AIX-MARSEILLE UNIVERSITE

FACULTÉ DE DROIT ET DE SCIENCE POLITIQUE

INSTITUT DE FORMATION UNIVERSITAIRE ET DE RECHERCHE DU TRANSPORT AERIEN

MASTER 2 Professionnel

Droit et Management du Transport Aérien

MÉMOIRE DE FIN D'ÉTUDES

Année 2017 - 2018

ETUDE DE LA MISE EN ŒUVRE DE LA DIRECTIVE PNR

ANNEXES

THABET LEILA

Sous la direction de :
Madame Julie LABORDE, Directrice de l'IFURTA,
et de
Monsieur Jean FRAYSSINET, Professeur Emérite
de la Faculté de droit d'Aix-En-Provence

3 avenue Robert Schuman - 13628 Aix-en-Provence Cedex 1

ANNEXE 1

DIRECTIVE (UE) 2016/681 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 27 avril 2016

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

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 82, paragraphe 1, point d), et son article 87, paragraphe 2, point a),

vu la proposition de la Commission européenne,

après transmission du projet d'acte

législatif aux parlements nationaux,

vu l'avis du Comité économique et

social européen ([1]),

après consultation du Comité des régions,

statuant conformément à la

procédure législative

ordinaire ([2]), considérant

ce qui suit:

(1) Le 6 novembre 2007, la Commission a adopté une proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (PNR) à des fins répressives. Cependant, n'ayant pas encore été adoptée par le Conseil lors de l'entrée en vigueur du traité de Lisbonne le 1er décembre 2009, la proposition de la Commission est devenue obsolète.

(2) «Le programme de Stockholm — Une Europe ouverte et sûre qui sert et protège les citoyens» ([3]) invite la Commission à présenter une proposition concernant l'utilisation des données PNR aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité, ainsi que des enquêtes et des poursuites en la matière.

(3) Dans sa communication du 21 septembre 2010 relative à la démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers, la Commission a décrit un certain nombre d'éléments essentiels d'une politique de l'Union dans ce domaine.

(4) La directive 2004/82/CE du Conseil ([4]) régit la transmission aux autorités nationales compétentes, par les transporteurs aériens, d'informations préalables relatives aux passagers (ci-après dénommées «données API»), en vue d'améliorer les contrôles aux frontières et de lutter contre l'immigration illégale.

(5) Les objectifs de la présente directive sont, entre autres, d'assurer la sécurité, de protéger la vie et la sécurité des personnes, et de créer un cadre juridique pour la

protection des données PNR en ce qui concerne leur traitement par les autorités compétentes.

(6) L'utilisation effective des données PNR, par exemple la confrontation des données PNR à diverses bases de données de personnes ou d'objets recherchés, est nécessaire pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, et donc pour renforcer la sécurité intérieure, pour rassembler des preuves et, le cas échéant, pour trouver les complices de criminels et démanteler des réseaux criminels.

(7) L'évaluation des données PNR permet d'identifier des personnes qui n'étaient pas soupçonnées de participation à des infractions terroristes ou à des formes graves de criminalité avant cette évaluation et qui devraient être soumises à un examen plus approfondi par les autorités compétentes. L'utilisation des données PNR permet de contrer la menace que représentent les infractions terroristes et les formes graves de criminalité sous un angle autre que par le traitement d'autres catégories de données à caractère personnel. Cependant, pour veiller à ce que le traitement de données PNR reste limité à ce qui est nécessaire, la création et l'application de critères d'évaluation devraient être limitées aux infractions terroristes et aux formes graves de criminalité pour lesquelles l'utilisation de tels critères est pertinente. Par ailleurs, les critères d'évaluation devraient être définis d'une manière qui réduise au minimum le nombre d'identifications erronées de personnes innocentes par le système.

---

(1) JO C 218 du 23.7.2011, p. 107.
(2) Position du Parlement européen du 14 avril 2016 (non encore parue au Journal officiel) et décision du Conseil du 21 avril 2016. (3) JO C 115 du 4.5.2010, p. 1.

(8) Les transporteurs aériens recueillent et traitent déjà des données PNR de leurs passagers pour leur propre usage commercial. La présente directive ne devrait pas leur imposer l'obligation de recueillir ou de conserver des données supplémentaires des passagers et ne devrait pas non plus contraindre les passagers à communiquer des données en sus de celles qui sont déjà transmises aux transporteurs aériens.

(9) Certains transporteurs aériens conservent les données API qu'ils recueillent en les regroupant avec les données PNR, alors que d'autres ne le font pas. L'utilisation combinée des données PNR et des données API présente une valeur ajoutée en ce qu'elle aide les États membres à vérifier l'identité d'une personne, renforçant ainsi la valeur du résultat en termes de prévention, de détection et de répression des infractions et réduisant au minimum le risque de soumettre des personnes innocentes à des vérifications et à des enquêtes. C'est pourquoi il est important de veiller à ce que, lorsque les transporteurs aériens recueillent des données API, ils les transfèrent, que les données API soient conservées ou non par des moyens techniques différents de ceux utilisés pour d'autres données PNR.

(10) Aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité, ainsi que des enquêtes et des poursuites en la matière, il est essentiel que tous les États membres adoptent des dispositions obligeant les transporteurs aériens qui assurent des vols extra-UE à transférer les données PNR qu'ils recueillent, y compris les données API. Les États membres devraient également avoir la possibilité d'étendre cette obligation aux transporteurs aériens qui assurent des vols intra-UE. Ces dispositions devraient s'entendre sans préjudice de la directive 2004/82/CE.

(11) Le traitement des données à caractère personnel devrait être proportionné aux objectifs de sécurité spécifiques poursuivis par la présente directive.

(12) La définition des infractions terroristes appliquée dans le cadre de la présente directive devrait être la même que celle figurant dans la décision-cadre 2002/475/JAI du Conseil (1). La définition des formes graves de criminalité devrait englober les catégories d'infractions énumérées à l'annexe II de la présente directive.

(13) Il convient que les données PNR soient transmises à une seule unité d'information passagers désignée (UIP) dans l'État membre concerné, de manière à garantir la clarté

et à réduire les coûts supportés par les transporteurs aériens. L'UIP peut avoir plusieurs antennes dans un même État membre et les États membres peuvent également mettre en place conjointement une seule UIP. Les États membres devraient échanger leurs informations par l'inter- médiaire de réseaux d'échange d'informations appropriés afin de faciliter le partage des informations et de garantir l'interopérabilité.

(14) Les États membres devraient assumer les coûts liés à l'utilisation, à la conservation et à l'échange de données PNR.

(15) Une liste des données PNR à transmettre à une UIP devrait être établie dans le but de refléter les exigences légitimes des pouvoirs publics en matière de prévention et de détection des infractions terroristes ou des formes graves de criminalité, ainsi que d'enquêtes et de poursuites en la matière, renforçant par là la sécurité intérieure de l'Union et la protection des droits fondamentaux, notamment le respect de la vie privée et la protection des données à caractère personnel. À cette fin, il convient d'appliquer des normes élevées conformément à la Charte des droits fondamentaux de l'Union européenne (ci-après dénommée «Charte»), la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ci-après dénommée «convention n° 108») et la convention de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH). Une telle liste ne devrait pas être fondée sur l'origine raciale ou ethnique, la religion ou les convictions, les opinions politiques ou toute autre opinion, l'appartenance à un syndicat, la santé, la vie sexuelle ou l'orientation sexuelle d'une personne. Les données PNR ne devraient comporter que des informations relatives aux réservations et aux itinéraires de voyage des passagers qui permettent aux autorités compétentes d'identifier les passagers aériens représentant une menace pour la sécurité intérieure.

(16) Actuellement, deux méthodes de transfert des données sont possibles: la méthode «pull», par laquelle les autorités compétentes de l'État membre qui requièrent les données PNR peuvent accéder au système de réservation du transporteur aérien et en extraire («pull») une copie des données PNR requises, et la méthode «push», par laquelle les transporteurs aériens transmettent («push») les données PNR requises à l'autorité requérante, ce qui permet aux transporteurs aériens de garder le contrôle sur les données transmises. La méthode «push» est réputée offrir un niveau plus élevé de protection des données et devrait être obligatoire pour tous les transporteurs aériens.

([1]) Décision-cadre 2002/475/JAI du Conseil du 13 juin 2002 relative à la lutte contre le terrorisme (JO L 164 du 22.6.2002, p. 3).

(17) La Commission soutient les lignes directrices de l'organisation de l'aviation civile internationale (OACI) relatives aux données PNR. Ces lignes directrices devraient, par conséquent, servir de base pour l'adoption des formats de données reconnus pour les transferts des données PNR par les transporteurs aériens aux États membres. Afin d'assurer des conditions uniformes d'exécution des formats de données reconnus et des protocoles correspondants applicables au transfert des données provenant des transporteurs aériens, il convient de conférer des compétences d'exécution à la Commission. Ces compétences devraient être exercées en conformité avec le règlement (UE) n° 182/2011 du Parlement européen et du Conseil ([1]).

(18) Les États membres devraient prendre toutes les mesures nécessaires pour permettre aux transporteurs aériens de remplir leurs obligations au titre de la présente directive. Il y a lieu que les États membres prévoient des sanctions effectives, proportionnées et dissuasives, y compris des sanctions financières, à l'encontre des transporteurs aériens qui ne respectent pas leurs obligations en matière de transfert de données PNR.

(19) Chaque État membre devrait être responsable de l'évaluation des menaces potentielles liées aux infractions terroristes et aux formes graves de criminalité.

(20) En tenant pleinement compte du droit à la protection des données à caractère personnel et du droit à la non- discrimination, aucune décision qui produit des effets juridiques préjudiciables à une personne ou l'affecte de manière significative ne devrait être prise sur la seule base du traitement automatisé des données PNR. Par

ailleurs, conformément aux articles 8 et 21 de la Charte, aucune décision de cette nature ne devrait introduire de discrimination fondée notamment sur le sexe, la race, la couleur, les origines ethniques ou sociales, les caractéris- tiques génétiques, la langue, la religion ou les convictions, les opinions politiques ou toute autre opinion, l'appartenance à une minorité nationale, la fortune, la naissance, un handicap, l'âge ou l'orientation sexuelle. La Commission devrait également prendre en compte ces principes lors du réexamen de l'application de la présente directive.

(21) Le résultat du traitement des données PNR ne devrait en aucun cas être utilisé par les États membres comme motif pour se soustraire à leurs obligations internationales au titre de la convention du 28 juillet 1951 relative au statut des réfugiés, telle qu'amendée par le protocole du 31 janvier 1967, ni être invoqué pour refuser aux demandeurs d'asile des voies sûres et effectives d'entrée légales sur le territoire de l'Union afin d'y exercer leur droit à la protection internationale.

(22) En tenant pleinement compte des principes mis en évidence par la récente jurisprudence pertinente de la Cour de justice de l'Union européenne, l'application de la présente directive devrait garantir le plein respect des droits fondamentaux et du droit au respect de la vie privée ainsi que du principe de proportionnalité. Elle devrait aussi véritablement remplir les objectifs de nécessité et de proportionnalité afin de répondre aux intérêts généraux reconnus par l'Union et à la nécessité de protéger les droits et libertés d'autrui dans la lutte contre les infractions terroristes et les formes graves de criminalité. L'application de la présente directive devrait être dûment justifiée et les garanties nécessaires devraient être mises en place afin d'assurer la légalité de tout stockage, de toute analyse, de tout transfert ou de toute utilisation des données PNR.

(23) Les États membres devraient échanger entre eux et avec Europol les données PNR qu'ils reçoivent, lorsque cela est jugé nécessaire aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité, ainsi que des enquêtes et des poursuites en la matière. Les UIP devraient, le cas échéant, transmettre sans tarder le résultat du traitement des données PNR aux UIP des autres États membres en vue d'un complément d'enquête. Les dispositions de la présente directive devraient s'entendre sans préjudice d'autres instruments de l'Union relatifs à l'échange d'informations entre les services de police et d'autres services répressifs et les autorités judiciaires, y compris la décision 2009/371/JAI du Conseil ([2]) et la décision-cadre 2006/960/JAI du Conseil ([3]). Il convient que les échanges de données PNR soient régis par les règles relatives à la coopération policière et judiciaire et ne portent pas atteinte au niveau élevé de protection de la vie privée et des données à caractère personnel exigé par la Charte, la convention n° 108 et la CEDH.

(24) L'échange sécurisé d'informations relatives aux données PNR entre les États membres devrait être assuré par l'intermédiaire de tout canal de coopération existant entre les autorités compétentes des États membres, et en particulier avec Europol, par l'intermédiaire de son application de réseau d'échange sécurisé d'informations (SIENA).

---

(1) Règlement (UE) n° 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

(2) Décision 2009/371/JAI du Conseil du 6 avril 2009 portant création de l'Office européen de police (Europol) (JO L 121 du 15.5.2009, p. 37).

(3) Décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de rensei- gnements entre les services répressifs des États membres de l'Union européenne (JO L 386 du 29.12.2006, p. 89).

(25) Les données PNR ne devraient être conservées que pour la durée nécessaire et proportionnée aux objectifs de prévention et de détection des infractions terroristes et des formes graves de criminalité, ainsi que d'enquêtes et de poursuites en la matière.

En raison de leur nature et de leurs utilisations, il est indispensable que les données PNR soient conservées pendant une période suffisamment longue pour permettre leur analyse et leur utilisation dans le cadre d'enquêtes. Pour éviter toute utilisation disproportionnée, il convient que, après le délai initial de conservation, les données PNR soient dépersonnalisées par le masquage d'éléments des données. Afin de garantir le niveau le plus élevé de protection de données, l'accès à l'intégralité des données PNR, qui permettent l'identifi- cation directe de la personne concernée, ne devrait être accordé que dans des conditions très strictes et limitées après ce délai initial.

(26) Lorsque des données PNR spécifiques ont été transmises à une autorité compétente et servent dans le cadre d'enquêtes ou de poursuites pénales spécifiques, leur durée de conservation par cette autorité devrait être fixée par le droit national, indépendamment des périodes de conservation de données prévues par la présente directive.

(27) Dans chaque État membre, le traitement de données PNR effectué par l'UIP et par les autorités compétentes devrait être soumis à une norme de protection des données à caractère personnel du droit national conforme à la décision-cadre 2008/977/JAI du Conseil ([1]) et aux exigences spécifiques de protection des données énoncées dans la présente directive. Les références à la décision-cadre 2008/977/JAI devraient s'entendre comme des références faites à la législation actuellement en vigueur ainsi qu'à la législation qui la remplacera.

(28) Compte tenu du droit à la protection des données à caractère personnel, il convient que les droits des personnes concernées en ce qui concerne le traitement de leurs données PNR, tels que les droits d'accès, de rectification, d'effacement et de limitation, ainsi que le droit à réparation et le droit à un recours juridictionnel, soient conformes à la décision-cadre 2008/977/JAI et au niveau de protection élevé conféré par la Charte et la CEDH.

(29) Eu égard au droit des passagers d'être informés du traitement des données à caractère personnel les concernant, les États membres devraient veiller à ce que les passagers reçoivent des informations précises, aisément accessibles et facilement compréhensibles, sur la collecte des données PNR, le transfert de celles-ci à l'UIP et leurs droits en tant que personnes concernées.

(30) La présente directive s'applique sans préjudice du droit de l'Union et du droit national concernant le principe de l'accès du public aux documents officiels.

(31) Les États membres ne devraient être autorisés à transférer des données PNR vers des pays tiers qu'au cas par cas et dans le plein respect des dispositions adoptées par les États membres en vertu de la décision-cadre 2008/977/JAI. Pour assurer la protection des données à caractère personnel, ces transferts devraient être soumis à des exigences supplémentaires relatives à leur finalité. Ils devraient également être soumis aux principes de nécessité et de proportionnalité et au niveau de protection élevé conféré par la Charte et la CEDH.

(32) Les autorités de contrôle nationales mises en place en application de la décision-cadre 2008/977/JAI devraient également être chargées de fournir des conseils sur l'application des dispositions adoptées par les États membres en vertu de la présente directive et de surveiller l'application de celles-ci.

(33) La présente directive est sans préjudice de la possibilité pour les États membres de prévoir, en vertu de leur droit national, un système de collecte et de traitement des données PNR auprès d'opérateurs économiques autres que les transporteurs, tels que des agences ou des organisateurs de voyages qui fournissent des services liés aux voyages, y compris la réservation de vols, pour lesquels ils recueillent et traitent les données PNR, ou de transporteurs autres que ceux que la présente directive mentionne, sous réserve que ce droit national respecte le droit de l'Union.

(34) La présente directive est sans préjudice des règles actuelles de l'Union sur les modalités des contrôles aux frontières ou des règles de l'Union régissant l'entrée sur le territoire del'Union et la sortie de celui-ci.

(1) 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 (JO L 350 du 30.12.2008, p. 60).

(35) Comme les dispositions nationales relatives au traitement des données à caractère personnel, y compris des données PNR, divergent sur le plan juridique et technique, les transporteurs aériens doivent et devront faire face à des exigences différentes en ce qui concerne le type d'informations à transmettre et les conditions dans lesquelles ces informations doivent être communiquées aux autorités nationales compétentes. Ces divergences peuvent nuire à une coopération efficace entre ces autorités aux fins de la prévention et de la détection des infractions terroristes ou des formes graves de criminalité, ainsi que des enquêtes et des poursuites en la matière. Il est dès lors nécessaire d'établir, au niveau de l'Union, un cadre juridique commun pour le transfert et le traitement des données PNR.

(36) La présente directive respecte les droits fondamentaux et les principes énoncés dans la Charte, en particulier le droit à la protection des données à caractère personnel, le droit au respect de la vie privée et le droit à la non- discrimination consacrés par ses articles 8, 7 et 21; elle devrait dès lors être mise en œuvre en conséquence. La présente directive est compatible avec les principes de la protection des données et ses dispositions sont conformes à la décision-cadre 2008/977/JAI. En outre, afin de respecter le principe de proportionnalité, la présente directive prévoit, pour des points spécifiques, des règles de protection des données plus strictes que celles prévues dans la décision-cadre 2008/977/JAI.

(37) Le champ d'application de la présente directive est aussi limité que possible dès lors que: il prévoit que la conservation des données PNR dans les UIP est autorisée pendant une période n'excédant pas cinq ans au terme de laquelle les données devraient être effacées; il prévoit que les données sont dépersonnalisées par le masquage d'éléments des données après une période initiale de six mois; et il interdit la collecte et l'utilisation des données sensibles. Pour garantir l'efficacité et un niveau élevé de protection des données, les États membres sont tenus de veiller à ce qu'une autorité de contrôle nationale indépendante et, notamment, un délégué à la protection des données soient chargés de fournir des conseils et de surveiller la manière dont les données PNR sont traitées. Tout traitement de données PNR devrait être consigné ou faire l'objet d'une trace documentaire à des fins de vérification de sa licéité et d'autocontrôle et pour garantir de manière adéquate l'intégrité des données et la sécurité du traitement. Les États membres devraient également veiller à ce que les passagers reçoivent des informations claires et précises sur la collecte des données PNR et sur leurs droits.

(38) Étant donné que les objectifs de la présente directive — à savoir le transfert de données PNR par les transporteurs aériens et leur traitement aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière — ne peuvent pas être atteints de manière suffisante par les États membres mais peuvent l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité tel qu'énoncé audit article, la présente directive n'excède pas ce qui est nécessaire pour atteindre ces objectifs.

(39) Conformément à l'article 3 du protocole n° 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, ces États membres ont notifié leur souhait de participer à l'adoption et à l'application de la présente directive.

(40) Conformément aux articles 1er et 2 du protocole nº 22 sur la position du Danemark, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, le Danemark ne participe pas à l'adoption de la présente directive et n'est pas lié par celle-ci ni soumis à son application.

(41) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 28, paragraphe 2, du règlement (CE) nº 45/2001 du Parlement européen et du Conseil ([1]) et a rendu son avis le 25 mars 2011,

([1]) Règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO L 8 du 12.1.2001, p. 1).

ONT ADOPTÉ LA PRÉSENTE DIRECTIVE:

CHAPITRE I Dispositions générales

Article premier

Objet et champ d'application

1. La présente directive prévoit:

a) le transfert, par les transporteurs aériens, de données des dossiers des passagers (PNR) de vols extra-UE;

b) le traitement des données visées au point a), notamment leur collecte, leur utilisation et leur conservation par les États membres et leur échange entre les États membres.

2. Les données PNR recueillies conformément à la présente directive ne peuvent être traitées qu'à des fins de prévention et de détection des infractions terroristes et des formes graves de criminalité ainsi que d'enquêtes et de poursuites en la matière, comme prévu à l'article 6, paragraphe 2, points a), b) et c).

Article 2

Application de la présente directive aux vols intra-UE

1. Si un État membre décide d'appliquer la présente directive aux vols intra-UE, il le notifie à la Commission par écrit. Un État membre peut adresser ou révoquer une telle notification à tout moment. La Commission publie cette notification et la révocation éventuelle de celle-ci au *Journal officiel de l'Union européenne*.

2. Lorsqu'une notification visée au paragraphe 1 est adressée, toutes les dispositions de la présente directive s'appliquent aux vols intra-UE comme s'il s'agissait de vols extra-UE et aux données PNR des vols intra-UE comme s'il s'agissait de données PNR de vols extra-UE.

3. Un État membre peut décider d'appliquer la présente directive uniquement à certains vols intra-UE. Lorsqu'il prend une telle décision, l'État membre sélectionne les vols qu'il juge nécessaires afin de poursuivre les objectifs de la présente directive. L'État membre peut décider à tout moment de modifier la sélection des vols intra-UE.

Article 3

Définitions

Aux fins de la présente directive, on entend par:

1) «transporteur aérien», une entreprise de transport aérien possédant une licence d'exploitation en cours de validité ou l'équivalent lui permettant d'assurer le transport aérien de passagers;

2) «vol extra-UE», tout vol, régulier ou non, effectué par un transporteur aérien en provenance d'un pays tiers et devant atterrir sur le territoire d'un État membre ou en provenance du territoire d'un État membre et devant atterrir dans un pays tiers, y compris, dans les deux cas, les vols comportant d'éventuelles escales sur le territoire d'États membres ou de pays tiers;

3) «vol intra-UE», tout vol, régulier ou non, effectué par un transporteur aérien en provenance du territoire d'un État membre et devant atterrir sur le territoire d'un ou de plusieurs États membres, sans escale sur le territoire d'un pays tiers;

4) «passager», toute personne, y compris une personne en correspondance ou en transit et à l'exception du personnel d'équipage, transportée ou devant être transportée par un aéronef avec le consentement du transporteur aérien, lequel se traduit par l'inscription de cette personne sur la liste des passagers;

5) «dossier(s) passager(s)» ou «PNR», un dossier relatif aux conditions de voyage de chaque passager, qui contient les informations nécessaires pour permettre le traitement et le contrôle des réservations par les transporteurs aériens concernés qui assurent les réservations, pour chaque voyage réservé par une personne ou en son nom, que ce dossier figure dans des systèmes de réservation, des systèmes de contrôle des départs (utilisés pour contrôler les passagers lors de l'embarquement) ou des systèmes équivalents offrant les mêmes fonctionnalités;

6) «système de réservation», le système interne du transporteur aérien, dans lequel les données PNR sont recueillies aux fins du traitement des réservations;

7) «méthode push», la méthode par laquelle les transporteurs aériens transfèrent les données PNR énumérées à l'annexe I vers la base de données de l'autorité requérante;

8) «infractions terroristes», les infractions prévues par le droit national visées aux articles 1er à 4 de la décision-cadre 2002/475/JAI;

9) «formes graves de criminalité», les infractions énumérées à l'annexe II qui sont passibles d'une peine privative de liberté ou d'une mesure de sûreté d'une durée maximale d'au moins trois ans au titre du droit national d'un État membre;

10) «dépersonnaliser par le masquage d'éléments des données», rendre invisibles pour un utilisateur les éléments des données qui pourraient servir à identifier directement la personne concernée.

CHAPITRE II

Responsabilités des états membres

Article 4

Unité d'informations passagers

1. Chaque État membre met en place ou désigne une autorité compétente en matière de prévention et de détection des infractions terroristes et des formes graves de criminalité, ainsi que d'enquêtes et de poursuites en la matière, ou crée ou désigne une antenne d'une telle autorité, en tant que son UIP.

2. L'UIP est chargée:

a) de la collecte des données PNR auprès des transporteurs aériens, de la conservation et du traitement de ces données, et du transfert de ces données ou du résultat de leur traitement aux autorités compétentes visées à l'article 7;

b) de l'échange à la fois des données PNR et du résultat de leur traitement avec les UIP d'autres États membres et avec Europol, conformément aux articles 9 et 10.

3. Les membres du personnel de l'UIP peuvent être des agents détachés par les autorités compétentes. Les États membres dotent les UIP des ressources adéquates pour l'accomplissement de leurs missions.

4. Deux États membres ou plus (ci-après dénommés «États membres participants») peuvent mettre en place ou désigner une autorité unique en tant qu'UIP. Cette UIP est établie dans l'un des États membres participants et est considérée comme l'UIP nationale de tous les États membres participants. Ces derniers conviennent conjointement des modalités de fonctionnement de l'UIP et respectent les exigences prévues dans la présente directive.

5. Chaque État membre notifie à la Commission la mise en place de son UIP dans un délai d'un mois à compter de cette mise en place et peut, à tout moment, modifier sa notification. La Commission publie cette notification et toute modification y afférente au *Journal officiel de l'Union européenne*.

Article 5

Délégué à la protection des données au sein de l'UIP

1. L'UIP nomme un délégué à la protection des données chargé de contrôler le traitement des données PNR et de mettre en œuvre les garanties pertinentes.

Les États membres dotent les délégués à la protection des données des moyens pour accomplir leurs missions et obligations, conformément au présent article, de

2. manière effective et en toute indépendance.

3. Les États membres veillent à ce que la personne concernée ait le droit de s'adresser au délégué à la protection des données, en sa qualité de point de contact unique, pour toutes les questions relatives au traitement des données PNR la concernant.

Article 6

Traitement des données PNR

1. Les données PNR transférées par les transporteurs aériens sont recueillies par l'UIP de l'État membre concerné comme prévu à l'article 8. Lorsque les données PNR

transférées par les transporteurs aériens comportent des données autres que celles énumérées à l'annexe I, l'UIP efface ces données immédiatement et de façon définitive dès leur réception.

2. L'UIP ne traite les données PNR qu'aux fins suivantes:

a) réaliser une évaluation des passagers avant leur arrivée prévue dans l'État membre ou leur départ prévu de celui-ci, afin d'identifier les personnes pour lesquelles est requis un examen plus approfondi par les autorités compétentes visées à l'article 7 et, le cas échéant, par Europol conformément à l'article 10, compte tenu du fait que ces personnes peuvent être impliquées dans une infraction terroriste ou une forme grave de criminalité;

b) répondre, au cas par cas, aux demandes dûment motivées fondées sur des motifs suffisants des autorités compétentes, visant à ce que des données PNR leur soient communiquées et à ce que celles-ci fassent l'objet d'un traitement dans des cas spécifiques, aux fins de la prévention et de la détection d'infractions terroristes ou de formes graves de criminalité, ainsi qu'aux fins d'enquêtes et de poursuites en la matière, et visant à communiquer aux autorités compétentes ou, le cas échéant, à Europol le résultat de ce traitement; et

c) analyser les données PNR aux fins de mettre à jour ou de définir de nouveaux critères à utiliser pour les évaluations réalisées au titre du paragraphe 3, point b), en vue d'identifier toute personne pouvant être impliquée dans une infraction terroriste ou une forme grave de criminalité.

3. Lorsqu'elle réalise l'évaluation visée au paragraphe 2, point a), l'UIP peut:

a) confronter les données PNR aux bases de données utiles aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité ainsi que des enquêtes et des poursuites en la matière, y compris les bases de données concernant les personnes ou les objets recherchés ou faisant l'objet d'un signalement, conformément aux règles nationales, internationales et de l'Union applicables à de telles bases de données; ou

b) traiter les données PNR au regard de critères préétablis.

4. L'évaluation des passagers avant leur arrivée prévue dans l'État membre ou leur départ prévu de celui-ci effectuée au titre du paragraphe 3, point b), au regard de critères préétablis est réalisée de façon non discriminatoire. Ces critères préétablis doivent être ciblés, proportionnés et spécifiques. Les États membres veillent à ce que ces critères soient fixés et réexaminés à intervalles réguliers par les UIP en coopération avec les autorités compétentes visées à l'article 7. Lesdits critères ne sont en aucun cas fondés sur l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle.

5. Les États membres s'assurent que toute concordance positive obtenue à la suite du traitement automatisé des données PNR effectué au titre du paragraphe 2, point a), est réexaminée individuellement par des moyens non automatisés, afin de vérifier si l'autorité compétente visée à l'article 7 doit prendre des mesures en vertu du droit national.

6. L'UIP d'un État membre transmet, en vue d'un examen plus approfondi, les données PNR des personnes identifiées conformément au paragraphe 2, point a), ou le résultat du traitement de ces données aux autorités compétentes visées à l'article 7 de ce même État membre. Ces transferts ne sont effectués qu'au cas par cas et, en cas de traitement automatisé des données PNR, après un réexamen individuel par des moyens non automatisés.

7. Les États membres veillent à ce que le délégué à la protection des données ait accès à toutes les données traitées par l'UIP. Si le délégué à la protection des données estime que le traitement de certaines données n'était pas licite, le délégué à la protection des données peut renvoyer l'affaire à l'autorité de contrôle nationale.

8. Le stockage, le traitement et l'analyse des données PNR par les UIP sont effectués exclusivement dans un ou des endroits sécurisés situés sur le territoire des États membres.

9. Les conséquences des évaluations des passagers visées au paragraphe 2, point a), du présent article ne compro- mettent pas le droit d'entrée des personnes jouissant du droit de l'Union à la libre circulation sur le territoire de l'État membre concerné prévu dans la directive 2004/38/CE du Parlement européen et du Conseil (1). En outre, lorsque des évaluations sont réalisées pour des vols intra-UE entre des États membres auxquels s'applique le règlement (CE) n° 562/2006 du Parlement européen et du Conseil (2), les conséquences de ces évaluations doivent respecter ledit règlement.

(1) Directive 2004/38/CE du Parlement européen et du Conseil du 29 avril 2004 relative au droit des citoyens de l'Union et des membres de leurs familles de circuler et de séjourner librement sur le territoire des États membres, modifiant le règlement (CEE) n° 1612/68 et abrogeant les directives 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE et 93/96/CEE (JO L 158 du 30.4.2004, p. 77).

(2) Règlement (CE) n° 562/2006 du Parlement européen et du Conseil du 15 mars 2006 établissant un code communautaire relatif au régime de franchissement des frontières par les personnes (code frontières Schengen) (JO L 105 du 13.4.2006, p. 1).

Article 7

Autorités compétentes

1. Chaque État membre arrête une liste des autorités compétentes habilitées à demander aux UIP ou à recevoir de celles-ci des données PNR ou le résultat du traitement de telles données en vue de procéder à un examen plus approfondi de ces informations ou de prendre les mesures appropriées aux fins de la prévention et de la détection d'infractions terroristes ou de formes graves de criminalité, ainsi que des enquêtes et des poursuites en la matière.

2. Les autorités visées au paragraphe 1 sont des autorités compétentes en matière de prévention ou de détection des infractions terroristes ou des formes graves de criminalité, ainsi que d'enquêtes ou de poursuites en la matière.

3. Aux fins de l'article 9, paragraphe 3, chaque État membre notifie à la Commission la liste de ses autorités compétentes au plus tard 25 mai 2017 et peut modifier sa notification à tout moment. La Commission publie cette notification et toute modification y afférente au *Journal officiel de l'Union européenne*.

4. Les données PNR et le résultat du traitement de ces données reçus par l'UIP ne peuvent faire l'objet d'un traitement ultérieur par les autorités compétentes des États membres qu'aux seules fins spécifiques de la prévention ou de la détection d'infractions terroristes ou de formes graves de criminalité, ainsi que des enquêtes ou des poursuites en la matière.

5. Le paragraphe 4 s'applique sans préjudice des compétences des autorités répressives ou judiciaires nationales, lorsque d'autres infractions, ou des indices d'autres infractions, sont détectés dans le cadre d'actions répressives menées à la suite de ce traitement.

6. Les autorités compétentes ne peuvent prendre aucune décision produisant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative sur la seule base du traitement automatisé de données PNR. Ces décisions ne peuvent pas être fondées sur l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle.

Article 8

Obligations imposées aux transporteurs aériens concernant les transferts de données

Les États membres adoptent les mesures nécessaires pour veiller à ce que les transporteurs aériens transfèrent, par la «méthode push», les données PNR énumérées à l'annexe I, pour autant qu'ils aient déjà recueilli de telles données dans le cours normal de leurs activités, vers la base de données de l'UIP de l'État membre sur le territoire duquel le vol atterrira ou du territoire duquel il décollera. Lorsqu'il s'agit d'un vol en partage de code entre un ou plusieurs transporteurs aériens, l'obligation de transférer les données PNR de tous les passagers du vol incombe au transporteur aérien qui assure le vol. Lorsqu'un vol extra-UE comporte une ou plusieurs escales dans des aéroports des États membres, les transporteurs aériens transfèrent les données PNR de tous les passagers aux UIP

1. de tous les États membres concernés. Il en est de même lorsqu'un vol intra-UE comporte une ou plusieurs escales dans les aéroports de différents États membres, mais uniquement en ce qui concerne les États membres qui recueillent les données PNR des vols intra- UE.

2. Dans l'hypothèse où les transporteurs aériens ont recueilli des informations préalables sur les passagers (ci-après dénommées «données API») énumérées à l'annexe I, point 18, mais ne les conservent pas par les mêmes moyens techniques que ceux utilisés pour d'autres données PNR, les États membres adoptent les mesures nécessaires pour veiller à ce que les transporteurs aériens transfèrent également ces données, par la «méthode push», à l'UIP des États membres visés au paragraphe 1. Dans le cas d'un tel transfert, toutes les dispositions de la présente directive s'appliquent à ces données API.

3. Les transporteurs aériens transfèrent les données PNR par voie électronique au moyen de protocoles communs et de formats de données reconnus à adopter en conformité avec la procédure d'examen visée à l'article 17, paragraphe 2, ou, en cas de défaillance technique, par tout autre moyen approprié garantissant un niveau de sécurité des données approprié:

a) 24 à 48 heures avant l'heure de départ programmée du vol; et

b) immédiatement après la clôture du vol, c'est-à-dire dès que les passagers ont embarqué à bord de l'aéronef prêt à partir et qu'ils ne peuvent plus embarquer ou débarquer.

4. Les États membres autorisent les transporteurs aériens à limiter le transfert visé au paragraphe 3, point b), aux mises à jour des transferts visés au point a) dudit paragraphe.

5. Lorsque l'accès à des données PNR est nécessaire pour répondre à une menace précise et réelle liée à des infractions terroristes ou à des formes graves de criminalité, les transporteurs aériens transfèrent, au cas par cas, des données PNR à d'autres moments que ceux mentionnés au paragraphe 3, à la demande d'une UIP conformément au droit national.

Article 9

Échange d'informations entre États membres

1. Les États membres veillent à ce que, en ce qui concerne les personnes identifiées par une UIP conformément à l'article 6, paragraphe 2, toutes les données PNR pertinentes et nécessaires ou le résultat du traitement de ces données soient transmis par ladite UIP aux UIP correspondantes des autres États membres. Les UIP des États membres destina- taires transmettent les informations reçues à leurs autorités compétentes, conformément à l'article 6, paragraphe 6.

2. L'UIP d'un État membre a le droit de demander, si nécessaire, à l'UIP de tout autre État membre de lui communiquer des données PNR qui sont conservées dans sa base de données et qui n'ont pas encore été dépersonna- lisées par le masquage d'éléments des données au titre de l'article 12, paragraphe 2, ainsi que, si nécessaire, le résultat de tout traitement de ces données, si celui-ci a déjà été réalisé en vertu de l'article 6, paragraphe 2, point a). Cette demande est dûment motivée. Elle peut être fondée sur un quelconque élément de ces données ou sur une combinaison de tels éléments, selon ce que l'UIP requérante estime nécessaire dans un cas spécifique de prévention ou de détection d'infractions terroristes ou de formes graves de criminalité, ou d'enquêtes ou de poursuites en la matière. Les UIP transmettent dès que possible les informations demandées. Si les données demandées ont été dépersonnalisées par le masquage d'éléments des données conformément à l'article 12, paragraphe 2, l'UIP ne transmet l'intégralité des données PNR que lorsqu'il existe des motifs raisonnables de croire que cela est nécessaire aux fins visées à l'article 6, paragraphe 2, point b), et uniquement si elle y est autorisée par une autorité visée à l'article 12, paragraphe 3, point b).

3. Les autorités compétentes d'un État membre ne peuvent demander directement à l'UIP d'un autre État membre de leur communiquer des données PNR qui sont conservées dans sa base de données que lorsque cela est nécessaire dans les cas d'urgence et dans les conditions fixées au paragraphe 2. Les demandes des autorités compétentes sont motivées. Une copie de la demande est toujours envoyée à l'UIP de l'État membre requérant. Dans tous les autres cas, les autorités compétentes canalisent leurs demandes par l'intermédiaire de l' UIP de leur propre État membre.

4. À titre exceptionnel, lorsque l'accès à des données PNR est nécessaire pour répondre à une menace précise et réelle liée à des infractions terroristes ou à des formes graves de criminalité, l'UIP d'un État membre a le droit de demander à ce que l'UIP d'un autre État membre obtienne des données PNR conformément à l'article 8, paragraphe 5, et les communique à l'UIP requérante.

5. L'échange d'informations au titre du présent article peut avoir lieu par l'intermédiaire de n'importe quel canal de coopération existant entre les autorités compétentes des États membres. La langue utilisée pour la demande et l'échange

d'informations est celle applicable au canal utilisé. Lorsqu'ils procèdent aux notifications conformément à l'article 4, paragraphe 5, les États membres communiquent également à la Commission les coordonnées des points de contact auxquels les demandes peuvent être adressées en cas d'urgence. La Commission communique lesdites coordonnées aux États membres.

Article 10

Conditions d'accès aux données PNR par Europol

1. Europol est habilité à demander aux UIP des États membres des données PNR ou le résultat du traitement de ces données dans les limites de ses compétences et pour l'accomplissement de ses missions.

2. Europol peut présenter, au cas par cas, à l'UIP de tout État membre par l'intermédiaire de l'unité nationale Europol, une demande électronique dûment motivée de transmission de données PNR spécifiques ou du résultat du traitement de ces données. Europol peut présenter cette demande lorsque cela est strictement nécessaire au soutien et au renforcement de l'action des États membres en vue de prévenir ou de détecter une infraction terroriste spécifique ou une forme grave de criminalité spécifique, ou de mener des enquêtes en la matière, dans la mesure où ladite infraction ou ladite forme de criminalité relève de la compétence d'Europol en vertu de la décision 2009/371/JAI. Cette demande énonce les motifs raisonnables sur lesquels se fonde Europol pour estimer que la transmission des données PNR ou du résultat du traitement de ces données contribuera de manière substantielle à la prévention ou à la détection de l'infraction concernée, ou à des enquêtes en la matière.

3. Europol informe le délégué à la protection des données nommé conformément à l'article 28 de la décision 2009/371/JAI de chaque échange d'informations au titre du présent article.

4. Les échanges d'information au titre du présent article ont lieu par l'intermédiaire de SIENA et conformément à la décision 2009/371/JAI. La langue utilisée pour la demande et l'échange d'informations est celle applicable à SIENA.

Article 11

Transfert de données vers des pays tiers

1. Un État membre peut transférer à un pays tiers des données PNR et le résultat du traitement de ces données, qui sont conservés par l'UIP conformément à l'article 12, uniquement au cas par cas et si:

a) les conditions prévues à l'article 13 de la décision-cadre 2008/977/JAI sont remplies;

b) le transfert est nécessaire aux fins de la présente directive visées à l'article 1er, paragraphe 2;

c) le pays tiers n'accepte de transférer les données à un autre pays tiers que lorsque cela est strictement nécessaire aux fins de la présente directive visées à l'article 1er, paragraphe 2, et uniquement avec l'accord exprès dudit État membre; et

d) les mêmes conditions que celles prévues à l'article 9, paragraphe 2, sont remplies.

2. Nonobstant l'article 13, paragraphe 2, de la décision-cadre 2008/977/JAI, les transferts de données PNR sans l'accord préalable de l'État membre dont les données ont été obtenues, ne sont autorisés que dans des circonstances exceptionnelles et uniquement si:

a) ces transferts sont essentiels pour répondre à une menace précise et réelle liée à une infraction terroriste ou à une forme grave de criminalité dans un État membre ou un pays tiers; et

b) l'accord préalable ne peut pas être obtenu en temps utile.

L'autorité chargée de donner son accord est informée sans retard et le transfert est dûment enregistré et soumis à une vérification ex post.

3. Les États membres ne transfèrent des données PNR aux autorités compétentes de pays tiers que dans des conditions compatibles avec la présente directive et après avoir obtenu l'assurance que l'utilisation que les destinataires entendent faire de ces données PNR respecte ces conditions et garanties.

4. Chaque fois qu'un État membre transfère des données PNR en vertu du

présent article, le délégué à la protection des données de l'UIP de cet État membre en est informé.

Article 12

Période de conservation et dépersonnalisation des données

1. Les États membres veillent à ce que les données PNR fournies par les transporteurs aériens à l'UIP y soient conservées dans une base de données pendant une période de cinq ans suivant leur transfert à l'UIP de l'État membre sur le territoire duquel se situe le point d'arrivée ou de départ du vol.

2. À l'expiration d'une période de six mois suivant le transfert des données PNR visé au paragraphe 1, toutes les données PNR sont dépersonnalisées par le masquage des éléments des données suivants qui pourraient servir à identifier directement le passager auquel se rapportent les données PNR:

a) le(s) nom(s), y compris les noms d'autres passagers mentionnés dans le PNR, ainsi que le nombre de passagers voyageant ensemble figurant dans le PNR;

b) l'adresse et les coordonnées;

c) des informations sur tous les modes de paiement, y compris l'adresse de facturation, dans la mesure où y figurent des informations pouvant servir à identifier directement le passager auquel le PNR se rapporte ou toute autre personne;

d) les informations «grands voyageurs»;

e) les remarques générales, dans la mesure où elles comportent des informations qui pourraient servir à identifier directement le passager auquel le PNR se rapporte; et

f) toute donnée API qui a été recueillie.

3. À l'expiration de la période de six mois visée au paragraphe 2, la communication de l'intégralité des données PNR n'est autorisée que:

a) lorsqu'il existe des motifs raisonnables de croire qu'elle est nécessaire aux fins visées à l'article 6, paragraphe 2, point b); et

b) lorsqu'elle a été approuvée par:

i) une autorité judiciaire; ou

ii) une autre autorité nationale compétente en vertu du droit national pour vérifier si les conditions de communi- cation sont remplies, sous réserve que le délégué à la protection des données de l'UIP en soit informé et procède à un examen ex post.

4. Les États membres veillent à ce que les données PNR soient effacées de manière définitive à l'issue de la période visée au paragraphe 1. Cette obligation s'applique sans préjudice des cas où des données PNR spécifiques ont été transférées à une autorité compétente et sont utilisées dans le cadre de cas spécifiques à des fins de prévention, de détection d'infractions terroristes ou de formes graves de criminalité ou d'enquêtes ou de poursuites en la matière, auquel cas la conservation de ces données par l'autorité compétente est régie par le droit national.

5. Le résultat du traitement visé à l'article 6, paragraphe 2, point a), n'est conservé par l'UIP que le temps nécessaire pour informer les autorités compétentes et, conformément à l'article 9, paragraphe 1, pour informer les UIP des autres États membres de l'existence d'une concordance positive. Lorsque, à la suite du réexamen individuel par des moyens non automatisés visé à l'article 6, paragraphe 5, le résultat du traitement automatisé s'est révélé négatif, il peut néanmoins être archivé tant que les données de base n'ont pas été effacées au titre du paragraphe 4 du présent article, de

manière à éviter de futures «fausses» concordances positives.

Article 13

Protection des données à caractère personnel

1. Chaque État membre veille à ce que, pour tout traitement de données à caractère personnel effectué au titre de la présente directive, chaque passager dispose du même droit à la protection de ses données à caractère personnel, des mêmes droits d'accès, de rectification, d'effacement et de limitation, et droits à réparation et à un recours juridictionnel prévus dans le droit de l'Union et le droit national et en application des articles 17, 18, 19 et 20 de la décision-cadre 2008/977/JAI. Lesdits articles sont par conséquent applicables.

2. Chaque État membre veille à ce que les dispositions adoptées en droit national en application des articles 21 et 22 de la décision-cadre 2008/977/JAI concernant la confidentialité du traitement et la sécurité des données s'appliquent également à tous les traitements de données à caractère personnel effectués en vertu de la présente directive.

3. La présente directive est sans préjudice de l'applicabilité de la directive 95/46/CE du Parlement européen et du Conseil ([1]) au traitement des données à caractère personnel par les transporteurs aériens, en particulier en ce qui concerne leurs obligations de prendre des mesures techniques et organisationnelles appropriées pour protéger la sécurité et la confidentialité des données à caractère personnel.

4. Les États membres interdisent le traitement des données PNR qui révèlent l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle. Dans l'hypothèse où l'UIP reçoit des données PNR révélant de telles informations, elle les efface immédiatement.

5. Les États membres veillent à ce que l'UIP conserve une trace documentaire relative à tous les systèmes et procédures de traitement sous leur responsabilité. Cette documentation comprend au minimum:

a) le nom et les coordonnées de l'organisation et du personnel chargés du traitement des données PNR au sein de l'UIP et les différents niveaux d'autorisation d'accès;

b) les demandes formulées par les autorités compétentes et les UIP d'autres États membres;

c) toutes les demandes et tous les transferts de données PNR vers un pays tiers.

L'UIP met toute la documentation à la disposition de l'autorité de contrôle nationale, à la demande de celle-ci.

6. Les États membres veillent à ce que l'UIP tienne des registres au moins pour les opérations de traitement suivantes: la collecte, la consultation, la communication et l'effacement. Les registres des opérations de consultation et de communication indiquent, en particulier, la finalité, la date et l'heure de ces opérations et, dans la mesure du possible, l'identité de la personne qui a consulté ou communiqué les données PNR, ainsi que l'identité des destinataires de ces données. Les registres sont utilisés uniquement à des fins de vérification et d'autocontrôle, de garantie de l'intégrité et de la sécurité des données ou d'audit. L'UIP met les registres à la disposition de l'autorité de contrôle nationale, à la demande de celle-ci.

Ces registres sont conservés pendant cinq ans.

7. Les États membres veillent à ce que leur UIP mette en œuvre des mesures et des procédures techniques et organisa- tionnelles appropriées afin de garantir un niveau élevé de sécurité adapté aux risques présentés par le traitement et à la nature des données PNR.

8. Lorsqu'une atteinte aux données à caractère personnel est susceptible d'entraîner un risque élevé pour la protection des données à caractère personnel ou d'affecter négativement la vie privée de la personne concernée, les États membres veillent à ce que l'UIP fasse part de cette atteinte à la personne concernée et à l'autorité de contrôle nationale sans retard injustifié.

Article 14

Sanctions

Les États membres déterminent le régime des sanctions applicables aux violations des dispositions nationales adoptées en vertu de la présente directive et prennent toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions.

En particulier, les États membres déterminent le régime des sanctions, y compris des sanctions financières, à l'encontre des transporteurs aériens qui ne transmettent pas de données comme le prévoit l'article 8, ou ne les transmettent pas dans le format requis.

Les sanctions prévues doivent être effectives, proportionnées et dissuasives.

---

(1) 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 ces données (JO L 281 du 23.11.1995, p. 31).

Article 15

Autorité de contrôle nationale

1. Chaque État membre prévoit que l'autorité de contrôle nationale visée à l'article 25 de la décision-cadre 2008/977/JAI est chargée de fournir des conseils sur l'application, sur son territoire, des dispositions adoptées par les États membres en vertu de la présente directive et de surveiller l'application de celles-ci. L'article 25 de ladite décision- cadre s'applique.

2. Ces autorités de contrôle nationales exercent les activités au titre du paragraphe 1 en ayant en vue la protection des droits fondamentaux en matière de traitement des données à caractère personnel.

3. Chaque autorité de contrôle nationale:

a) traite les réclamations introduites par toute personne concernée, enquête sur l'affaire et informe la personne concernée de l'état d'avancement du dossier et de l'issue de la réclamation dans un délai raisonnable;

b) vérifie la licéité du traitement des données, effectue des enquêtes, des inspections et des audits conformément au droit national, de sa propre initiative ou en se fondant sur une réclamation visée au point a).

4. Chaque autorité de contrôle nationale conseille, sur demande, toute personne concernée quant à l'exercice des droits que lui confèrent les dispositions adoptées en vertu de la présente directive.

CHAPITRE III

Mesures d'exécution

Article 16

Protocoles communs et formats de données reconnus

1. Tous les transferts de données PNR effectués par des transporteurs aériens vers les UIP aux fins de la présente directive sont effectués par des moyens électroniques qui offrent des garanties suffisantes en ce qui concerne les mesures de sécurité techniques et les mesures organisationnelles régissant le traitement à effectuer. En cas de défaillance technique, les données PNR peuvent être transférées par tout autre moyen approprié, pour autant que le même niveau de sécurité soit maintenu et que le droit de l'Union en matière de protection des données soit pleinement respecté.

2. À partir de l'année qui suit la date à laquelle la Commission adopte pour la première fois des protocoles communs et des formats de données reconnus conformément au paragraphe 3, tous les transferts de données PNR effectués par des transporteurs aériens vers les UIP aux fins de la présente directive se font par voie électronique à l'aide de méthodes sécurisées respectant ces protocoles communs. Ces protocoles sont identiques pour tous les transferts afin d'assurer la sécurité des données PNR pendant le transfert. Les données PNR sont transférées sous un format de données reconnu afin d'en assurer la lisibilité par toutes les parties concernées. Tous les transporteurs aériens sont tenus de choisir et de préciser à l'UIP le protocole commun et le format de données qu'ils ont l'intention d'utiliser pour leurs transferts.

3. La Commission dresse la liste des protocoles communs et des formats de données reconnus et, si nécessaire, l'adapte au moyen d'actes d'exécution. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 17, paragraphe 2.

4. Tant que les protocoles communs et les formats de données reconnus visés aux paragraphes 2 et 3 ne sont pas disponibles, le paragraphe 1 s'applique.

5. Dans un délai d'un an à compter de la date d'adoption des protocoles communs et des formats de données reconnus visés au paragraphe 2, chaque État membre veille à ce que les mesures techniques nécessaires soient adoptées pour pouvoir utiliser ces protocoles communs et formats de données.

Article 17

Comité

1. La Commission est assistée par un comité. Ledit comité est un comité au sens du règlement (UE) n° 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) n° 182/2011 s'applique.

Lorsque le comité n'émet aucun avis, la Commission n'adopte pas le projet d'acte d'exécution, et l'article 5, paragraphe 4, troisième alinéa, du règlement (UE) n° 182/2011 s'applique.

CHAPITRE IV

Dispositions finales

Article 18

Transposition

1. Les États membres mettent en vigueur les dispositions législatives, réglementaires et administratives nécessaires
pour se conformer à la présente directive au plus tard le 25 mai 2018. Ils en informent immédiatement la Commission.

Lorsque les États membres adoptent ces dispositions, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de leur publication officielle. Les modalités de cette référence sont arrêtées par les États membres.

2. Les États membres communiquent à la Commission le texte des dispositions essentielles de droit interne qu'ils adoptent dans le domaine régi par la présente directive.

Article 19

Réexamen

1. Sur la base des informations communiquées par les États membres, y compris les informations statistiques visées à l'article 20, paragraphe 2, la Commission procède, au plus tard le 25 mai 2020, au réexamen de tous les éléments de la présente directive et communique et présente un rapport au Parlement européen et au Conseil.

2. Dans le cadre de son réexamen, la Commission accorde une attention particulière:

a) au respect des normes applicables de protection des données à caractère personnel;

b) à la nécessité et à la proportionnalité de la collecte et du traitement des données PNR au

regard de chacune des finalités énoncées dans la présente directive;

c) à la durée de la période de conservation des données;

d) à l'efficacité de l'échange d'informations entre les États membres; et

e) à la qualité des évaluations, y compris en ce qui concerne les informations statistiques recueillies en vertu de l'article 20.

Le rapport visé au paragraphe 1 examine également s'il est nécessaire, proportionné et efficace d'inclure dans le champ d'application de la présente directive la collecte et le transfert des données PNR, à titre obligatoire, pour l'ensemble des vols intra-UE ou une sélection de ceux-ci. La Commission tient compte de l'expérience acquise par

3. les États membres, en particulier ceux qui appliquent la présente directive aux vols intra-UE conformément à l'article 2. Le rapport examine également s'il est nécessaire d'inclure des opérateurs économiques autres que les transporteurs, tels que des agences et des organisateurs de voyages qui fournissent des services liés aux voyages, y compris la réservation de vols, dans le champ d'application de la présente directive.

4. Le cas échéant, au vu du réexamen effectué au titre du présent article, la Commission soumet une proposition législative au Parlement européen et au Conseil en vue de modifier la présente directive.

Article 20

Données statistiques

1. Les États membres fournissent chaque année à la Commission une série de statistiques sur les données PNR communiquées aux UIP. Ces statistiques ne contiennent pas de données à caractère personnel.

2. Les statistiques concernent au moins:

a) le nombre total de passagers dont les données PNR ont été recueillies et échangées;

b) le nombre de passagers identifiés en vue d'un examen plus approfondi.

Article 21

Rapports avec d'autres instruments

1. Les États membres peuvent continuer d'appliquer les accords ou arrangements bilatéraux ou multilatéraux en matière d'échange d'informations entre les autorités compétentes qu'ils ont conclus entre eux et qui sont en vigueur au 24 mai 2016, dans la mesure où ceux-ci sont compatibles avec la présente directive.

2. La présente directive s'applique sans préjudice de l'applicabilité de la directive 95/46/CE au traitement des données à caractère personnel par les transporteurs aériens.

3. La présente directive s'applique sans préjudice des obligations et engagements d'États membres ou de l'Union qui découlent d'accords bilatéraux ou multilatéraux avec des pays tiers.

Article 22

Entrée en vigueur

La présente directive entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Les États membres sont destinataires de la présente directive conformément aux traités

Fait à Bruxelles, le 27 avril 2016.

Par le Parlement européen Le président
M. SCHULZ

Par le Conseil Le président
J.A. HENNIS-PLASSCHAERT

ANNEXE I

Données des dossiers passagers telles qu'elles sont recueillies par les transporteurs aériens

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

ANNEXE II

Liste des infractions visées à l'article 3, point 9)

1. Participation à une organisation criminelle
2. Traite des êtres humains
3. Exploitation sexuelle des enfants et pédopornographie
4. Trafic de stupéfiants et de substances psychotropes
5. Trafic d'armes, de munitions et d'explosifs
6. Corruption
7. Fraude, y compris la fraude portant atteinte aux intérêts financiers de l'Union
8. Blanchiment du produit du crime et faux monnayage, y compris la contrefaçon de l'euro
9. Cybercriminalité
10. Infractions graves contre l'environnement, y compris le trafic d'espèces animales menacées et le trafic d'espèces et d'essences végétales menacées
11. Aide à l'entrée et au séjour irréguliers
12. Meurtre, coups et blessures graves
13. Trafic d'organes et de tissus humains
14. Enlèvement, séquestration et prise d'otage
15. Vol organisé ou vol à main armée
16. Trafic de biens culturels, y compris d'antiquités et d'œuvres d'art
17. Contrefaçon et piratage de produits
18. Falsification de documents administratifs et trafic de faux
19. Trafic de substances hormonales et d'autres facteurs de croissance
20. Trafic de matières nucléaires et radioactives
21. Viol
22. Infractions graves relevant de la Cour pénale internationale
23. Détournement d'avion/de navire
24. Sabotage
25. Trafic de véhicules volés
26. Espionnage industrie

ANNEXE 2

QUESTIONNAIRE – MISSION PNR FRANCE

Ce questionnaire a été rédigé pour la Mission PNR. L'objectif était d'apprendre à connaître le fonctionnement du système expérimental API-PNR France.

1. Pensez-vous qu'il est possible qu'un jour se développe une unité centrale européenne qui serait en charge de gérer toutes les demandes de transfert de données en provenance et à destination de l'Union Européenne?

   C'est peu probable car les problématiques traitées relèvent de la souveraineté de l'Etat.

2. Quelle est la particularité du PNR?

   La particularité est que le Fichier est utilisé à des fins de ciblage et de criblage: les interrogations du Fichier PNR permettent de repérer des signaux faibles.

3. La Directive PNR est silencieuse sur le mode de résolution de litige entre UIP. Comment se fait la résolution de litige entre deux Etats membres ou deux UIP?

   En cas de litige, les UIP seraient amenées à discuter entre elles.

   Des groupes de travail ont déjà été constitués dans l'Union afin de réfléchir à la manière dont doivent être échangées les données et sous quelles conditions (comment doivent être motivées les demandes d'échanges de données etc.).

4. Comment vous assurez-vous que les données sont effacées de manière permanente?

Les données sont supprimées physiquement de manière définitive des serveurs après 5 ans.

5. Est-ce que des « Données Sensibles » sont déjà arrivées, par accident, en mode « visible » à l'UIP?

Non. Mais il est vrai que l'UIP a accès aux « free texts », complétées par les compagnies aériennes, dans lesquels peuvent se trouver des Données Sensibles.

6. Quelle est la procédure en cas de démasquage ?

Le démasquage doit être demandé par les autorités compétentes ayant émis la requête, au directeur de l'UIP ou à son adjoint. Ce sont les deux seules personnes habilitées à démasquer les données. Il s'agit d'une garantie permettant d'éviter un accès aux données sans raison « dûment motivée » (selon l'expression employée à l'article 6§2.b de la Directive PNR).

7. Dans l'hypothèse où le logiciel rejette par erreur un envoi de Fichier, l'UIP pourrait-elle avoir accès au système des compagnies aériennes pour récupérer l'envoi ou bien faudrait-il redemander un envoi?

Il faudrait dans ce cas redemander à la compagnie aérienne de faire un envoi. L'UIP ne peut pas avoir accès à leur système. Les données sont uniquement transmises vers l'UIP par méthode dite « push » par les compagnies aériennes et les Fournisseurs de Données.

La France pourrait-elle avoir accès à un PNR qui n'a aucun lien avec son territoire?

Non, sauf à revenir aux circuits traditionnels de coopérations policières ou en interrogeant une autre UIP sur sollicitation primaire d'une autorité compétente française. Il s'agit alors de relations inter-UIP comme décrite dans la Directive PNR.

8. Dans les faits, comment l'UIP s'assure du fait que l'Autorité Compétente ait le droit de faire une demande ?

L'UIP doit s'assurer que le Service Utilisateur qui demande l'accès à une donnée soit bien habilité. En revanche, l'UIP n'est pas responsable de l'utilisation ultérieure des données par les Services Utilisateurs.

9. Pensez- vous qu'il serait possible pour un Etat membre de ne pas passer par son UIP et de directement s'adresser à un autre Etat membre pour avoir le PNR d'un passager?

Non. Les UIP pourraient être mises de côté dans l'hypothèse du retour à la coopération classique entre les Etat en matière policière et judiciaire. Mais cela ne relèverait pas du cadre d'application de la Directive PNR.

10. Les Fichiers PNR sont-ils conservés de manière indifférenciée ou bien sont-ils classés?

Aucune liste n'est créée: les Fichiers sont conservés de manière brute, tels que reçus. Les agents de l'UIP n'ont pas accès aux données stockées dans la base de données, sauf dans le cas d'un hit ou une requête d'une Autorité Compétente.

11. Savez-vous, pour la France, parmi la liste des infractions visées en annexe de la Directive PNR, lesquelles sont les plus utilisées en pratique ?

Il n'existe pas encore de statistiques à ce sujet. A priori, on peut considérer que le Fichier PNR est davantage sollicité pour les trafics de stupéfiants, d'armes, la fraude, le meurtre et le vol organisé.

Les Services Utilisateurs qui sollicitent le plus l'UIP sont la douane, la police nationale et les services de renseignement.

12. Savez-vous pourquoi la Directive PNR ne mentionne pas la liste des Fichiers avec lesquels il y peut y avoir des interconnexions ?

Le choix des Fichiers avec lesquels seront effectuées les interconnexions est propre à chaque Etat. Mais le silence de la Directive PNR soulève des difficultés d'application notamment celle de savoir quels Fichiers choisir. Il s'agit d'une décision politique et juridique car les Fichiers sollicités devront être légalement conformes aux finalités imposées par la Directive.

13. Savez-vous pourquoi la France a décidé que l'UIP relèverait de 4 ministères (le ministère de l'intérieur, le ministère des armées, le ministère de la transition écologique et solidaire - chargé des Transports et le ministère de l'action et des comptes publics) ? Pourquoi le choix de la « collégialité » ? Pourquoi le choix de ces 4 ministères en particulier ?

Les agents de l'UIP sont issus de ces 4 ministères. L'intérêt est de disposer d'agents possédant une expertise dans leur domaine respectif : le renseignement, la lutte contre la fraude…
Cela permet aux agents d'être en mesure de comprendre et d'analyser les requêtes des Services Utilisateurs afin d'effectuer les meilleures levées de doute possibles.

14. A propos du champ d'application géographique :la France compte-elle étendre l'utilisation du PNR aux vols intra-européens ?

Oui la France compte étendre l'utilisation du PNR aux vols intra-européens.

Chaque Etat peut choisir d'étendre le champ d'application aux vols intra-européens. Il suffit de le notifier à la Commission.

La Directive PNR ne prévoit pas d'étendre le Traitement aux vols internes.

15. Savez-vous si d'autres Etats membres prévoient d'étendre le PNR à d'autres modes de transports ?

Oui. Le Royaume-Uni et Belgique ont déjà étendu le système PNR au transport maritime et ferroviaire par exemple. En France, des réflexions sont en cours pour l'étendre au transport ferroviaire et le principe d'un PNR maritime est acté. Mais cela pourrait s'accélérer en cas de durcissement du contexte sécuritaire.

L'intérêt d'un système multimodal est de permettre de cartographier tout le territoire, de repérer les réseaux. D'autant plus qu'en général, les « criminels » utilisent une combinaison de moyens de déplacements.

La difficulté pour le transport ferroviaire est la possibilité d'accéder au train sans contrôle d'identité, voire sans carte d'embarquement, ce qui réduirait l'efficacité du PNR ferroviaire. Par ailleurs, imposer des contrôles d'identité aurait un impact négatif sur la fluidité du trafic dans les gares.

16. Combien de requêtes et de demandes de consultations de la part « des Autorités Compétentes » ont été reçues par l'UIP ? Quelle est la variation de ce nombre?

4000 à 5000 hits (de ciblage et de criblage confondus) sont transmis par mois aux Autorités Compétentes. L'UIP reçoit actuellement en moyenne 200 à 300 demandes de requêtes par mois.

17. Quel est le nombre d'interconnexions effectuées avec d'autres Fichiers (par rapport au nombre total de Fichiers) ? Quelle est la variation de ce nombre depuis la mise en place du système (augmentation ou diminution ou tendance identifiée / identifiable) ?

Les statistiques à ce propos sont décentralisées au sein des Autorités Compétentes. L'UIP n'a pas de statistiques à ce sujet.

18. Quel est le nombre de personnes concernées (suspects déjà connus et inconnus des Fichiers) ? Quelle est la variation de ce nombre ?

Il n'y a pas de statistiques à ce sujet. L'UIP n'a pas accès à cette donnée. Chaque Autorité Compétente réalise ses propres statistiques.

19. Combien d'employés travaillent dans l'UIP ? Quels profils composent l'UIP :

Aujourd'hui, 50 agents sont employés par l'UIP, en particulier des informaticiens, douaniers, policiers et militaires et des gendarmes. A termes, l'UIP comptera 68 agents.

20. Certains Etats sont-ils déjà plus réticents que d'autres à fournir des informations ?
Non.

21. Est-il possible de refuser de collaborer avec certains Etats ?

La France n'a pas de réticence particulière pour collaborer.

C'est l'UIP qui a le pouvoir d'accepter ou de refuser une requête.

L'UIP ne fait pas de politique et à partir du moment où une requête est suffisamment motivée et justifiée, l'UIP transmettra les informations demandées.

22. Avez-vous accès aux PNR de membres de gouvernements (ministres, présidents…) ou de familles royales (Arabie Saoudite) ?

Si ces personnes voyagent sur un vol commercial, leurs données sont effectivement enregistrées. Mais elles ne seront visibles et accessibles qu'en cas de hit à la suite d'une requête dans le système par une Autorité Compétente.

23. Certaines compagnies de certains pays sont-elles plus récalcitrantes à vous fournir les données ?

La problématique de réciprocité existe. Mais ce sont en fait les compagnies aériennes qui seront sanctionnées si elles refusent de communiquer les données de leurs passagers. Ce cas de figure peut se produire avec les compagnies nationales dont l'Etat impose de ne pas transmettre les données PNR, ce qui peut se produire avec des pays tiers avec lesquels l'UE n'a pas d'accord.

24. Des sanctions ont-elles déjà été infligées à certaines compagnies ? Y-a-il déjà eu des contestations ? Pensez-vous que se « limiter » à des sanctions financières pour les compagnies aériennes en cas de manquement est suffisant ?

Le système étant toujours en montée en puissance, aucune sanction n'a encore été prononcée. Le principe est plutôt d'avoir de bonnes relations avec les compagnies aériennes et autres Fournisseurs de Données, de travailler « main dans la main ».

25. Des personnes n'ayant jamais commis d'infractions ont-elles déjà été identifiées par le système (par exemple : homonymie) ? *Oui.*

Quelle procédure est mise en place ? *Une liste blanche au sein de laquelle ces personnes sont identifiées et grace à laquelle leurs données sont alors exclues des recherches.*

26. Une violation des données personnelles des passagers a-t-elle déjà eu lieu ?

Non.

27. Comment les « Autorités Compétentes » formulent-elles les requêtes de transferts de Fichiers ?

Il s'agit d'une demande manuelle au cas par cas faite à l'UIP. L'UIP intervient ensuite pour valider cette requête et transmettre le cas échéant les informations demandées après la levée de doute.

28. La littérature parle de la possibilité d'effectuer des vérifications « en temps réel » dans les aéroports ? Comment cela se passe-t-il en pratique ?

Puisque les données PNR sont à envoyer 48h à l'avance, les Autorités Compétentes qui ont besoin d'en connaître ont le temps d'être prévenues. Les autorités de police aéroportuaires peuvent être informées du hit et des raisons pour lesquelles un hit a eu lieu. Elles peuvent être amenées à contrôler le passager sur la plateforme aéroportuaire afin de procéder à des vérifications. Ce contrôle peut mener à l'interpellation de la personne.

29. Quels sont les critères utilisés par les Autorités Compétentes pour "évaluer" les passagers à risque ? Pourriez-vous donner quelques exemples de critères ?

Ce sont les Autorités Compétentes qui déterminent les critères partir des données envoyées par les compagnies aériennes. L'envoi de ces données commerciales aux autorités publiques se fait selon des normes internationales établies par IATA et l'OACI (PAXLIST ou PNRGOV). Un dossier passager contient 286 champs d'informations. Tous les champs ne sont pas remplis par les compagnies. C'est à partir de ces champs d'information que les Autorités Compétentes sélectionnent les crières qui les intéressent pour établir les profils de recherche. Ces profils correspondent à des comportements qui ont statistiquement le plus de chance d'être à risque. Puis en cas de correspondance entre l'un de ces profils et un dossier passager, l'UIP intervient pour valider le profil établit et la correspondance obtenue.

Les critères peuvent être les suivants : faire des ruptures dans son voyage, payer un billet dans un pays X, pour partir d'un pays Z etc.

30. Des audits (par la CNIL ?) sont-ils organisés pour s'assurer du respect de l'équilibre entre les libertés publiques et la sécurité publique et du non transfert de données sensibles ?

Oui deux audits ont déjà été effectués par la CNIL et trois par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) tout au long du développement du système.

31. Comment l'UIP et l'Etat s'assurent de la légalité/légitimité/proportionnalité/nécessité de l'analyse qui est menée ?

Ce sont les agents de l'UIP, grâce à leurs compétences, qui sont garants de la légalité du système. Ils vérifient la légitimité et la conformité des requêtes qui sont formulées. Tant qu'ils ne valident pas les requêtes des Autorités Compétentes, ces deniers ne peuvent pas avoir accès à l'information souhaitée.

32. Quelle est la fréquence de la mise à jour des Fichiers avec lesquels sont effectuées les interconnexions pour éviter que quelqu'un qui n'ait plus à y figurer soit supprimé ?

Une mise à jour du FPR a lieu deux fois par jour. Si une personne n'a plus à figurer dans les Fichiers de Police, a priori son dossier disparaitra.

33. Quelles ont été les difficultés de transmission de la part des compagnies : données illisibles, incomplètes, logiciels incompatibles etc. ?

Les principales difficultés sont liées à des données non conformes (champs mal remplis ou bien traduction de noms étrangers). Une erreur ne serait-ce que d'une seule lettre sur un prénom peut compliquer les recherches. Dans ce cas, plutôt que d'effectuer « une recherche exacte » (fondée sur des informations certaines), il faut effectuer une recherche « floue » (fondée sur une recherche approximative : on recherche une période plutôt qu'un jour donné par exemple). En cas de hit, l'UIP devra sélectionner le

résultat le plus pertinent en fonction des critères de recherche choisis avant la transmission aux Autorités Compétentes. Dans ce type de recherche, le contrôle manuel de l'UIP est particulièrement important afin d'éviter des erreurs.

L'autre difficulté est que les compagnies ont généralement plusieurs sous-traitants pour le traitement de leurs données : certaines ont un prestataire pour les données API et un autre pour les données PNR. Il faut certifier chacun des acteurs et raccorder chacun des systèmes à l'UIP.

Par ailleurs, il n'existe pas d'obligation de transmettre les données API équipages ce qui représente un risque.

34. Quels ont été les dysfonctionnements du système ? Y en a-t-il encore ? Quelles améliorations seraient à apporter ?

Il faudrait améliorer les capacités de stockage qui peuvent devenir rapidement limitées.

35. Où sont stockées les données traitées ?

Les données sont stockées dans l'UE. En France, elles sont stockées par un service de l'Etat : le Service du Traitement de l'Information de la Gendarmerie (STIG).

36. La durée de conservation totale des données (5 ans) et non masquées (6 mois) est-elle correcte au regard de la durée des enquêtes?

Chaque voyage génère un Fichier PNR. La date d'entrée dans le système déclenche le décompte pour l'effacement des données qui a lieu au bout de 5 ans. La durée de conservation non masquée des données est trop courte. Pour pouvoir établir les habitudes de voyage d'un passager, il faut souvent du temps : une durée optimale serait de 2 ou 3 ans. En conséquence, il est possible que les demandes de démasquages soient très nombreuses.

37. Le système vous semble-t-il effectif au regard de sa finalité?

Oui.

38. Pensez-vous que les autres Fichiers (SIS II etc.) auraient été suffisant ou bien pensez-vous que le PNR apporte une plus-value (ex : données pro-active et réactive) ?

Le PNR présente l'avantage de permettre un croisement avec plusieurs Fichiers en même temps ce qui permet un gain de temps et une meilleure efficacité.

39. Pensez-vous que le Fichier PNR peut mener à des dérives ?

Les risques de dérives et d'abus sont très peu probables. Par exemple, les agents de l'UIP ne peuvent avoir accès aux données qu'en cas de demande de la part des Autorités Compétentes, toutes les activités sur un Fichier font l'objet d'une journalisation, des audits sont réalisés, toutes les autorités compétentes n'ont pas les mêmes droits d'accès aux données. Quant aux données « sensibles », elles sont détruites/effacées avant stockage dans le système PNR.

En revanche, l'utilisation ultérieure par les Autorités Compétentes ne peut pas être contrôlée par l'UIP.

40. Pensez-vous qu'il serait plus efficace d'avoir recours à un contrôle ciblé de certaines personnes identifiées plutôt qu'un contrôle de masse ?

La collecte de données « en masse » permettent d'analyser les signaux faibles, ce qui ne serait pas possible avec un ciblage sur un individu en particulier.
L'accès au Fichier d'un passager en particulier peut permettre de vérifier son alibi par exemple. Les utilisations répondent à différents besoins.

41. La France prévoit-elle de partager son UIP avec d'autres Etats ?

La France ne souhaite pas partager son UIP avec d'autres Etats pour des questions de souveraineté. Mais d'autres Etats membres ont prévu de le faire.

42. Les Données Sensibles sont-elles « réellement » non utilisées, dans la pratique ? Pensez-vous qu'il pourrait être intéressant, au regard des finalités de la Directive PNR d'utiliser ces données ?

Oui, les Données Sensibles sont bloquées par l'algorithme.

Il est préférable de ne pas avoir accès aux Données Sensibles, en particulier les données liées à la religion. Cela évite les amalgames.

43. Les agents de l'IUP sont-ils formés à la protection des données ?

Oui les agents de l'administration en général doivent être formés à la protection des données et les agents de l'UIP sont particulièrement formés à cette problématique.

44. Les compagnies seront-elles responsables d'informations erronées si les passagers donnent des informations erronées ?

A priori, les compagnies ne pourront pas être tenues pour responsables des erreurs dans la transmission des données PNR car celles-ci sont déclaratives, chaque passager complète les informations comme il le souhaite lors d'une réservation.

ANNEXE 3

<table>
<tr><th>Données API (données d'embarquement et de débarquement fournies par les transporteurs aériens)[1]</th><th>Données PNR telles que transposées en droit français[1]</th><th>Données enregistrées Bande MRZ (passeport, CI, visa)[2]</th></tr>
<tr><td colspan="3">Nom complet</td></tr>
<tr><td colspan="3">Date de naissance</td></tr>
<tr><td>Nationalité</td><td rowspan="2"></td><td>Nationalité</td></tr>
<tr><td>Sexe</td><td>Sexe</td></tr>
<tr><td rowspan="4"></td><td>Numéro de téléphone, adresse électronique</td><td rowspan="4"></td></tr>
<tr><td>Toutes les informations disponibles sur les mineurs non accompagnés de moins de 18 ans, telles que le nom et le sexe, son âge, la ou les langues parlées, le nom et les coordonnées de la personne présente au départ et son lien avec le mineur, le nom et les coordonnées de la personne présente à l'arrivée et son lien avec le mineur, l'agent présent au départ et à l'arrivée</td></tr>
<tr><td>Agence de voyages/agent de voyages</td></tr>
<tr><td>Remarques Générales (à l'exclusion de de toutes les informations susceptibles de révéler des données sensibles)</td></tr>
<tr><td>Numéro et type du document de voyage utilisé</td><td rowspan="3"></td><td>Date de validité</td></tr>
<tr><td>Date d'expiration du document de voyage</td><td>Etat émetteur</td></tr>
<tr><td>Etat ou organisation émettrice du document de voyage</td><td>Validité territoriale</td></tr>
<tr><td colspan="2">Code repère du dossier passager</td><td>Date d'expiration / de fin de validité du visa</td></tr>
<tr><td rowspan="5"></td><td rowspan="2"></td><td>Nombre d'entrées</td></tr>
<tr><td>Durée du séjour</td></tr>
<tr><td>Informations sur l'établissement des billets, y compris le numéro du billet, la date d'émission, les allers simples, décomposition tarifaire</td><td rowspan="4"></td></tr>
<tr><td>Date de réservation/d'émission du billet</td></tr>
<tr><td>Moyen de paiement, y compris l'adresse de facturation</td></tr>
<tr><td>Indications concernant la scission/division du PNR</td></tr>
</table>

[1] Article R232-14. I.b) du Code de la sécurité intérieure

[2] DUPONT PASCAL, *« Les Données des Passagers (PNR) dans le Transport Aérien »*. Revue Française de Droit Aérien et Spatial. Edition A. Pedone. Volume n°278 - n°2-2016. Soixante-dixième année, P.11 à 128.

	Informations "grands voyageurs" tel que les programmes de fidélité	
Statut du voyageur (toute information sur les correspondances)	Statut du voyageur, y compris les confirmations, l'enregistrement, la non-présentation ou un passager de dernière minute sans réservation	
Numéro de siège	Numéro du siège et autres informations concernant le siège	
Nombre, poids et identification des bagages	Toutes les informations relatives aux bagages	
	Itinéraire complet	
Heures de départ et d'arrivée du transport		
Point de départ et d'arrivée du vol		
Point d'embarquement initial et de débarquement final des passagers		
Point de passage frontalier utilisé pour entrer ou sortir du territoire français		
Nombre total des personnes transportées		
	Nombre et autres noms de voyageurs figurant dans le PNR	
Code de transport (numéro du vol et code du transporteur aérien)	Informations sur le partage de code	
Date(s) prévue(s) du voyage		
	Toutes les informations API	
	Historique complet des modifications	

ANNEXE 4

RECAPITULATIF DES TEXTES CITES			
Domaines concernés	Cadre législatif	Textes de référence	Finalités / Champ d'application
Traitements de Données à Caractère Personnel	Droit international	La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Conseil de l'Europe (1981)	Seul texte, en droit international relatif au Traitement automatisé des Données à Caractère Personnel dans les secteurs privés, publics et pénal.
	Droit de l'UE	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. Texte abrogé par la Directive (UE) 2016/680.	Traitement de données à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou d'exécution de sanctions pénales
		Directive (UE) 2016/680 du Parlement Européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil du 27/11/2008	Abroge et remplace la Décision-cadre 2008/977/JAI. Texte de référence dans l'UE en matière de protection des Données à Caractère Personnel dans le secteur judiciaire et le secteur pénal
		Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière.	Législation spécifique qui s'applique au Traitement des données PNR dans le secteur du transport aérien

		Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (RGPD)	Texte de référence dans l'UE en matière de protection des Données à Caractère Personnel dans les secteurs autres que judiciaire et pénal « Droit commun » du Traitement des Données à Caractère Personnel
		Directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers	Législation spécifique créant les données API et régissant leur Traitement afin d'améliorer le contrôle aux frontières et lutter contre l'immigration clandestine
		Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), JO 2002 L 201.	Textes spécifiques au Traitement des Données à Caractère Personnel dans le secteur des communications électroniques
		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, et modifiant la directive 2002/58/CE, (directive sur la conservation des données), JO 2006 L 105 (invalidée le 8 avril 2014).	
	Droit français	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	Texte de référence en France en matière de Traitement de Données à Caractère Personnel dans les secteurs publics, privés, y compris judiciaires et pénaux
		Décret n° 2018-714 du 3 août 2018 relatif au « système API-PNR France » et modifiant le code de la sécurité intérieure JORF n°0181 du 8 août 2018 texte n° 2	Décrets de transposition

		Décret n° 2018-722 du 3 août 2018 modifiant le décret n° 2014-1566 du 22 décembre 2014 portant création d'un service à compétence nationale dénommé « Unité Information Passagers » (UIP) JORF n°0181 du 8 août 2018 texte n° 39	de la Directive PNR
		Décret n° 2014-1095 du 26 septembre 2014 portant création d'un Traitement de Données à Caractère Personnel dénommé « système API-PNR France » pris pour l'application de l'article L. 232-7 du code de la sécurité intérieure. JORF n°0225 du 28 septembre 2014 page 15777	Décrets de création du système API PNR France
		Décret n° 2014-1566 du 22 décembre 2014 portant création d'un service à compétence nationale dénommé « Unité Information Passagers » (UIP)	
Terrorisme	Droit de l'UE	Décision-cadre 2002/475/JAI relative à la lutte contre le terrorisme	Harmoniser la définition des infractions pénales, des sanctions et des mesures de protection à mettre en place dans le domaine des infractions terroristes
		Directive (UE) 2017/541 Du Parlement Européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil	

Traitement de Données à Caractère Personnel	Droit international	Projet d'accord entre le Canada et l'Union Européenne sur le transfert et le Traitement de Données des dossiers passagers	Projet d'accord permettant le transfert de données PNR entre l'UE et le Canada (pas encore en vigueur)
		Accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers (données PNR) et leur transfert au ministère américain de la sécurité intérieure	Accord permettant le transfert de données PNR entre l'UE et les USA (en vigueur)