment nous pourrions revenir en arrière.

S'agissant des PNR, nous voudrions concilier les exigences de la sécurité et le respect des droits individuels en établissant des durées de conservation courtes, en définissant précisément la liste des destinataires et en précisant l'usage des données. Nous étions contre le traitement américain du problème. Maintenant que l'Europe s'y met, nous espérons que ce seront des PNR à l'européenne, reflet du droit communautaire, plutôt qu'une imitation du système américain. Nous serons plus forts vis-à-vis des Américains si nous leur démontrons qu'il est possible d'assurer la sécurité du transport aérien sans aller aussi loin qu'eux.

En matière de société de surveillance, les dossiers les plus inquiétants n'ont pas trait à la problématique européenne mais au développement de la biométrie, de la géolocalisation des personnes par le biais des puces RFID et bientôt des nanotechnologies. Les avancées sont éparses et passent encore inaperçues ; mais l'addition des moteurs de recherche et des réseaux sociaux sur Internet, de la biométrie, de la géolocalisation, de la vidéosurveillance et des nanotechnologies va se traduire par une transformation profonde de notre société.

Les vingt-sept « CNIL » européennes partagent ce point de vue ; la difficulté consiste à convaincre les exécutifs. Nous sommes disposés à nouer les contacts les plus étroits avec vous, en amont des décisions qu'il vous incombe de prendre. Si la CNIL, préalablement à l'examen de tout projet de loi, rédigeait un avis intégré dans une étude d'impact, le Parlement serait mieux éclairé sur certains dangers potentiels.

M^me^ Marietta Karamanli. J'ai été agréablement surprise par votre propos concernant les scanners corporels car il nous avait été rapporté que la CNIL n'estimait pas, à première vue, que les appareils en question entrent dans son champ de compétence et n'avait pas émis de réserves sur les appareils devant être déployés à Nice. Tout ce qui porte atteinte aux libertés publiques doit être visé par le législateur. Nous souhaitons donc que le Parlement soit saisi de cette question.

Nous avons exprimé des réserves à propos de l'enregistrement d'images à partir des scanners corporels et de leur association à d'autres fichiers. Il nous a d'abord été répondu que ce n'était pas envisagé. Or nous savons aujourd'hui que les progrès techniques ouvrent toutes les possibilités. Nous aimerions travailler sur ce dossier avec vous et approfondir la question.

M. Alex Türk. Nous avons pour objectif de nous saisir de la question et de l'étudier en séance plénière. J'ignore la position que prendra celle-ci mais nous ne pouvons faire l'économie de cette analyse. La CNIL est confrontée quotidiennement à des problématiques de ce type, liées à l'émergence de technologies : nous recevons des demandes, par exemple, au sujet des panneaux qui vous interpelleront bientôt directement dans le métro en vous appelant sur votre téléphone portable. Notre compétence en la matière n'est pas avérée mais nous ne pouvons pas négliger la question.

On prête à la CNIL bien des prises de positions qui ne sont pas toujours les siennes. En général c'est pour dire qu'elle est contre telle ou telle mesure. Certains font courir le bruit qu'elle serait hostile à toute lutte contre la fraude, ce qui revient à nous prendre pour des imbéciles. Nous ne sommes pas non plus opposés à toutes les interconnexions de fichiers : nous en avons déjà accepté trente, quand cela se justifiait. Et quand le Parlement a pris une décision dans ce sens, nous appliquons la loi.

Lorsque des parlementaires protestent contre l'interventionnisme de la CNIL, je leur rétorque qu'elle n'a pour compétences que celles que le Parlement lui a conférées en 2004, qu'elle ne se détermine que par rapport à des textes et qu'elle applique les lois. Par exemple, si le Parlement veut rendre possible l'établissement de fichiers positifs dans le domaine bancaire, il doit légiférer ; si le Parlement – autre exemple – souhaite aller plus loin en matière de statistiques ethniques, qu'il prenne ses responsabilités. La CNIL est une autorité administrative indépendante, pas une troisième chambre.

Le Président Pierre Lequiller. Mais elle a pour fonction d'éclairer le législateur.

M. Alex Türk. Elle éclaire le législateur puis vérifie que la loi est appliquée.

Le Président Pierre Lequiller. Je vous remercie pour cette intervention très intéressante. M[me] Karamanli, qui travaille sur les scanners corporels, et M. Geoffroy, qui se penche sur les PNR, sauront se rapprocher de M[me] Chatain-Marcel, qui s'occupe notamment à la CNIL des relations avec le Parlement.

*

* *

2. Audition de M[me] Michèle Alliot-Marie, ministre de l'intérieur, de l'outre-mer et des collectivités territoriales, sur le bilan de la présidence française dans le domaine des affaires intérieures et le « *Passenger name record* » (PNR) européen, le mercredi 3 décembre 2008

Le Président Pierre Lequiller. La commission chargée des affaires européennes est heureuse d'accueillir aujourd'hui Mme Michèle Alliot-Marie, ministre de l'intérieur, de l'outre-mer et des collectivités territoriales.

Nous étudions actuellement plusieurs dossiers relevant de vos compétences, madame la ministre : le projet de « *Passenger name record* » (PNR) européen, dont le suivi est assuré par notre collègue Guy Geoffroy, et le projet de scanner corporel, au sujet duquel nous avons délibéré ce matin et dont les rapporteurs sont M[me] Marietta Karamanli et M. Didier Quentin.

Après les attentats tragiques de Bombay, la lutte contre le terrorisme est plus que jamais d'actualité. Pourriez-vous faire le point sur la nécessaire coordination des États membres de l'Union européenne dans ce domaine ?

La semaine prochaine, MM. Thierry Mariani et Christophe Caresche nous informeront des suites à donner au programme de La Haye. Quels ont été les grands axes de vos travaux pour préparer le programme 2010-2014 ?

Le traité de Lisbonne aurait permis de traiter certains sujets à la majorité qualifiée. Quoi qu'il en soit, la coopération en matière de police nous tient beaucoup à cœur.

M[me] Michèle Alliot-Marie, ministre de l'intérieur, de l'outre-mer et des collectivités territoriales. Je me félicite de la transformation de la Délégation pour l'Union européenne en Commission chargée des affaires européennes et je

suis persuadée que l'esprit très constructif de la Délégation se maintiendra sous ce nouveau statut.

A mesure que nous nous approchons de la fin de la présidence française de l'Union européenne, il devient possible d'esquisser un bilan de notre action. Je voudrais tout d'abord décrire l'état d'esprit dans lequel je me suis efforcée de travailler. A mon sens, les citoyens des différents pays de l'Union attendent avant tout une Europe qui les protège, qui ne soit pas une abstraction bruxelloise mais quelque chose de concret, de proche de leurs préoccupations quotidiennes. Ce sont les discours abstraits et les décisions éloignées de la vie de tous les jours qui provoquent les réactions négatives. L'Europe de la sécurité apporte aux citoyens la démonstration du caractère protecteur de l'Europe. Un sondage a déjà montré que 80 % des citoyens européens considèrent que l'Europe de la défense est une bonne chose : je souhaite qu'il en soit de même en matière de sécurité.

Reste à savoir comment on peut faire avancer les choses. Considérant qu'il y a trop de déclarations et de verbiage, je me suis efforcée d'adopter une attitude pragmatique et de privilégier les réalisations concrètes. Annoncer que l'on chamboulerait tout en six mois, c'était se condamner à l'échec. C'est pourquoi ma méthode a visé à rapprocher des dispositifs en place pour accomplir de réels progrès dans la protection des citoyens. J'ai proposé à mes collègues européens de faire converger nos façons de travailler en partant de l'existant, en identifiant les pistes d'amélioration, en promouvant des projets concrets dans chaque domaine, en mettant en œuvre ces projets selon un calendrier précis, et enfin en évaluant nos réalisations.

Cette méthode a prévalu dans les trois domaines principaux qui relèvent de ma compétence : *la lutte contre le terrorisme*, la lutte contre toutes les formes de criminalité internationale, l'amélioration de nos capacités de protection civile face aux catastrophes naturelles et industrielles.

Les récents attentats de Bombay l'ont rappelé : la menace terroriste est permanente et n'épargne aucun pays. En Allemagne, en Belgique, en France, des attentats ont été déjoués. Nos concitoyens peuvent être frappés lorsqu'ils se rendent à l'étranger pour leur travail ou leurs loisirs. Nous avons donc besoin de nouveaux outils pour détecter les risques le plus tôt possible, pour anticiper la réalisation d'attentats et pour améliorer la coopération avec les Etats tiers. Sans cette coopération, la lutte antiterroriste, même à l'échelle du continent européen, se révélera inefficace.

Nous avons tout d'abord réalisé des progrès en matière de détection des individus susceptibles d'avoir des liens avec les milieux terroristes : désormais, au moment de l'instruction des demandes de visa pour entrer dans les pays de l'Union européenne, les consulats font remonter l'information au niveau central européen à des fins policières, ce qui permet la consultation du système d'information Schengen et la prise de mesures adaptées - surveillance de la personne ou refus du visa, par exemple. En proposant ce système qui ne modifie

pas la procédure de délivrance, nous avons pu surmonter les réticences de certains pays qui craignaient d'alourdir la tâche de leurs consulats.

Autre moyen de détection précoce, le PNR permet un contrôle aux frontières aériennes à partir des données des compagnies aériennes sur leurs passagers et un suivi des déplacements des personnes signalées comme susceptibles d'avoir des liens avec le terrorisme – c'est le cas, par exemple, lorsque certaines personnes résidant sur notre territoire effectuent un séjour au Pakistan, en Afghanistan ou en Irak. En sériant les problèmes, la présidence française a permis de lever les blocages de plusieurs pays à ce sujet. Les inquiétudes portaient notamment sur la protection des données personnelles et sur le gigantisme du système ; certains voulaient que les vols intracommunautaires soient exclus, d'autres objectaient que ce serait risquer de perdre la trace de certaines personnes.

Nous disposons pourtant de plusieurs précédents démontrant l'utilité d'un PNR. Ainsi, en octobre 2007, les services britanniques sont parvenus à démanteler un réseau en recherchant avec qui les deux personnes qu'ils avaient identifiées voyageaient régulièrement.

Par ailleurs, les principales données qui nous intéressent sont le nom du voyageur, son pays d'origine, le lieu de l'achat du billet et le moyen de paiement utilisé. Ces deux derniers éléments étant particulièrement importants en matière de lutte contre le trafic de stupéfiants : on sait par exemple que l'on doit plus particulièrement surveiller les personnes qui ont acheté leur billet dans la région de Bogota et qui ont payé en liquide ou dans une certaine agence. En revanche, d'autres informations, telles que le régime alimentaire suivi par le passager, ne nous intéressent nullement.

Nous sommes également parvenus à la conclusion qu'il était impossible de gérer toutes les informations relatives aux voyageurs intracommunautaires et qu'il valait mieux se concentrer sur les vols de transit qui sont en connexion avec l'extérieur.

C'est de cette manière que nous avons progressé et que j'ai pu mettre d'accord les Vingt-sept sur le cadre général du PNR.

Nous avons en outre proposé des actions contre la radicalisation et le recrutement, notamment en milieu carcéral. Nous avons élaboré et distribué un guide de bonnes pratiques à l'intention des policiers et du personnel pénitentiaire, dans le but de leur indiquer les attitudes et les comportements qui doivent attirer leur attention et de les sensibiliser à un comportement respectueux vis-à-vis des personnes incarcérées : si la prison est un lieu de radicalisation, elle peut être aussi un moyen de lutter contre celle-ci moyennant une certaine compréhension culturelle.

Nous avons enfin fait progresser le plan d'action de l'Union contre les réseaux de recrutement, en facilitant par exemple le repérage des imams radicaux

sur l'ensemble du territoire européen, en déterminant quelles sont les pratiques radicales et en favorisant le dialogue interculturel, y compris sur internet.

Deuxième composante de la lutte antiterroriste : l'anticipation. Dans ce domaine, nous avons concentré nos efforts sur la menace nucléaire, radiologique, biologique et chimique (NRBC), qui est assurément la menace de demain – il est même étonnant que, à l'exception de l'attentat perpétré par la secte Aoun dans le métro de Tokyo et de la diffusion de l'anthrax par courrier aux États-Unis, on ait eu essentiellement affaire à des attentats à l'explosif alors que plusieurs sites internet expliquent la fabrication de certaines armes chimiques et bactériologiques. Une base de données européenne sera prochainement mise en place auprès d'Europol. Elle permettra de centraliser les informations sur les produits à risque et sur les événements relatifs au terrorisme NRBC. On sait par exemple qu'il est possible d'utiliser certains engrais agricoles pour fabriquer des explosifs. En nous appuyant sur cette base de données, nous pourrons faire pression sur les producteurs pour qu'ils modifient la composition de leurs produits.

Au début du mois de novembre, sur la base militaire de Canjuers, un exercice NRBC a rassemblé neuf États européens pendant trois jours. C'est la démonstration que l'Union européenne peut renforcer sa capacité de réponse coordonnée en cas d'acte terroriste majeur.

Troisième composante : la coopération avec les Etats tiers. La présidence française a tenu à nourrir les relations avec nos partenaires stratégiques. A cet égard, la troïka Union européenne-Russie qui s'est tenue à Paris le 15 octobre dernier s'est révélée particulièrement positive et concrète. Nous avons également engagé des échanges avec les États-Unis pour arrêter une position politique commune sur les échanges d'informations et sur la cybercriminalité. Pour la première fois, j'ai trouvé les Américains prêts à intervenir sur internet, notamment en matière de fabrication d'armements et d'explosifs.

J'en viens à *la lutte contre la criminalité*. Sur ce sujet, mon action a été guidée par trois idées forces : le rapprochement des pratiques, la modernisation des techniques et la maîtrise des itinéraires.

La criminalité organisée, on le sait, ne connaît pas de frontière. En conséquence, l'efficacité exige que l'action des polices européennes ne soit pas entravée par d'autres frontières, celles qu'engendrent des législations ou des pratiques policières différentes. Voilà pourquoi nous engageons des actions qui permettent aux policiers de divers pays d'agir ensemble, de se connaître et d'échanger leurs pratiques.

La coopération policière et douanière est de ce point de vue un atout majeur. Les centres de coopération policière et douanière bilatéraux que nous avons mis en place avec l'Espagne et l'Allemagne permettent d'arrêter de nombreux trafiquants ou auteurs de hold-up. Il faut maintenant obtenir que

davantage de pays s'engagent dans cette démarche. C'est dans ce but que nous avons élaboré un guide des bonnes pratiques consacré aux centres de coopération policière et douanière : il s'agit d'expliquer aux nouveaux pays les règles de fonctionnement et d'évaluation de ces centres et les possibilités qui existent pour les adapter au terrain. Le centre de coopération associant pour la première fois quatre pays – l'Allemagne, la Belgique, le Luxembourg et la France –, que nous avons créé le 24 octobre dernier, préfigure ce que pourrait être une police européenne.

Nous avons également mis en place des « commissariats européens », c'est-à-dire des commissariats où sont accueillis des policiers d'autres pays pour mener un travail commun. C'est une manière de répondre aux difficultés des citoyens lorsqu'ils sont victimes d'un vol ou sont mis en cause dans un autre pays de l'Union : le fait de pouvoir s'adresser à des policiers de son pays d'origine facilite les choses. Nous avons choisi d'installer ces structures dans des lieux très touristiques ou accueillant des événements importants. L'opération, décidée à la fin de juin, a été lancée dès le mois d'août à Paris, Versailles, Lourdes et Nice, ainsi qu'en Italie et en Hongrie. Le retour d'expérience s'étant avéré très positif, on peut s'attendre à ce que de nombreux pays s'engagent dans cette voie en 2009.

Deuxième axe de l'action contre la grande criminalité : la modernisation des techniques. Les grands délinquants sont extrêmement réactifs et ne tardent jamais à utiliser toutes les possibilités qu'ouvrent les nouvelles technologies. Pour les combattre, nous devons au moins être au même niveau qu'eux, et si possible nous ménager une marge d'avance. Voilà pourquoi j'ai fait de la lutte contre la cybercriminalité une des priorités de la présidence française. La pédopornographie et l'apologie du terrorisme et de l'antisémitisme, qui sont les principales menaces au plan européen, sont les premières cibles. Le programme d'action adopté par le Conseil – à l'initiative de la présidence française – comprend notamment la création d'une plate-forme européenne de signalement des infractions relevées sur internet, dont la Commission a accepté d'assurer le financement. C'est Europol qui hébergera cette structure qui devrait commencer à fonctionner dans les prochaines semaines et qui collectera en temps réel les signalements enregistrés par les dispositifs nationaux.

Nous développons également des partenariats public-privé afin d'agir en concertation avec les hébergeurs. Enfin, nous renforçons la formation des acteurs de la lutte contre la cybercriminalité : ce qui se fait actuellement au niveau européen est en quelque sorte la transposition de ce que j'avais lancé en France en créant les cyberpatrouilles. En matière de pédopornographie, un accord général s'est dégagé pour consacrer nos efforts à la fermeture de tous les sites.

Il nous faut aussi moderniser les techniques d'identification. Les criminels utilisent l'anonymat qu'assurent les communications passées avec une carte de téléphone portable acquise sur le territoire d'un autre pays. Nous venons d'adopter un projet qui permettra l'identification et le suivi des puces téléphoniques acquises dans n'importe quel pays de l'Union.

Troisième axe : la lutte contre les grands trafics. Le centre européen de coordination de la lutte antidrogue en Méditerranée, que j'ai créé, collectera les informations et les transmettra aux marines nationales, qui pourront ainsi intercepter les navires acheminant la drogue en provenance d'Afrique. Semblable à la structure créée à Lisbonne pour l'océan Atlantique, ce centre est « armé » par les pays du sud de l'Union européenne – France, Italie, Espagne, Grèce, Portugal, Chypre, Malte – et par les États du sud de la Méditerranée - Maroc, Algérie, Tunisie, Libye, mais aussi Mauritanie.

Les circuits de la drogue ont connu un transfert de l'Atlantique vers l'Afrique pour échapper au dispositif mis en place à Lisbonne. Tout ce que nous pourrons arrêter grâce aux pays nord-africains, c'est autant que nous n'aurons pas à intercepter en Méditerranée.

En outre, nous soutenons matériellement et financièrement les services de répression des pays d'Afrique par où transite la drogue, en particulier au Sénégal, au Mali, au Niger et en Mauritanie. Nous les aiderons à établir des plateformes opérationnelles, à former des officiers, bref, à se donner les moyens d'intervenir, la prise en charge financière étant très largement assumée par l'Europe.

Pour ces pays, c'est à la fois un enjeu de santé publique et une condition de la stabilité politique. L'Afrique est déjà très déstabilisée par les luttes interethniques. Si l'on ajoute à cela les trafics de drogue, qui génèrent une corruption généralisée, c'est l'Etat lui-même qui disparaît, avec pour conséquences des drames terribles et une pression migratoire considérable sur l'Europe. Si nous n'aidons pas ces pays à reconstruire leur Etat et leur économie, nous aurons un jour des millions de personnes qui arriveront en force en Europe et nous n'y pourrons rien. Ce qui est arrivé au Maroc il y a quelque temps n'est rien à côté de ce qui nous attend en cas de déstabilisation totale.

Le trafic d'armes est également préoccupant. Sur notre territoire, on constate la présence de Kalachnikovs et d'autres armes qui, de toute évidence, proviennent des pays de l'ancienne Yougoslavie. Certaines sont le reliquat des conflits qui se sont produits dans cette région, d'autres sont des approvisionnements nouveaux en provenance, probablement, de Biélorussie, d'Ukraine, *etc*.

Le Président Pierre Lequiller. Les pays de l'ex-Yougoslavie sont-ils aussi producteurs ?

M^me^ Michèle Alliot-Marie. Pas directement. Ils peuvent utiliser des pièces détachées. Lors du forum Union européenne-Balkans, qui s'est tenu récemment à Zagreb, j'ai bien précisé que la résolution de ces problèmes était une condition à l'entrée dans l'Union. Il a été convenu que les services de police des Etats de la région prennent part à des opérations communes avec les pays de l'Union contre les armes et les explosifs encore présents dans la région. Au début

de la semaine dernière, une opération coup de poing a permis de tester la capacité des Vingt-sept à se coordonner et à travailler conjointement sur ces problèmes. Nous avons prévu la création d'une plateforme destinée à améliorer les échanges entre les officiers de liaison des Etats membres et ceux des Balkans.

Troisième grande priorité de la présidence française dans mon champ de compétences : *le renforcement des capacités de protection civile*, qui est l'exemple type de ce qu'attendent les citoyens européens. Lorsque quatre pays de l'Union envoient des Canadairs pour combattre les incendies meurtriers qui touchent la Grèce, les gens comprennent ce que c'est que l'Europe. C'est l'esprit même de l'Europe que de se montrer solidaire lorsqu'un Etat membre ou un pays tiers n'a pas les moyens de faire face à une catastrophe de grande ampleur. A cet égard, j'ai gardé un très mauvais souvenir de notre action après le tsunami : les pays européens sont arrivés en ordre dispersé quinze jours après la catastrophe ! Il en a été de même après le tremblement de terre qui a frappé le Pakistan, et ce malgré la décision européenne.

J'ai donc proposé d'améliorer notre organisation en dotant l'Union de capacités opérationnelles rapides et efficaces. De même, j'ai fait adopter le 27 novembre à Bruxelles l'assistance mutuelle européenne, aux termes de laquelle les Etats membres mettent à disposition des capacités sur une base totalement volontaire et en regroupant les moyens selon les types d'intervention – incendies, inondations, séismes, *etc*. L'idée est de mettre en place des modules nationaux que les pays indiquent pouvoir mettre à disposition pendant une durée donnée. Mais ce ne seront pas toujours les mêmes pays qui feront tout : chacun doit s'équiper pour lui-même car le dispositif n'est mis en œuvre que lorsque la catastrophe est majeure. Il est également prévu un droit de retrait en cas de survenue d'un besoin local.

Afin d'améliorer les capacités de réaction, d'interopérabilité et de préparation, j'ai demandé que l'on recense les moyens dont chaque pays dispose. Au moment des incendies en Grèce, les Canadairs ne pouvaient agir en même temps car leurs moyens de communication n'étaient pas interopérables ! Il faut renforcer le centre de suivi et d'information de la Commission européenne afin qu'il soit en mesure de vérifier que les équipes peuvent travailler ensemble et de coordonner les moyens apportés par chaque pays. Le 8 décembre, le Conseil des affaires générales et des relations extérieures adoptera une feuille de route qui permettra de disposer rapidement d'un dispositif global, ajustable, efficace et réactif, couvrant toute la chaîne concernée, aussi bien au niveau national qu'au niveau communautaire.

Parallèlement, nous devons mettre en place des formations adaptées au travail en commun. J'ai proposé la création d'un véritable réseau européen de formation pour rapprocher les méthodes et les pratiques de tous les professionnels de la sécurité civile. L'objectif est de faire converger les modules d'enseignement, de procéder à des échanges d'étudiants et de mettre en place des entraînements communs.

Certains pays étaient au départ réticents car tous n'ont pas le processus décisionnel relativement centralisé auquel nous nous conformons lorsqu'il s'agit d'intervenir dans un autre pays. Par exemple, il est très difficile aux ministres fédéraux allemands de prendre des décisions à la place des *Länder*.

Au total, il aurait sans doute été difficile d'en faire davantage compte tenu des blocages habituels. Si nous pouvons être satisfaits de ce qui a été réalisé, nous devons aussi rester modestes : une présidence n'est qu'un maillon dans une longue chaîne. J'espère avoir convaincu mon collègue tchèque de poursuivre les actions engagées. Quoi qu'il en soit, je me suis gardée des grandes déclarations et je me suis efforcée de suivre la démarche très concrète qui correspond, j'en suis persuadée, aux attentes réelles des citoyens.

Le Président Pierre Lequiller. Je vous remercie pour cet exposé où vous avez mis autant de passion que de précision.

La création de commissariats européens dans les aéroports et les gares est-elle envisageable ?

M^me^ Michèle Alliot-Marie. Tout à fait. D'ailleurs, plusieurs éléments sont déjà en place.

Le Président Pierre Lequiller. Je suis très favorable à l'action européenne en matière de sécurité civile. C'est un symbole fort. Les forces d'intervention pourront-elles enfin apposer un sigle européen sur leurs véhicules et leurs uniformes ?

M^me^ Michèle Alliot-Marie. Je pense que cela pourra se faire facilement. Le seul point de crispation, c'est que les pays veulent conserver le choix d'envoyer ou non des forces.

Le Président Pierre Lequiller. La proposition avait été formulée, en son temps, par Michel Barnier et elle avait rencontré bon nombre de réticences.

M^me^ Michèle Alliot-Marie. Au départ, j'ai constaté les mêmes réticences car les responsables craignaient la création d'une structure purement européenne qui aurait été composée de personnels mis à disposition et attendant, l'arme au pied, que quelque chose se passe !

M. Jacques Desallangre. Vous placez vos propositions sous le signe du concret, Madame la ministre. Espérons qu'elles seront adoptées et appliquées tout aussi concrètement.

En matière de détection précoce des menaces liées au terrorisme et à la criminalité organisée, le Conseil « JAI » a conclu à « *la nécessité d'évaluer si des modifications des instruments juridiques existants sont nécessaires afin de rendre juridiquement contraignante l'application de ce mécanisme* ». L'intention est

louable mais comment mesurer l'effort – ou, le cas échéant, le laxisme – de tel ou tel pays membre ?

M^me^ Michèle Alliot-Marie. Je précise que toutes les mesures sont déjà adoptées, à l'exception de celles qui le seront le 8 décembre. Je me suis efforcée qu'elles soient applicables. Quant à leur application, c'est un autre point.

Certaines des modifications juridiques que vous évoquez sont obligatoires. La mesure de l'effort fourni par les pays membres est de la responsabilité de la Commission européenne. Elle dépendra aussi de la pression que chaque pays exercera sur cette dernière. C'est donc une question de volonté politique. Je n'ai aucun souci pour ce qui concerne la Commission, même s'il faut parfois la pousser un peu.

M. Guy Geoffroy. Ne pourrait-on tout d'abord, pour le PNR, proposer un sigle français ? Par exemple CD2P, pour « collecte des données personnelles des passagers »…

M^me^ Michèle Alliot-Marie. J'ai de toute façon horreur des sigles. *(Sourires.)*

M. Guy Geoffroy. Je crains que nous ne devions conserver « PNR », tant l'Europe nous pousse aux anglicismes.

Toujours est-il que la question de la transmission de ces données se situe à l'intersection de deux principes qui peuvent paraître inconciliables et qui revêtent une importance égale : la sécurité due à nos concitoyens dans leurs déplacements et les libertés fondamentales. Nous sommes partis d'assez loin, tant nous avons été échaudés par l'accord PNR qui nous a fait passer sous les fourches caudines des Etats-Unis – il est vrai que nous n'avions pas le choix puisqu'un refus aurait impliqué le refus d'accueillir sur le sol américain les personnes ne satisfaisant pas aux exigences posées. Il me semble toutefois que nous arrivons à un point d'équilibre qui devrait nous permettre de progresser, étant entendu que la future présidence tchèque a déjà manifesté l'intention de ne pas relâcher la pression à ce sujet.

Pourriez-vous, Madame la ministre, apporter à la Commission des précisions sur la durée de conservation et sur la volatilité des informations recueillies ? Les pays de l'Union s'accordent sur ce qu'il est nécessaire et suffisant de collecter. Encore faut-il savoir quelle est la destination de ces informations. La multiplicité des canaux peut faire craindre qu'on ne puisse plus les tracer.

Enfin, nos collègues du Parlement européen, très attachés à la défense des libertés fondamentales et ayant peu apprécié d'être mis devant le fait accompli en ce qui concerne le PNR américain, se montrent rétifs à l'adoption du dispositif européen. Comment les convaincre ? Peut-on envisager une mise en place en 2009 ?

M^me^ Michèle Alliot-Marie. La durée de conservation des informations est déterminée par deux types d'usage : d'une part, le suivi des personnes qui feraient peser un risque terroriste ; d'autre part, la possibilité de mettre hors de cause des personnes soupçonnées. Ces données permettent d'établir l'endroit où elles se trouvaient à tel ou tel moment. Le délai de trois ans nous est apparu à la fois normal et gérable, sachant qu'il sera possible de le porter à sept ans pour les individus très dangereux et pour les problèmes particulièrement sensibles. Malgré les réticences des Etats-Unis et des Anglo-saxons en général, je crois qu'il s'agit d'une base solide.

Pour ce qui est de la volatilité, je ne puis que rappeler notre grand attachement à la préservation des données personnelles. Nous travaillons d'ailleurs en concertation avec plusieurs organismes dédiés à cette préservation. Mais la traçabilité implique des contraintes qui ont créé, il est vrai, des difficultés dans notre négociation avec les Etats-Unis.

Enfin, c'est en parlant et en travaillant avec lui que l'on parviendra à convaincre le Parlement européen. J'y étais avant-hier et j'ai constaté des évolutions considérables par rapport au mois de juin. J'ai communiqué les nouveaux éléments à la commission des libertés civiles, de la justice et des affaires intérieures, dont le président m'est apparu beaucoup plus ouvert qu'auparavant. A l'exception d'une parlementaire libérale qui a fait, autant qu'il m'en a semblé, une intervention purement idéologique, je crois que la commission a beaucoup évolué.

Le Président Pierre Lequiller. Cette députée a-t-elle pour nom Sarah Ludford ?

M^me^ Michèle Alliot-Marie. Votre Commission tiendrait-elle un fichier, monsieur le Président ?

Pour le reste, je ne sais si 2009 sera l'année de la mise en place du dispositif. Au vu des données politiques – la présidence tchèque – et techniques – le renouvellement du Parlement –, je considère qu'une mise en place en 2010 serait déjà une bonne chose.

M. Jérôme Lambert. Je partage les préoccupations de Guy Geoffroy. En novembre dernier, j'ai eu connaissance d'une note relative au projet de résolution de la commission des libertés publiques du Parlement européen : j'ai été frappé par son contenu !

M^me^ Michèle Alliot-Marie. La résolution s'appuyait sur un premier rapport, établi avant l'été. Depuis, les choses ont évolué, parce que j'ai voulu les aborder concrètement et les sérier.

M. Jérôme Lambert. Si tel est le cas, je suis rassuré. J'étais préoccupé par les relations difficiles entre nos collègues du Parlement européen et le Conseil.

S'agissant des visas, les expérimentations que vous avez évoquées sont-elles systématiques ou ciblées sur certains pays ?

M^me^ Michèle Alliot-Marie. Elles sont naturellement ciblées, mais le système, d'une manière générale, est de plus en plus automatisé.

M. Jérôme Lambert. L'allongement des délais pour l'obtention des visas est-il lié à cette automatisation ?

M^me^ Michèle Alliot-Marie. Non, car la procédure est exactement la même : le consul transmet les données à la base centrale du système d'information sur les visas. Elles peuvent ensuite être examinées à des fins policières. Et si des décisions doivent être prises, elles le sont au niveau central et non dans les consulats.

M. Didier Quentin. Ce matin même, notre Commission a examiné la communication sur les scanners corporels, que M^me^ Karamanli et moi-même avons présentée. Nous sommes parvenus à la conclusion suivante : « *Le scanner corporel constitue certainement un outil intéressant pour procéder à la fouille d'un passager, car il épargne à la personne l'obligation d'être palpée ou de se déshabiller devant un tiers. Cependant, au vu des atteintes à l'intimité de la personne liées à l'utilisation du scanner corporel, il n'est pas possible que celui-ci puisse être mis en œuvre, fût-ce à titre expérimental – je rappelle que quelques scanners ont été installés dans la zone « abonnés » de l'aéroport de Nice-Côte d'Azur – sur le territoire français... Ce type d'appareil ne peut être utilisé que si la réglementation l'autorise expressément. Dans un domaine touchant aux libertés publiques, l'intervention du législateur est nécessaire, conformément à l'article 34 de la Constitution* ». Cela dit, nous nous félicitons du rôle joué par le Parlement européen, auquel nous nous sommes volontiers associés.

Au terme du débat, la Commission chargée des affaires européennes a adopté les conclusions suivantes : « *La Commission s'oppose à la mise en place des scanners corporels, tant que des garanties encadrant leur usage n'auront pas été fixées par la loi. A titre d'exemples, les garanties suivantes pourraient être retenues : examen par une personne seule dans un local isolé, floutage des parties sensibles, interdiction du stockage des données et, surtout, volontariat des passagers.*

« Il appartient au seul législateur, et non à l'administration, de fixer ces garanties, de nature à concilier les impératifs de sécurité et le respect des libertés publiques ».

Je vous indique que l'expérience de l'aéroport de Nice a été suspendue. Cela dit, je suis toujours surpris quand je compare les précautions que l'on prend dans les aéronefs et l'absence de précautions dans les trains internationaux et les ferries.

M^me^ Michèle Alliot-Marie. Dans les trains internationaux, il y a des patrouilles.

M. Didier Quentin. Certes, mais il serait très facile pour un terroriste d'embarquer dans un ferry et de mettre en péril plusieurs centaines de passagers.

M^me^ Michèle Alliot-Marie. En matière de lutte contre le terrorisme, il faut trouver un équilibre entre des impératifs de sécurité et le respect des libertés. Obliger chaque passager à passer un scanner provoquerait de longues files d'attente, que personne ne supporterait. Cela dit, le terrorisme a beaucoup évolué ces dernières années. Ce qui intéresse essentiellement les terroristes, c'est la communication : ce qu'ils recherchent à travers leurs actions, c'est moins de tuer des gens que d'obtenir le maximum d'impact psychologique pour déstabiliser les sociétés par le biais des médias, lesquels leur sont indispensables. Ils visent donc des moments ou des lieux particulièrement symboliques. A ce titre, il me semble que la Tour Eiffel est plus menacée qu'un ferry.

M. Didier Quentin. Mais dans un ferry, l'été, plus d'une dizaine de nationalités sont représentées.

M^me^ Michèle Alliot-Marie. Vous ne m'entendrez jamais dire qu'il existe un endroit où l'on est à l'abri d'un acte terroriste.

M. Didier Quentin. Autre sujet d'étonnement, les contrôles. L'aéroport d'Amsterdam dispose d'un scanner, mais on peut acheter des sabres au *Duty Free* et, dans l'avion, on nous propose des couverts en métal.

Vous considérez, Madame la ministre, que votre action au cours des six derniers mois est le maillon d'une longue chaîne. Dès lors, quelles doivent être, selon vous, les priorités de la présidence tchèque ?

M^me^ Michèle Alliot-Marie. Outre le PNR, les Tchèques proposent de poursuivre notre action en matière de protection civile et de lutte contre le terrorisme.

Nous avons récemment signé des accords pour établir des centres de contrôle aux frontières avec quatre pays. Outre la lutte contre le terrorisme et le crime organisé, la présidence tchèque semble vouloir faire un effort particulier en direction des nouvelles technologies, mais il ne lui est pas facile d'aborder de tels enjeux. Quant à la présidence suédoise, elle sera axée sur la lutte contre le trafic des êtres humains.

Ce que je peux vous dire, c'est que mon collègue tchèque a compris ce que nous essayons de faire et qu'il nous a apporté son soutien. J'espère qu'il restera en fonction encore quelque temps.

M. Christophe Caresche. Nous avons abordé la question des données sous l'angle de la lutte contre le terrorisme et réaffirmé notre volonté de nous en

donner les moyens. Mais nous assistons depuis plusieurs années au développement d'une nouvelle criminalité liée au transfert des données, comme le piratage de comptes bancaires – même celui du Président de la République ! Cette forme de criminalité, en forte progression, doit être combattue à la fois le plan national et sur le plan européen.

S'agissant du PNR, je rappelle que le dispositif américain a été mis en place sous la pression des événements dramatiques du 11 septembre 2001. Nous avons négocié ce PNR à deux reprises avec les Américains, mais nous avons cédé sur tous les points. La durée de conservation des données de quinze ans, mais également la transmission à des autorités non identifiées en font un dispositif très déséquilibré.

Il y a environ un an, j'ai participé à une rencontre interparlementaire sur ces questions : j'ai été surpris de la sensibilité des parlementaires européens et des parlementaires nationaux allemands à ces thèmes. Je suppose que le Parlement européen sera très attentif à tout ce qui sera fait dans ce domaine et je compte sur l'Europe pour réaliser un PNR acceptable. Mais pourrons-nous concilier un PNR américain, totalement déséquilibré, et un PNR européen reposant sur une durée de conservation des données de trois ans et sur des garanties beaucoup plus importantes ? Les autorités européennes ne seront-elles pas amenées à engager une négociation sur le PNR américain ? Il serait paradoxal que l'Europe adopte une disposition conservatoire en matière de libertés, tout en acceptant que le PNR américain les bafoue !

M^me^ Michèle Alliot-Marie. Je suis d'accord avec vous, la criminalité liée à la falsification des données et à leur utilisation fallacieuse se développe. C'est pourquoi je m'apprête à lancer, dans quelques semaines, un grand plan de lutte contre les escroqueries, notamment celles liées à internet, en pleine extension dans notre pays. Nous allons répondre en partie à ce problème avec le titre d'identité sécurisé, dont l'objectif est d'empêcher les captations d'identité, ce qui devrait permettre de bloquer une partie de ces escroqueries.

En matière de protection des données personnelles, nous mettons en place un système assurant la traçabilité. Au-delà de la sécurisation du dispositif, la traçabilité permet de vérifier que personne ne peut utiliser sa fonction pour vendre des données. J'ajoute que les sanctions qui s'appliquent à un tel délit sont exemplaires.

S'agissant du PNR européen, je peux vous dire que nos propositions ont été très bien reçues. Quant aux Américains, il est clair qu'ils recherchent le dialogue, mais j'ai indiqué à mon homologue américain qu'il ne pourrait y avoir de dialogue entre nous tant que son pays ne prévoira pas de garanties équivalentes aux garanties européennes. Je reconnais que c'est un point de blocage, auquel je ne désespère pas de trouver une issue. Quoi qu'il en soit, rien ne sera fait avant l'entrée en fonction de la nouvelle administration américaine.

M^me^ Marietta Karamanli. Je partage les préoccupations de mes collègues sur l'utilisation et la protection des données. Cela étant, je voudrais souligner l'importance des évaluations périodiques du PNR européen.

S'agissant des scanners corporels, nous avons en effet insisté, ce matin même, sur la nécessité d'être vigilants et de fixer dans la loi française un cadre juridique à ce dispositif, qui, s'il touche aux libertés publiques, pose peut-être également un problème de santé publique et d'efficacité financière.

Le Président Pierre Lequiller. Le Gouvernement envisage-t-il de déposer un texte sur cette question ?

M^me^ Michèle Alliot-Marie. Le Parlement aura à légiférer sur tout ce qui a trait aux titres sécurisés. Sur la mise en place du scanner corporel, j'avoue être réticente, et je pense qu'il est urgent de ne pas se presser… D'ailleurs, je ne suis pas certaine que cette question relève du domaine législatif – même si le Parlement a un droit de regard sur tout ce qui relève du domaine réglementaire.

M. Christophe Caresche. J'ai cru comprendre que la France appliquait avec une rigueur particulière les dispositions européennes en matière de contrôle dans les aéroports, au risque de perturber les transports par des mesures trop contraignantes.

M^me^ Michèle Alliot-Marie. Je ne peux vous répondre pour l'ensemble des pays européens, mais je sais que, dans nombre d'entre eux, l'application des règles européennes est au moins aussi rigoureuse que dans notre pays. Il est vrai que certains systèmes sont aberrants, et je reconnais, s'agissant des règles appliquées en France, qu'il est difficile de commettre un attentat avec une pince à épiler.

J'ai par ailleurs l'intention d'engager une réflexion sur la confiscation automatique d'objets personnels, étant entendu que les contrôles sont souvent confiés à des sociétés privées.

M^me^ Marietta Karamanli. Ce contrôle a été mis en place à partir d'un unique incident et il devrait être supprimé en 2010. Nous savons qu'il mobilise d'énormes moyens humains, mais son efficacité n'est pas démontrée.

Le Président Pierre Lequiller. De plus, il ternit l'image de l'Europe.

M^me^ Michèle Alliot-Marie. C'est encore pire aux Etats-Unis et en Chine – sans parler d'Israël ! Certaines personnes sont tétanisées par un tel contrôle. Nous devons certes être vigilants, mais en évitant d'en faire trop.

M^me^ Marietta Karamanli. Vous dites que nous vivons sous la menace constante d'un terrorisme qui joue sur la peur : faisons en sorte de ne pas alimenter cette peur.

J'ai été très sensible à vos propos sur la protection, mais cela ne suffit pas. Les lois sociales contribuent à la protection des personnes ; or les lois sociales européennes font cruellement défaut – mais je sais bien que vous ne pouvez agir sur l'ensemble des Etats de l'Union européenne.

M^me^ Michèle Alliot-Marie. Je suis tout à fait favorable aux lois sociales. Il y a longtemps que je plaide pour l'Europe sociale – j'ai même fait mes débuts en politique sur ce thème –, d'autant que notre pays y gagnerait sur le plan économique. J'avais même fait une proposition en ce sens à Jacques Delors – qui l'avait refusée –, selon laquelle l'Europe devait demander à l'Espagne, en contrepartie de fonds structurels, de faire des efforts en matière de protection sociale. Cela aurait eu pour effet d'augmenter les prix de revient espagnols, qui faussaient la concurrence au détriment de ma région, le Pays Basque. Si cela avait été fait, il est probable que les entreprises françaises en auraient bénéficié.

M^me^ Marietta Karamanli. En effet, les présidences européennes se succèdent et aucune ne fait sienne cette priorité.

M^me^ Michèle Alliot-Marie. Pour une raison simple : les pays qui ont peu de protection sociale ne souhaitent pas procéder à des améliorations. Sur ce point, la Commission, quel que soit son président, n'a guère avancé.

M. Gérard Voisin. En tant qu'élu d'un territoire voisin de la Suisse, je suis très heureux d'apprendre que l'Union européenne a donné son feu vert à l'entrée de ce pays dans l'espace Schengen. En vertu du principe de libre circulation, tous les ressortissants de l'Union auront la possibilité de s'installer en Suisse pour travailler, et inversement. Mais est-ce véritablement une avancée, dans la mesure où la Suisse est déjà une passoire ?

M^me^ Michèle Alliot-Marie. Cet accord porte surtout sur les transports. Après les frontières terrestres, l'ouverture des frontières aériennes est prévue en mars 2009. Cela supprimera certaines choses et entraînera une coopération.

M. Gérard Voisin. Justement, cela ne supprime pas grand-chose…

M^me^ Michèle Alliot-Marie. Si, au niveau des frontières.

M. Gérard Voisin. Notre président m'a chargé de réfléchir à une proposition de directive visant à faciliter l'application transfrontalière de la législation en matière de sécurité routière. Je sais déjà ce qu'en pensent les Français, mais quel est votre sentiment personnel, Madame la ministre ?

M^me^ Michèle Alliot-Marie. Il est absolument indispensable d'appliquer de façon similaire les règles de sécurité routière dans tous les pays européens. Actuellement, les Belges, les Britanniques et les Néerlandais viennent faire du rodéo sur les routes françaises, protégés par le fait que leur permis de conduire a été délivré dans un autre pays. Je suis tout à fait favorable à un système qui nous

permettrait de retenir le permis de conduire de ceux qui enfreignent les règles de sécurité sur notre territoire.

D'autres harmonisations sont envisageables et nous avons intérêt à rapprocher les réglementations en la matière – je pense aux limitations de vitesse, qui diffèrent selon les pays. Il faudra régler ces questions, qui relèvent du domaine réglementaire. Il serait intéressant, monsieur Voisin, que vous évoquiez dans votre rapport la nécessité d'une plus grande homogénéité des règles de circulation.

Je regarde ce qui se passe à l'étranger : pour lutter contre l'alcool au volant, les juges, en Allemagne et aux Pays-Bas, peuvent prononcer en tant que peine complémentaire l'installation d'éthylotests obligatoires. Je vous proposerai donc une mesure similaire dans la loi d'orientation et de programmation pour la sécurité intérieure.

M. Robert Lecou. Je tiens tout d'abord à vous remercier, madame la ministre, d'avoir maintenu la présence d'un escadron de gendarmerie dans une commune de ma circonscription.

La réforme de la gendarmerie va-t-elle entraîner des modifications au niveau des unités d'élite françaises chargées de lutter contre le terrorisme ?

M. Jacques Desallangre. Allez-vous, Madame la ministre, revoir l'harmonisation sur le terrain – par exemple, dans un bassin d'emploi de 70 000 habitants où cohabitent la gendarmerie et la police ?

M^me^ Michèle Alliot-Marie. Naturellement !

Il n'est pas question de fusionner les unités d'élite, car j'ai besoin des savoir-faire des uns et des autres. Le GIGN et le RAID existeront comme tels. En revanche, j'ai souhaité qu'ils participent à des entraînements communs. Nous avons organisé une simulation de prise d'otages au Stade de France. Pour la première fois, ces unités ont travaillé ensemble, et cette opération fut extrêmement instructive.

Il paraît logique de mutualiser les formations de plongeurs ou les formations cynophiles, mais il n'est nullement question de toucher aux spécificités des uns et des autres.

Je reviens sur la sécurité routière, pour vous indiquer que j'envisage d'affecter des effectifs de la gendarmerie des autoroutes à la surveillance des routes secondaires, où le nombre d'accidents est très supérieur.

Depuis six ans, la gendarmerie nationale est mise à la disposition du ministre de l'intérieur pour les actions de sécurité. Au reste, nous avons lancé une réforme des structures pour donner plus de cohérence au dispositif : les zones urbaines étant réservées à la police ; les zones rurales étant réservées à la gendarmerie. Il est à noter que certaines brigades de gendarmerie qui se trouvaient

auparavant en zone rurale se retrouvent aujourd'hui en zone péri-urbaine, voire en zone urbaine. Il est important d'utiliser les spécificités de la gendarmerie. Or, ce qui la différencie de la police, c'est essentiellement sa capacité de renseignement. Son rôle repose sur les contacts qu'elle noue avec la population. Les renseignements qu'elle a fournis ont souvent été très utiles, notamment dans la lutte contre l'ETA. Lorsqu'ils se retrouvent dans une cité-dortoir, les gendarmes ne peuvent plus jouer ce rôle. Dans cette logique, il y aura des ajustements, mais ils seront marginaux – une vingtaine seulement – alors que nous avions procédé, il y quelques années, à environ 450 modifications dont le coût, en termes de logements, s'élevait à plus de 15 millions d'euros.

Le Président Pierre Lequiller. Je vous remercie, Madame la ministre, d'avoir répondu à toutes nos questions.

*

* *

3. Examen du rapport d'information de M. Guy Geoffroy sur les données des dossiers passagers (PNR) à des fins répressives, le mercredi 11 février 2009

La Commission s'est réunie le mercredi 11 février 2009, sous la présidence de M. Thierry Mariani, Vice-président, pour examiner le présent rapport d'information.

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

Le Président Thierry Mariani. C'est un sujet important pour l'avenir. Ces données sont certainement un outil nécessaire pour prévenir des actions terroristes et la proposition de ramener leur délai de conservation à une durée de trois à six ans est certainement plus raisonnable. Trois questions se posent : quelle est la position de la nouvelle administration américaine dans ce domaine, comment assurer le respect des libertés à chaque étape de la collecte et du traitement des données et qu'en sera-t-il de la réciprocité de leur accès pour les pays tiers ?

Le rapporteur. Il n'y a pas encore d'information précise quant à l'attitude de la nouvelle administration américaine même si on peut estimer qu'elle ne changera guère.

La protection des données à chaque étape est essentielle, de la transmission par les compagnies aériennes jusqu'à, le cas échéant, la transmission d'un Etat membre vers un pays tiers. Le recueil des données doit être encadré, tout comme leur traitement ultérieur, bien que l'utilisation faite par les autorités répressives relève bien entendu du droit national.

En matière de réciprocité, l'établissement d'un recueil de données PNR au niveau européen permettra de négocier, avec nos principes, sur des bases solides et équilibrées avec des pays comme les Etats-Unis et l'Australie. Il faut relever que la Grande-Bretagne a bien pris part au débat sur le projet alors qu'elle-même dispose déjà de son propre régime de collecte et de traitement.

M. Jérôme Lambert. Il est nécessaire de tout mettre en œuvre pour lutter contre le terrorisme mais il est permis d'être dubitatif sur le fait de récolter ainsi des milliards de données. Sommes-nous face à une forme de dérive ?

La proposition de résolution insiste de façon positive sur le nécessaire respect de la vie privée mais celui-ci apparaît contradictoire avec le principe même du recueil de données comme, par exemple, celui des habitudes alimentaires. L'atteinte à la vie privée est indéniable. Je ne méconnais pas la nécessité de la lutte contre le terrorisme, mais un certain scepticisme est de mise quant à l'efficacité d'une collecte de données sur une aussi vaste échelle.

Les terroristes voulant arriver à leurs fins emploieront un certain nombre de moyens afin de ne pas être découverts. Il me semble donc que le point crucial est de repérer le terroriste avant qu'il ne monte dans l'avion, les moyens les plus importants devant être employés en amont.

Je ne m'oppose pas à cette résolution mais le Parlement européen a émis des réserves compte tenu des possibilités de dérives. Le risque terroriste existe mais ce n'est pas avec de telles mesures qu'on s'attaquera aux racines du mal.

M. Gérard Voisin. Je rejoins un peu notre collègue Jérôme Lambert car on s'expose à se noyer dans les détails. J'approuve le rapport mais toutes ces mesures consomment du temps et sont coûteuses. Finalement, trop de sécurité tue la sécurité.

Le rapporteur. Les demandes de certains repas sont des informations sensibles. Je suis persuadé qu'on ne pourra pas échapper au recueil de ces données qui ne devraient être utilisées que dans le cadre de poursuites déjà engagées. Mais ce point fait encore l'objet de discussions. Le problème central est de rendre conciliables la défense des libertés individuelles et la lutte contre le terrorisme. Il est certain que cet outil touche aux libertés fondamentales mais ces atteintes doivent être proportionnées et strictement encadrées. Il est préférable d'avoir un dispositif cohérent en Europe qui minimisera les inconvénients plutôt que des régimes disparates et de se trouver en grand déséquilibre avec les Etats auxquels les données PNR sont transférées et qui n'ont pas d'état d'âme.

Le Président Thierry Mariani. Les terroristes sauront probablement trouver des parades. Il me semble qu'on réagit continuellement avec retard comme le montre le fait que le contrôle des explosifs persiste alors que cette menace contre les avions a pratiquement disparu.

Les attentats du 11 septembre 2001 ont montré que le problème essentiel résidait dans l'utilisation de faux papiers. J'estime donc que le moyen le plus efficace réside dans le contrôle des attributions de papiers d'identité, notamment de la part de certains pays.

Enfin il ne faut pas se cacher que ces recueils de données PNR sont utilisés comme un moyen d'espionnage économique autant que comme arme de lutte contre le terrorisme. Je suis vraiment persuadé que la lutte contre les faux passeports devrait être prioritaire en ce domaine. »

Sur proposition du rapporteur, la Commission *a* ensuite *adopté* la proposition de résolution dont le texte figure ci-après.

PROPOSITION DE RESOLUTION

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.

ANNEXE :
LISTE DES PERSONNES ENTENDUES PAR LE RAPPORTEUR

- Mme Michèle ALLIOT-MARIE, ministre de l'intérieur, de l'outre-mer et des collectivités territoriales ;

- M. Alex TURK, président de la Commission nationale de l'informatique et des libertés ;

- M. Jonathan FAULL, directeur général de la DG « Justice liberté et sécurité » à la Commission européenne **;**

- M. Peter HUSTINX, contrôleur européen de la protection des données ;

- M. Daniel LECRUBIER, Conseiller, chef du service JAI, et Mme Claire Rocheteau, conseiller JAI à la Représentation permanente de la France auprès de l'Union européenne ;

- M. Laurent TOUVET, directeur des libertés publiques et des affaires juridiques (DLPAJ), ministère de l'intérieur, de l'outre-mer et des collectivités territoriales ;

- M. Jacques POINAS, inspecteur général de la police nationale, mission de la Présidence française pour l'Union européenne, ministère de l'intérieur, de l'outre-mer et des collectivités territoriales ;

- Mme Muriel SYLVAN, attachée principale d'administration centrale, mission Présidence française pour l'Union européenne, ministère de l'intérieur, de l'outre-mer et des collectivités territoriales ;

- M. Gérard SCHOEN, sous-directeur des affaires juridiques, du contentieux, des contrôles et de la lutte contre la fraude à la direction générale des douanes, ministère du budget, des comptes publics et de la fonction publique ;

- M. Patrick LANSMAN, sous-directeur de la concurrence, de la facilitation et des clients à la direction générale de l'aviation civile, ministère de l'écologie, de l'énergie, du développement durable et de l'aménagement du territoire ;

- Mme Laurence NAVARRI, adjointe au bureau de la législation pénale générale, direction des affaires criminelles et des grâces, ministère de la justice.

*

* *